ELEMENTY ARYTMETYKI I TEORII LICZB Z ZADANIAMI

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Ryszard R. Andruszkiewicz

ELEMENTY ARYTMETYKI I TEORII LICZB Z ZADANIAMI

Białystok 2023

Recenzenci:
prof. dr hab. Jarosław Grytczuk (PW)
dr hab. Tomasz Jędrzejak, prof. US

Opracowanie graficzne:
Karol Pryszczepko

Redakcja i korekta:
Janina Demianowicz

Korekta merytoryczna:
Karol Pryszczepko

Redakcja techniczna i skład:
Ryszard R. Andruszkiewicz

ISBN 978-83-7431-769-6

Wydanie publikacji zostało sfinansowane ze środków
Wydziału Matematyki Uniwersytetu w Białymstoku

Wydawnictwo Uniwersytetu w Białymstoku
15-328 Białystok, ul. Świerkowa 20B, tel. 857 457 120
http://wydawnictwo.uwb.edu.pl, wydawnictwo@uwb.edu.pl

Druk i oprawa: Volumina.pl sp. z o.o.

Spis treści

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Wstęp

Ta książka przeznaczona jest głównie dla studentów matematyki i informatyki, którzy na różnych uczelniach wyższych mają przedmioty o nazwie „Elementy arytmetyki i algebry", czy też „Elementarna teoria liczb", „Wstęp do teorii liczb"i inne. Może też być przydatna dla słuchaczy studiów podyplomowych z matematyki oraz dla nauczycieli szkół podstawowych i średnich. Zawarty tu materiał będzie też bardzo pomocny uczestnikom olimpiad matematycznych i różnorodnych konkursów matematycznych. Właśnie z myślą o młodych adeptach matematyki autor podał rozwiązania kilkuset zadań w jak najprostszej postaci, unikając zbyt rozbudowanego aparatu pojęciowego.

W przekonaniu autora szkolna edukacja z teorii liczb jest bardzo chaotyczna, a zadania z egzaminów ósmoklasistów i maturalne potwierdzają to, że ta tematyka sprawia bardzo duże problemy uczniom. Także materiały przygotowujące do takich egzaminów bardzo rzadko zawierają usystematyzowany wykład podstawowych twierdzeń i pojęć z teorii liczb, nie mówiąc już o ich dowodzeniu. Dociekliwy uczeń może pragnąć wytłumaczenia, dlaczego przedstawiony mu algorytm jest poprawny, albo na przykład stawiać pytania typu „dlaczego $(-1)\cdot(-1) = 1$?"i wprowadzić w zakłopotanie nauczyciela lekceważącego algebraiczne aspekty arytmetyki. Ambicją autora tej książki jest dołączenie do tych, którzy pragną zmienić ten stan rzeczy.

W publikacji arytmetyka jest rozumiana jako konstrukcja różnych zbiorów liczbowych. Aby nie odsyłać Czytelnika do innych pozycji, przedstawiono kompletną teorię liczb naturalnych opartych na aksjomatach Peano, następnie skonstruowano pierścień liczb całkowitych, a później ciała liczb wymiernych, rzeczywistych i zespolonych. W prze-

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

konaniu autora taka kolejność wykładu odpowiada kolejności historycznej i ma ważne zalety dydaktyczne. Niektóre osoby mogą bardziej interesować się dowodami twierdzeń dotyczących podstawowych własności liczb naturalnych lub liczb całkowitych, a inne osoby mogą bardziej interesować się konstrukcją ciała liczb rzeczywistych lub ciała liczb zespolonych, inne wreszcie osoby mogą uzupełnić i usystematyzować swoją wiedzę o ciałach abstrakcyjnych i ciałach uporządkowanych. Wszystko to jest zawarte w jednej książce. Autor celowo przechodzi od prostszych pojęć i struktur algebraicznych do bardziej abstrakcyjnych, kierując się przekonaniem, że lepiej najpierw poznać prostsze obiekty (jakim są na przykład liczby naturalne), a dopiero później przechodzić do bardziej abstrakcyjnych rzeczy (jakim są na przykład ciała uporządkowane). Znajomość wielu przykładów prostych struktur algebraicznych i rozumowań stosowanych przy ich badaniu pozwala łatwiej przejść do struktur bardziej złożonych pod względem abstrakcyjnym. Z troski o Czytelnika niezaznajomionego z algebrą abstrakcyjną taka właśnie idea przyświecała autorowi. Czytelnicy zaznajomieni lub nie zainteresowani podstawowymi aspektami arytmetyki, mogą pominąć te rozdziały i przejść od razu do lektury drugiej części monografii dotyczącej teorii liczb.

Piękno teorii liczb polega między innymi na tym, że posługuje się ona ciekawymi rozumowaniami logicznymi, stawia często prosto sformułowane problemy, których rozwiązania nierzadko zadziwiają, a niekiedy zmuszają do rozbudowania narzędzi badawczych. Jak pisze W. Sierpiński w [34] „Rozumowania używane w teorii liczb są przeważnie bardzo proste co do swej konstrukcji logicznej, stanowią więc one doskonały materiał do ćwiczenia się w myśleniu matematycznym. Z drugiej strony teoria liczb musi się nieraz, przy rozwiązywaniu zagadnień całkiem elementarnych, posługiwać różnymi działami matematyki wyższej, co jest niezmiernie pouczające i otwiera szerokie horyzonty". W pełni podzielając tę opinię, życzymy Czytelnikowi przyjemnej lektury i pożytku w stosowaniu prezentowanej tu wiedzy.

Rozdział 1

Liczby naturalne

1.1 Różne aspekty liczb naturalnych

Jednym z najdawniejszych pojęć abstrakcyjnych są liczby naturalne: 1, 2, 3, ... Pojęcie to zaczęło kształtować się wiele tysięcy lat przed narodzeniem Chrystusa, właściwie od chwili, gdy rozróżnienie między „jeden" i „wiele" przestało człowiekowi wystarczać. Związane było z liczeniem zwierząt, owoców i różnych przedmiotów i przy tej czynności spotkano się z różnymi zbiorami skończonymi równolicznymi.

Liczba naturalna n jest więc cechą posiadania dokładnie n elementów przez pewien zbiór. Jest to tak zwany **aspekt mnogościowy (kardynalny)** pojęcia liczby naturalnej - bardzo ważny ze szkolnego punktu widzenia.

Innym, naturalnym i ważnym aspektem pojęcia liczby naturalnej jest **aspekt porządkowy**, związany z pytaniem: „który z kolei?", a więc: pierwszy, drugi, trzeci, itd.

W dydaktyce szkolnej występuje także **aspekt miarowy** liczby naturalnej („ile kilogramów?", „ile metrów?", itd.). Wykorzystywanie tych aspektów ma na celu wyrobienie i ukształtowanie abstrakcyjnego spojrzenia na liczby naturalne. Oczywiście zależy nam także na wyrobieniu sprawności rachunkowej u uczniów, a to z kolei ma związek z **aspektem algebraicznym** liczby naturalnej.

Zero, jak mówi historia matematyki, jest liczbą o wiele młodszą od

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

liczb naturalnych. Zostało wprowadzone prawdopodobnie przez Hindusów około połowy X wieku. **Zera nie będziemy zaliczać do liczb naturalnych**. Oczywiście, zaliczanie lub niezaliczanie zera do liczb naturalnych zależy od umowy. Każda z dwóch możliwych decyzji jest poprawna (w szkole zero zalicza się do liczb naturalnych!), ale raz podjęta musi być konsekwentnie przestrzegana.

Teraz zostanie przedstawione aksjomatyczne podejście do liczb naturalnych, które pochodzi od Giuseppe Peano (1858-1932), włoskiego matematyka. Robimy to w celu zaznajomienia z teoriami aksjomatycznymi w matematyce. Właśnie aksjomatyka Peano jest bardzo dobrą i klarowną ilustracją budowania takich teorii.

1.2 Aksjomatyka Peano

Za pojęcia pierwotne przyjmujemy zbiór liczb naturalnych $\mathbb{N}$, 1 oraz pojęcie: m jest następnikiem k. Intuicyjny sens tego ostatniego pojęcia jest taki, że liczba m jest liczbą naturalną następującą bezpośrednio po liczbie k. Następnikiem 1 jest 2, następnikiem 2 jest 3, itd.

Aksjomat 1. $1 \in \mathbb{N}$.

Aksjomat 2. 1 nie jest następnikiem żadnej liczby naturalnej.

Aksjomat 3. Dla każdego $k \in \mathbb{N}$ istnieje dokładnie jedno $n \in \mathbb{N}$ takie, że n jest następnikiem k (to jedyne n oznaczamy dalej przez k^*).

Aksjomat 4. Jeżeli $m, n \in \mathbb{N}$ i $m^* = n^*$, to $m = n$.

Aksjomat 5 (Zasada indukcji zupełnej). Jeżeli $A \subseteq \mathbb{N}$ i spełnione są warunki:

(1) $1 \in A$ oraz

(2) dla każdej liczby naturalnej n prawdziwa jest implikacja:
$n \in A \Rightarrow n^* \in A$,

to każda liczba naturalna należy do A, czyli $A = \mathbb{N}$.

Wszystkie dalsze pojęcia, którymi operuje się w arytmetyce liczb naturalnych, jak działania dodawania i mnożenia, relacja mniejszości, itp. dają się zdefiniować za pomocą przyjętych terminów pierwotnych i podanych aksjomatów.

Stwierdzenie 1.1. *Dla dowolnego $n \in \mathbb{N}$: $n \neq n^*$.*

Dowód. Niech $A = \{m \in \mathbb{N} \ : \ m \neq m^*\}$. Z Aksjomatu 1 mamy, że $1 \in \mathbb{N}$, zaś z Aksjomatu 2 wynika, że $1 \neq 1^*$. Wobec tego $1 \in A$. Weźmy dowolne $n \in \mathbb{N}$ takie, że $n \in A$. Wtedy $n \neq n^*$. Z Aksjomatu 3, $n^* \in \mathbb{N}$. Jeśli $n^* = (n^*)^*$, to na mocy Aksjomatu 4, $n = n^*$, wbrew założeniu. Zatem $n^* \neq (n^*)^*$, ale dodatkowo $n^* \in \mathbb{N}$, więc $n^* \in A$. Wobec tego zbiór A spełnia wszystkie założenia Aksjomatu 5 i w konsekwencji, $A = \mathbb{N}$, co oznacza, że $n \neq n^*$ dla każdego $n \in \mathbb{N}$. □

Stwierdzenie 1.2. *Dla dowolnego $n \in \mathbb{N} \setminus \{1\}$ istnieje dokładnie jedno $m \in \mathbb{N}$ takie, że $n = m^*$.*

Dowód. Niech $A = \{1\} \cup B$, gdzie $B = \{n \in \mathbb{N} \ : \ n = m^*$ dla pewnego $m \in \mathbb{N}\}$. Wówczas na mocy Aksjomatu 2, $1 \notin B$. Ponadto $1 \in A$. Niech n będzie taką liczbą naturalną, że $n \in A$. Wtedy $n^* \in \mathbb{N}$ i $n^* = m^*$ dla $m = n$, więc $n^* \in B$, skąd $n^* \in A$. Wobec tego zbiór A spełnia wszystkie założenia Aksjomatu 5 i w konsekwencji, $A = \mathbb{N}$. Weźmy dowolne $n \in \mathbb{N} \setminus \{1\}$. Wtedy $n \in B$, więc $n = m^*$ dla pewnego $m \in \mathbb{N}$. Jeśli $n = k^*$ dla pewnego $k \in \mathbb{N}$, to $m^* = k^*$, więc z Aksjomatu 4, $k = m$. Zatem dla każdego $n \in \mathbb{N} \setminus \{1\}$ istnieje dokładnie jedno $m \in \mathbb{N}$ takie, że $n = m^*$. □

Dodawanie liczb naturalnych określamy przy pomocy formuł:

$$n + 1 = n^* \ \text{ dla każdego } n \in \mathbb{N}, \tag{1.1}$$

$$n + m^* = (n + m)^* \ \text{ dla dowolnych } m, n \in \mathbb{N}. \tag{1.2}$$

Przykład 1.3. Opierając się na wzorach (1.1)-(1.2) obliczymy $2 + 2$. Ze wzoru (1.1): $2 + 1 = 2^* = 3$. Ze wzoru (1.2): $2 + 2 = 2 + 1^* = (2 + 1)^* = 3^* = 4$. Zatem $2 + 2 = 4$.

Obliczmy teraz $2 + 3$ oraz $3 + 2$. Ze wzoru (1.2), $2 + 3 = 2 + 2^* = = (2 + 2)^* = 4^* = 5$ i $3 + 2 = 3 + 1^* = (3 + 1)^*$, ale ze wzoru (1.1), $3 + 1 = 3^* = 4$, więc $3 + 2 = 4^* = 5$. Widzimy stąd, że pokazanie równości: $2 + 3 = 3 + 2$ nie było wcale takie proste!

Ćwiczenie 1.4. Opierając się na wzorach (1.1)-(1.2) oblicz $4 + 5$ oraz $5 + 4$.

Wykażemy, że dla każdej pary (a, b) liczb naturalnych jest zdefiniowana w ten sposób jednoznacznie suma $a + b$. Niech n będzie dowolną liczbą naturalną i niech A będzie zbiorem tych liczb naturalnych m, że suma $n + m$ jest jednoznacznie zdefiniowana. Z (1.1) i z Aksjomatu 3 wynika, że $1 \in A$. Niech teraz m będzie taką liczbą naturalną, że $n+m$ jest zdefiniowane jednoznacznie. Wtedy ze wzoru (1.2): $n+m^* = (n+m)^*$, więc na mocy Aksjomatu 3 suma $n+m^*$ jest zdefiniowana jednoznacznie. Zatem $m^* \in A$ i na mocy Aksjomatu 5, $A = \mathbb{N}$, co oznacza, że dla każdej pary (a, b) liczb naturalnych zdefiniowana jest w ten sposób jednoznacznie suma $a + b$.

Przykład 1.5. Pokażemy, że $n + m \neq 1$ dla dowolnych $m, n \in \mathbb{N}$. Załóżmy, że tak nie jest. Wtedy istnieją $n, m \in \mathbb{N}$ takie, że $n + m = 1$. Jeśli $m = 1$, to ze wzoru (1.1), $1 = n^*$, co przeczy Aksjomatowi 2. Jeśli zaś $m \neq 1$, to ze stwierdzenia 1.2, $m = k^*$ dla pewnego $k \in \mathbb{N}$ i wtedy ze wzoru (1.2), $1 = (n + k)^*$, wbrew Aksjomatowi 2. Przypuszczenie, że $1 = n + m$ dla pewnych $n, m \in \mathbb{N}$ doprowadziło nas do sprzeczności. Zatem $n + m \neq 1$ dla dowolnych $m, n \in \mathbb{N}$.

Stwierdzenie 1.6. *Dodawanie liczb naturalnych jest łączne, to znaczy dla dowolnych $k, m, n \in \mathbb{N}$:*

$$(k + m) + n = k + (m + n).$$

Dowód. Weźmy dowolne ustalone $k, m \in \mathbb{N}$ i niech A będzie zbiorem wszystkich liczb naturalnych n takich, że $(k + m) + n = k + (m + n)$. Ze wzoru (1.1): $(k + m) + 1 = (k + m)^*$ oraz $m + 1 = m^*$. Stąd i ze wzoru (1.2), $k + (m + 1) = k + m^* = (k + m)^*$. Wobec tego $1 \in A$. Niech teraz n będzie dowolną liczbą naturalną taką, że $n \in A$. Wtedy $(k + m) + n = k + (m + n)$. Stąd i ze wzoru (1.2), $(k + m) + n^* = [(k+m)+n]^* = [k+(m+n)]^*$ oraz $m+n^* = (n+m)^*$ i $k+(m+n^*) = k+(m+n)^* = [k+(m+n)]^*$. Wobec tego $n^* \in A$ i na mocy Aksjomatu 5, $A = \mathbb{N}$, co oznacza, że $(k + m) + n = k + (m + n)$ dla dowolnych $k, m, n \in \mathbb{N}$. □

Stwierdzenie 1.7. *Dodawanie liczb naturalnych jest przemienne, to znaczy dla dowolnych $m, n \in \mathbb{N}$:*

$$m + n = n + m.$$

Dowód. Niech $A = \{n \in \mathbb{N} : n+1 = 1+n\}$. Wtedy oczywiście $1 \in A$. Jeśli zaś pewna liczba naturalna n należy do A, to $n+1 = 1+n$. Stąd i na mocy wzorów (1.1) i (1.2): $1+n^* = (1+n)^* = (n+1)^* = (n^*)^* = n^*+1$. Zatem $n^* \in A$. Wobec tego na mocy Aksjomatu 5, $A = \mathbb{N}$, co oznacza, że $n+1 = 1+n$ dla każdego $n \in \mathbb{N}$.

Weźmy teraz dowolne $m \in \mathbb{N}$ i niech $B = \{n \in \mathbb{N} : m+n = n+m\}$. Wówczas z pierwszej części dowodu $1 \in B$. Weźmy dowolną liczbę naturalną n należącą do zbioru B. Wtedy $m+n = n+m$, więc ze wzoru (1.2) i ze stwierdzenia 1.6, $m+n^* = (m+n)^* = (n+m)^*$ oraz $n^*+m = (n+1)+m = n+(1+m) = n+(m+1) = n+m^* = (n+m)^*$, skąd $n^* \in B$. Wobec tego z Aksjomatu 5, $B = \mathbb{N}$, co oznacza, że $n+m = m+n$ dla wszystkich $m, n \in \mathbb{N}$. □

Stwierdzenie 1.8. *Dla dowolnych liczb naturalnych k, m, n:*

$$k+n = m+n \Rightarrow k = m.$$

Dowód. Ustalmy dowolne $k, m \in \mathbb{N}$ i niech A będzie zbiorem wszystkich liczb naturalnych n, dla których prawdziwa jest implikacja: $k+n = m+n \Rightarrow k = m$. Jeśli $k+1 = m+1$, to ze wzoru (1.1), $k^* = m^*$, więc z Aksjomatu 4, $k = m$. Zatem $1 \in A$. Weźmy dowolną liczbę naturalną n taką, że $n \in A$ i niech $k+n^* = m+n^*$. Wtedy ze wzoru (1.2), $(k+n)^* = (m+n)^*$, więc z Aksjomatu 4, $k+n = m+n$, ale $n \in A$, więc stąd $k = m$, czyli $n^* \in A$. Na mocy Aksjomatu 5, $A = \mathbb{N}$, co kończy nasz dowód. □

Mnożenie liczb naturalnych określamy za pomocą dodawania liczb naturalnych i formuł:

$$1 \cdot n = n \text{ dla każdego } n \in \mathbb{N}, \tag{1.3}$$

$$m^* \cdot n = m \cdot n + n \text{ dla dowolnych } m, n \in \mathbb{N}. \tag{1.4}$$

Wzór (1.4) w ujęciu intuicyjnym oznacza, że tak jak w dydaktyce szkolnej:

$$m \cdot n = \underbrace{n+n+\ldots+n}_{m}.$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Przykład 1.9. Ze wzorów (1.3)-(1.4) i z przykładu 1.3 mamy, że $2 \cdot 2 = 1^* \cdot 2 = 1 \cdot 2 + 2 = 2 + 2 = 4$. Zatem na mocy wzorów (1.4), (1.2) i (1.3), $3 \cdot 2 = 2^* \cdot 2 = 2 \cdot 2 + 2 = 4 + 2 = 4 + 1^* = (4 + 1)^* = 5^* = 6$ oraz $2 \cdot 3 = 1^* \cdot 3 = 1 \cdot 3 + 3 = 3 + 3 = 3 + 2^* = (3 + 2)^* = 5^* = 6$ na mocy przykładu 1.3.

Ćwiczenie 1.10. Opierając się na wzorach (1.1)-(1.2) i (1.3)-(1.4) oblicz $4 \cdot 5$ i $5 \cdot 4$.

Stwierdzenie 1.11. *Mnożenie liczb naturalnych jest rozdzielne względem dodawania, to znaczy dla dowolnych $k, m, n \in \mathbb{N}$:*

$$n \cdot (k + m) = n \cdot k + n \cdot m \text{ oraz } (k + m) \cdot n = k \cdot n + m \cdot n.$$

Dowód. Ustalmy dowolne $k, m \in \mathbb{N}$ i niech A będzie zbiorem wszystkich liczb naturalnych n takich, że $n \cdot (k+m) = n \cdot k + n \cdot m$. Ze wzoru (1.3), $1 \cdot (k + m) = k + l = 1 \cdot k + 1 \cdot m$, więc $1 \in A$. Niech n będzie taką liczbą naturalną, że $n \in A$, to znaczy $n \cdot (k + m) = n \cdot k + n \cdot m$. Wtedy ze wzoru (1.4) , $n^* \cdot (k + m) = n \cdot (k + m) + (k + m)$ oraz $n^* \cdot k + n^* \cdot m = (n \cdot k + k) + (n \cdot m + m)$, więc z udowodnionych własności dodawania liczb naturalnych, $n^* \cdot (k + m) = n^* \cdot k + n^* \cdot m$, co oznacza, że $n^* \in A$. Wobec tego z Aksjomatu 5, $A = \mathbb{N}$, co oznacza, że $n \cdot (k + m) = n \cdot k + n \cdot m$ dla dowolnych $k, m, n \in \mathbb{N}$.

Ustalmy dowolne $m, n \in \mathbb{N}$ i niech B będzie zbiorem wszystkich liczb naturalnych k takich, że $(k+m) \cdot n = k \cdot n + m \cdot n$. Z udowodnionych praw wynika, że $(1 + m) \cdot n = m^* \cdot n = m \cdot n + n = 1 \cdot n + m \cdot n$, co oznacza, że $1 \in B$. Niech k będzie taką liczbą naturalną, że $k \in B$. Wtedy $(k + m) \cdot n = k \cdot n + m \cdot n$. Z udowodnionych praw wynika, że $(k^* + m) \cdot n = (m + k^*) \cdot n = (m + k)^* \cdot n = (k + m)^* \cdot n = (k + m) \cdot n + n$, więc $(k^* + m) \cdot n = k \cdot n + m \cdot n + n = (k \cdot n + n) + m \cdot n = k^* \cdot n + m \cdot n$. Zatem $k^* \in B$ i na mocy Aksjomatu 5, $B = \mathbb{N}$, czyli $(k + m) \cdot n = k \cdot n + m \cdot n$ dla dowolnych $k, m, n \in \mathbb{N}$. □

Stwierdzenie 1.12. *Mnożenie liczb naturalnych jest łączne, to znaczy dla dowolnych $k, m, n \in \mathbb{N}$:*

$$(n \cdot m) \cdot k = n \cdot (m \cdot k).$$

Dowód. Ustalmy dowolne $k, m \in \mathbb{N}$ i niech A będzie zbiorem wszystkich liczb naturalnych k takich, że $(n \cdot m) \cdot k = n \cdot (m \cdot k)$. Ze wzoru (1.3) mamy, że $(1 \cdot m) \cdot k = m \cdot k = 1 \cdot (m \cdot k)$, co oznacza, że $1 \in A$. Niech n będzie taką liczbą naturalną, że $n \in A$, to znaczy $(n \cdot m) \cdot k = n \cdot (m \cdot k)$. Wtedy ze wzoru (1.4) i ze stwierdzenia 1.11: $(n^* \cdot m) \cdot k = (n \cdot m + m) \cdot k = (n \cdot m) \cdot k + m \cdot k = n \cdot (m \cdot k) + m \cdot k = n^* \cdot (m \cdot k)$, co oznacza, że $n^* \in A$. Zatem z Aksjomatu 5, $A = \mathbb{N}$ i $(n \cdot m) \cdot k = n \cdot (m \cdot k)$ dla dowolnych $k, m, n \in \mathbb{N}$. □

Stwierdzenie 1.13. *Mnożenie liczb naturalnych jest przemienne, to znaczy dla dowolnych $m, n \in \mathbb{N}$:*

$$m \cdot n = n \cdot m.$$

Dowód. Niech B będzie zbiorem wszystkich liczb naturalnych n takich, że $n \cdot 1 = 1 \cdot n$. Stąd $1 \in B$. Niech n będzie taką liczbą naturalną, że $n \in B$. Wtedy $n \cdot 1 = 1 \cdot n$, więc stąd i ze stwierdzenia 1.11 oraz z (1.3), $n^* \cdot 1 = (n + 1) \cdot 1 = n \cdot 1 + 1 = 1 \cdot n + 1 = n + 1 = n^* = 1 \cdot n^*$, czyli $n^* \in B$. Zatem na mocy Aksjomatu 5, $B = \mathbb{N}$, co oznacza wobec (1.3), że $n \cdot 1 = 1 \cdot n = n$ dla każdego $n \in \mathbb{N}$.

Ustalmy teraz dowolne $n \in \mathbb{N}$ i niech A oznacza zbiór wszystkich liczb naturalnych m takich, że $m \cdot n = n \cdot m$. Z pierwszej części dowodu $1 \in A$. Niech m będzie taką liczbą naturalną, że $m \in A$. Wtedy $m \cdot n = n \cdot m$, więc stąd oraz ze stwierdzenia 1.9, z (1.4) i z równości $n = n \cdot 1$: $m^* \cdot n = m \cdot n + n = n \cdot m + n \cdot 1 = n \cdot (m + 1) = n \cdot m^*$. Zatem $m^* \in A$ i z Aksjomatu 5, $A = \mathbb{N}$. Oznacza to, że $n \cdot m = m \cdot n$ dla dowolnych $m, n \in \mathbb{N}$. □

Stwierdzenie 1.14. *Dla dowolnych liczb naturalnych k, m, n:*

$$k \cdot n = m \cdot n \Rightarrow k = m.$$

Dowód. Oznaczmy przez A zbiór wszystkich liczb naturalnych n takich, że dla dowolnych $k, m \in \mathbb{N}$ zachodzi implikacja: $k \cdot n = m \cdot n \Rightarrow k = m$. Ze stwierdzenia 1.13 i ze wzoru (1.3) wynika, że $1 \in A$. Weźmy dowolną liczbę naturalną n taką, że $n \in A$. Niech $k, m \in \mathbb{N}$ będą takie, że $k \cdot n^* = m \cdot n^*$. Wtedy ze wzoru (1.4), $k \cdot n + n = m \cdot n + n$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zatem na mocy stwierdzenia 1.8, $k \cdot n = m \cdot n$, ale $n \in A$, więc $k = m$. Oznacza to, że $n^* \in A$. Wobec tego $A = \mathbb{N}$ na mocy Aksjomatu 5, co kończy dowód. □

Relację mniejszości $<$ w zbiorze liczb naturalnych określamy za pomocą formuły:

$$m < n \iff (n = m + k \text{ dla pewnego } k \in \mathbb{N}). \tag{1.5}$$

Stwierdzenie 1.15. *Relacja $<$ jest przechodnia, to znaczy dla dowolnych $k, m, n \in \mathbb{N}$:*

$$(k < m \text{ i } m < n) \Rightarrow k < n.$$

Dowód. Z naszych założeń i z (1.5) wynika, że $m = k + t$ i $n = m + s$ dla pewnych $s, t \in \mathbb{N}$. Stąd i na mocy stwierdzenia 1.6, $n = k + (t + s)$, a ponieważ $t + s \in \mathbb{N}$, więc na mocy (1.5), $k < n$. □

Stwierdzenie 1.16. *Dla każdego $n \in \mathbb{N} \setminus \{1\}$: $1 < n$.*

Dowód. Niech $n \in \mathbb{N} \setminus \{1\}$. Wtedy ze stwierdzenia 1.2, $n = m^*$ dla pewnego $m \in \mathbb{N}$. Stąd i na mocy stwierdzenia 1.7, $n = m + 1 = 1 + m$, więc na mocy (1.5), $1 < n$. □

Stwierdzenie 1.17. *Dla każdego $n \in \mathbb{N}$: $\sim (n < n)$.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje $n \in \mathbb{N}$ takie, że $n < n$. Zatem $n = n + k$ dla pewnego $k \in \mathbb{N}$, skąd $1 + n = (k + 1) + n$ i na mocy stwierdzenia 1.8, $1 = k + 1$. Zatem $1 = k^*$, wbrew Aksjomatowi 2. Wobec tego nie jest prawdą, że $n < n$. □

Stwierdzenie 1.18. *Dla dowolnych liczb naturalnych m, n:*

$$m < n \Rightarrow (m + k < n + k \text{ dla każdego } k \in \mathbb{N}).$$

Dowód. Z założenia $n = m + t$ dla pewnego $t \in \mathbb{N}$, więc dla każdego $k \in \mathbb{N}$ mamy, że $n + k = (m + k) + t$, skąd $m + k < n + k$. □

Stwierdzenie 1.19. *Dla dowolnych liczb naturalnych k, m, n:*

$$m + k < n + k \Rightarrow m < n.$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Z założenia $n + k = (m + k) + t$ dla pewnego $t \in \mathbb{N}$. Stąd $n + k = (m + t) + k$, więc na mocy stwierdzenia 1.8, $n = m + t$, skąd $m < n$. □

Stwierdzenie 1.20. *Dla każdego $n \in \mathbb{N}$ nie istnieje $m \in \mathbb{N}$ takie, że $n < m < n + 1$.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieją liczby naturalne m, n takie, że $n < m < n + 1$. Stąd $m = n + k$ dla pewnego $k \in \mathbb{N}$ i $n + k < n + 1$, więc ze stwierdzenia 1.19, $k < 1$. Zatem $1 = k + s$ dla pewnego $s \in \mathbb{N}$, co przeczy przykładowi 1.5. □

Stwierdzenie 1.21. *Dla dowolnych liczb naturalnych m, n zachodzi jeden i tylko jeden spośród następujących przypadków:*
(1) $m = n$, (2) $m < n$, (3) $n < m$.

Dowód. Jeśli zachodzą jednocześnie przypadki (1) i (2), to $n < n$, co przeczy stwierdzeniu 1.17. Jeśli zachodzą jednocześnie przypadki (1) i (3), to $n < n$, co przeczy stwierdzeniu 1.17. Jeśli zachodzą jednocześnie przypadki (2) i (3), to ze stwierdzenia 1.15, $m < m$, co przeczy stwierdzeniu 1.17. Wobec tego dla dowolnych liczb naturalnych m, n może zajść co najwyżej jeden z przypadków (1)-(3).

Niech teraz m będzie dowolną ustaloną liczbą naturalną. Oznaczmy przez A zbiór wszystkich liczb naturalnych n takich, że $n = m$ lub $n < m$ lub $m < n$. Wtedy $m \in A$. Jeśli $1 = m$, to $1 \in A$, a jeśli $1 \neq m$, to ze stwierdzenia 1.15, $1 < m$, więc wtedy także $1 \in A$. Wobec tego $1 \in A$. Niech n będzie taką liczbą naturalną, że $n \in A$. Wtedy $n = m$ lub $n < m$ lub $m < n$. Jeśli $n = m$, to $n^* = m + 1$, więc $m < n^*$, skąd $n^* \in A$. Jeśli $n < m$, to $m = n + k$ dla pewnego $k \in \mathbb{N}$, więc dla $k = 1$, $m = n^*$ i wtedy $n^* \in A$ lub $k \neq 1$ i wtedy ze stwierdzenia 1.2, $k = s^*$ dla pewnego $s \in \mathbb{N}$, skąd $m = (n+1)+s = n^*+s$, a zatem $n^* < m$ i też $n^* \in A$. W końcu, jeśli $m < n$, to $n = m + t$ dla pewnego $t \in \mathbb{N}$, więc $n^* = n + 1 = m + (t + 1)$, czyli $m < n^*$ i także $n^* \in A$. Wobec tego na mocy Aksjomatu 5, $A = \mathbb{N}$ i nasze stwierdzenie jest udowodnione. □

W zbiorze liczb naturalnych używa się też relacji większości $>$ określając ją dla dowolnych $m, n \in \mathbb{N}$ wzorem:

$$m > n \iff n < m. \tag{1.6}$$

W zbiorze liczb naturalnych używamy też relacji $\leqslant$ i $\geqslant$ określając je dla dowolnych $m, n \in \mathbb{N}$ formułami:

$$m \leqslant n \iff (m < n \ \vee \ m = n), \tag{1.7}$$

$$m \geqslant n \iff (n < m \ \vee \ n = m). \tag{1.8}$$

Zauważmy, że dla każdej liczby naturalnej n jest $n \leqslant n$, gdyż zdanie $n = n$ jest prawdziwe, a więc także alternatywa $(n < n \ \vee n = n)$ jest zdaniem prawdziwym!

Ze stwierdzenia 1.21 wynika w prosty sposób następujące

Stwierdzenie 1.22. *Dla dowolnych liczb naturalnych m, n:*
(i) $m \leqslant n$ lub $n \leqslant m$,
(ii) jeżeli $m \leqslant n$ i $n \leqslant m$, to $m = n$.

Stwierdzenie 1.23. *Dla dowolnych liczb naturalnych m, n:*

$$m < n \Rightarrow (m \cdot k < n \cdot k \ \text{ dla każdego } k \in \mathbb{N}).$$

Dowód. Z założenia $n = m + t$ dla pewnego $t \in \mathbb{N}$. Stąd dla dowolnego $k \in \mathbb{N}$ na mocy rozdzielności mnożenia względem dodawania, $n \cdot k = m \cdot k + t \cdot k$, ale $t \cdot k \in \mathbb{N}$, więc $m \cdot k < n \cdot k$. □

Stwierdzenie 1.24. *Dla dowolnych liczb naturalnych k, m, n:*

$$m \cdot k < n \cdot k \Rightarrow m < n.$$

Dowód. Załóżmy, że $m \cdot k < n \cdot k$. Wtedy ze stwierdzenia 1.21 mamy, że $m = n$ lub $n < m$ lub $m < n$. Jeśli $m = n$, to $m \cdot k = n \cdot k$ i mamy sprzeczność. Jeśli $n < m$, to ze stwierdzenia 1.21, $n \cdot k < m \cdot k$ i też mamy sprzeczność. Zatem $m < n$. □

Stwierdzenie 1.25. *Dla dowolnych liczb naturalnych m, n:*

$$n > m \Rightarrow n \geqslant m + 1.$$

Dowód. Z założenia $n = m + k$ dla pewnego $k \in \mathbb{N}$. Jeśli $k = 1$ to $n = m + 1$, a jeśli $k \neq 1$, to ze stwierdzenia 1.2 istnieje $t \in \mathbb{N}$ takie, że $k = t^* = t + 1$ i wtedy, $n = (m + 1) + t$, skąd $n > m + 1$. Z tych rozważań mamy zatem, że zawsze $n \geqslant m + 1$. □

1.3 Trzy ważne zasady

Twierdzenie 1.26. (zasada minimum). *W każdym niepustym podzbiorze zbioru liczb naturalnych istnieje liczba najmniejsza, czyli mniejsza lub równa od każdej liczby należącej do tego zbioru.*

Dowód. Niech X będzie niepustym podzbiorem zbioru $\mathbb{N}$ i załóżmy, że w zbiorze X nie ma elementu najmniejszego. Niech A będzie zbiorem liczb naturalnych n takich, że każda liczba naturalna $m \leqslant n$ nie należy do zbioru X. Jeśli $m \in \mathbb{N}$ i $m \leqslant 1$, to ze stwierdzenia 1.16, $m = 1$ i jeśli $1 \in X$, to zgodnie ze stwierdzeniem 1.16, 1 jest najmniejszą liczbą w zbiorze X, wbrew założeniu. Wobec tego $1 \notin X$ i $1 \in A$. Niech n będzie taką liczbą naturalną, że $n \in A$. Wówczas każda liczba naturalna $m \leqslant n$ nie należy do X. W szczególności $n \notin X$. Załóżmy, że $n^* \in X$. Weźmy dowolne $x \in X$. Wtedy nie jest prawdą, że $x \leqslant n$, więc na mocy stwierdzenia 1.21, $x > n$, skąd na mocy stwierdzenia 1.25, $x \geqslant n + 1 = n^*$. Stąd n^* jest najmniejszą liczbą w zbiorze X, wbrew założeniu. Wobec tego $n^* \notin X$ i w konsekwencji $n^* \in A$. Wobec tego na mocy Aksjomatu 5, $A = \mathbb{N}$. Oznacza to, że do X nie należy żadna liczba naturalna, czyli $X = \emptyset$.

Przypuszczenie, że podzbiór X nie posiada liczby najmniejszej doprowadziło nas zatem do sprzeczności. Wobec tego X posiada element najmniejszy. □

Definicja 1.27. Niech X będzie niepustym podzbiorem zbioru $\mathbb{N}$. Mówimy, że zbiór X jest **ograniczony z góry**, jeżeli istnieje $a \in \mathbb{N}$ takie, że $x \leqslant a$ dla wszystkich $x \in X$.

Twierdzenie 1.28. (zasada maksimum). *W każdym niepustym ograniczonym z góry podzbiorze zbioru liczb naturalnych istnieje liczba największa, czyli liczba większa lub równa od każdej liczby z tego podzbioru.*

Dowód. Niech X będzie niepustym i ograniczonym z góry podzbiorem zbioru $\mathbb{N}$. Wtedy istnieje $c \in \mathbb{N}$ takie, że $x \leqslant c$ dla każdego $x \in X$. Niech A będzie zbiorem wszystkich liczb naturalnych a takich, że $x \leqslant a$ dla wszystkich $x \in X$. Wtedy $c \in A$, więc zbiór A jest niepusty. Zatem

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

z Zasady minimum istnieje w A liczba najmniejsza s. Stąd $x \leqslant s$ dla wszystkich $x \in X$ oraz $s \leqslant a$ dla wszystkich $a \in A$. Jeśli $s \notin X$, to $x < s$ dla wszystkich $x \in X$, skąd $s \neq 1$ i na mocy stwierdzenia 1.24, $x + 1 \leqslant s$, ale ze stwierdzenia 1.2, $s = k + 1$ dla pewnego $k \in \mathbb{N}$, więc $x + 1 \leqslant k + 1$, skąd na mocy Stwierdzeń 1.8 i 1.19, $x \leqslant k$ dla wszystkich $x \in X$. Zatem z definicji zbioru A jest $k \in A$, ale $k < s$ i s jest najmniejszą liczbą zbioru A, więc mamy sprzeczność. Wobec tego $s \in X$ i w konsekwencji s jest największą liczbą zbioru X. □

W zbiorze liczb naturalnych można też zdefiniować ograniczone **odejmowanie**. Mianowicie, jeśli $m, n \in \mathbb{N}$ i $n > m$, to $n = m + k$ dla pewnego $k \in \mathbb{N}$, przy czym to k jest dokładnie jedno na mocy stwierdzenia 1.8. Wówczas przyjmujemy, że $n - m = k$. Na przykład $9 - 4 = 5$, bo $9 = 4 + 5$. Wobec tego $n - m = k \iff n = m + k$. Używając ograniczonego odejmowania możemy inaczej zapisywać udowodnione wcześniej rezultaty. Na przykład stwierdzenie 1.2 można sformułować tak: „Dla każdej liczby naturalnej $n \neq 1$ liczba $n - 1 \in \mathbb{N}$".

Od tej pory dla liczb naturalnych n będziemy pisali $n+1$ w miejsce n^* i nie będziemy używali symbolu n^*. Ponadto Aksjomat 5 będziemy dalej nazywali Zasadą indukcji zupełnej. Ze względu na dużą użyteczność tej Zasady sformułujemy ją jeszcze raz, w nowej, nieco ogólniejszej postaci.

Twierdzenie 1.29. (zasada indukcji matematycznej). *Niech $n_0 \in \mathbb{N}$ i $A \subseteq \mathbb{N}$. Jeżeli spełnione są warunki:*

1° *$n_0 \in A$ oraz*

2° *dla każdej liczby naturalnej $n \geqslant n_0$ prawdziwa jest implikacja: $n \in A \Rightarrow n + 1 \in A$,*

to z 1° i 2° wynika, że każda liczba naturalna $n \geqslant n_0$ należy do A.

Dowód. Przypuśćmy, że tak nie jest. Wtedy na mocy zasady minimum istnieje najmniejsza liczba naturalna $m \geqslant n_0$ taka, że $m \notin A$. Z 1° wynika, że $m \neq n_0$, ale $m \geqslant n_0$, więc $m > n_0$. Zatem na mocy stwierdzenia 1.25, $m - 1 \geqslant n_0$ i $m - 1 \in \mathbb{N}$. Z minimalności m i tego, że $m - 1 < m$ otrzymujemy, że $m - 1 \in A$. Stąd i na mocy 2° zastosowanego dla $n = m - 1$ uzyskujemy, że $(m - 1) + 1 \in A$, czyli $m \in A$ i mamy sprzeczność.

Przypuszczenie, że nasze twierdzenie jest fałszywe doprowadziło nas do sprzeczności. Wobec tego nasze twierdzenie jest prawdziwe. □

Przykład 1.30. Udowodnimy za pomocą indukcji matematycznej, że dla każdej liczby naturalnej $n \geqslant 3$ zachodzi nierówność:

$$2^n \geqslant 2n + 2. \tag{1.9}$$

Tutaj $n_0 = 3$ i A jest zbiorem wszystkich liczb naturalnych n takich, że $2^n \geqslant 2n + 2$.

1° Sprawdzamy, czy $3 \in A$? $2^3 = 8$ i $2 \cdot 3 + 2 = 8$, więc $2^3 \geqslant 2 \cdot 3 + 2$, skąd $3 \in A$.

2° Założenie indukcyjne: nierówność (1.9) zachodzi dla pewnej liczby naturalnej $n \geqslant 3$.

Teza indukcyjna: nierówność (1.9) zachodzi dla liczby $n + 1$, to znaczy $2^{n+1} \geqslant 2(n + 1) + 1$.

Dowód tezy indukcyjnej: Ponieważ $2^n \geqslant 2n + 2$ na mocy założenia indukcyjnego, więc po pomnożeniu tej nierówności przez 2 otrzymujemy, że $2^{n+1} \geqslant 4n + 4 = 2(n + 1) + 2 + 2n \geqslant 2(n + 1) + 2$, czyli $2^{n+1} \geqslant 2(n + 1) + 2$, co należało udowodnić.

Z 1° i 2° na mocy zasady indukcji zupełnej nierówność (1.9) zachodzi dla każdej liczby naturalnej $n \geqslant 3$.

Uwaga 1.31. Warto wspomnieć, że istnieją inne niż aksjomatyka Peano aksjomatyki liczb naturalnych. Mianowicie, można zbudować aksjomatykę opartą na zasadzie minimum i wykazać, że w niej zachodzi zasada indukcji oraz zasada maksimum. Można też skonstruować aksjomatykę liczb naturalnych opartą na zasadzie maksimum i wykazać, że w niej zachodzi zasada minimum i zasada indukcji. Wobec tego mówimy, że zasada indukcji, zasada minimum i zasada maksimum w zbiorze liczb naturalnych są ze sobą równoważne. Przykłady takich systemów aksjomatycznych można znaleźć na przykład w [12].

Ćwiczenie 1.32. Udowodnij za pomocą indukcji matematycznej, że dla każdej liczby naturalnej n zachodzą wzory:

$$1 + 2 + \ldots + n = \frac{n(n + 1)}{2}, \tag{1.10}$$

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}, \tag{1.11}$$

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4}. \tag{1.12}$$

Ćwiczenie 1.33. Udowodnij za pomocą indukcji matematycznej, że $2^n \geqslant n^2$ dla każdej liczby naturalnej $n \geqslant 4$.

Ćwiczenie 1.34. Wyznacz wszystkie liczby naturalne n takie, że $3^n \leqslant n^4$.

Ćwiczenie 1.35. Udowodnij za pomocą indukcji matematycznej, że dla każdej liczby naturalnej n zachodzą wzory:

$$(n+1) \cdot (n+2) \cdot \ldots \cdot (n+n) = 2^n \cdot 1 \cdot 3 \cdot \ldots \cdot (2n-1). \tag{1.13}$$

$$1 \cdot 2 + 2 \cdot 5 + \cdots n \cdot (3n-1) = n^2(n+1). \tag{1.14}$$

Ćwiczenie 1.36. Jaka jest maksymalna liczba regionów, na jaką można podzielić płaszczyznę n prostymi?

Ćwiczenie 1.37. Czy istnieją liczby naturalne m, n, t takie, że $m^6 + 2n^6 = 4t^6$?

Ćwiczenie 1.38. Niech n będzie dowolną liczbą naturalną. Udowodnij, że przedział $[n, 2n]$ zawiera pewną potęgę liczby 2.

Ćwiczenie 1.39. Udowodnij za pomocą indukcji matematycznej, że dla każdej liczby naturalnej $n > 1$ zachodzi nierówność:

$$1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1) < n^n. \tag{1.15}$$

Rozdział 2

Liczby całkowite

Najpierw zostaną przedstawione niezbyt formalnie idee związane z prezentowaną dalej konstrukcją pierścienia liczb całkowitych. W zbiorze liczb naturalnych $\mathbb{N}$ nie jest wykonalne odejmowanie (na przykład nie istnieje $1-2$). W związku z tym powstaje naturalny problem: jak powiększyć zbiór $\mathbb{N}$ za pomocą zbioru X rozłącznego z $\mathbb{N}$ do zbioru $\mathbb{N} \cup X$, w którym wykonalne będzie odejmowanie? Chodzi też o to aby w nowym zbiorze było określone dodawanie i mnożenie, które mają te same własności, co dodawanie i mnożenie liczb naturalnych, to znaczy aby dodawanie i mnożenie były przemienne, łączne, posiadały elementy neutralne oraz aby mnożenie było rozdzielne względem dodawania. Zależy nam także na tym, aby nowe dodawanie pokrywało się na zbiorze $\mathbb{N}$ z naturalnym dodawaniem i aby nowe mnożenie pokrywało się na zbiorze $\mathbb{N}$ z naturalnym mnożeniem. Pożądane jest też znalezienie minimalnego zbioru X, który spełnia te wszystkie warunki. Dobrym kandydatem wydaje się być $X = \{0\} \cup \{-n \ : \ n \in \mathbb{N}\}$. Przyjęte założenia implikują wiele zależności, które muszą być spełnione w zbiorze $\mathbb{N} \cup X$. Na przykład $1-2 = 2-3 = 3-4 = \ldots$, bo $1+3 = 2+2$ oraz $2+4 = 3+3$, i tak dalej. Ponadto $a + (1-1) = (a+1) - 1 = a$ dla $a \in \mathbb{N}$ oraz $1-1 = 2-2 = 3-3 = \ldots$. W takim razie $0 = 1-1 = 2-2 = 3-3 = \ldots$. Dalej, dla $a, b, c, d \in \mathbb{N}$: $a - b = c - d \iff a + d = c + b$, $(a-b)\cdot(c-d) = (ac+bd)-(ad+bc)$, $a-b < c-d \iff a+d < c+b$.

Nasuwa to nam pomysł zastosowania zasady abstrakcji do formalnego uzasadnienia przedstawionych wyżej idei.

2.1 Liczby całkowite jako klasy abstrakcji relacji równoważności w zbiorze $\mathbb{N}\times\mathbb{N}$

W zbiorze $\mathbb{N}\times\mathbb{N}$ określamy relację R przyjmując, że dla dowolnych $a,b,c,d\in\mathbb{N}$:

$$(a,b)R(c,d) \iff a+d=c+b. \tag{2.1}$$

Stwierdzenie 2.1. *R jest relacją równoważności.*

Dowód. Ponieważ dla dowolnych $a,b\in\mathbb{N}$ jest $a+b=a+b$, więc z (2.1) mamy, że $(a,b)R(a,b)$, co oznacza, że relacja R jest zwrotna.

Weźmy dowolne $a,b,c,d\in\mathbb{N}$ takie, że $(a,b)R(c,d)$. Wtedy $a+d=$ $=c+b$, więc $c+b=a+d$ i z (2.1), $(c,d)R(a,b)$, czyli relacja R jest symetryczna.

Niech $a,b,c,d,r,s\in\mathbb{N}$ będą takie, że $(a,b)R(c,d)$ i $(c,d)R(r,s)$. Wtedy $a+d=c+b$ i $c+s=r+d$. Stąd po dodaniu stronami tych równości: $a+d+c+s=c+b+r+d$, więc po skróceniu: $a+s=r+b$, czyli na mocy (2.1), $(a,b)R(r,s)$. Wobec tego relacja R jest przechodnia.

W takim razie relacja R jest zwrotna, symetryczna i przechodnia, a więc R jest relacją równoważności. □

Klasy abstrakcji relacji R będziemy nazywali **liczbami całkowitymi**, zaś zbiór wszystkich liczb całkowitych będziemy oznaczali przez $\mathbb{Z}$. Idea jest taka, żeby klasa abstrakcji o reprezentancie (a,b) odpowiadała liczbie całkowitej $a-b$. Umówmy się, że klasę abstrakcji o reprezentancie (a,b) relacji R będziemy oznaczali symbolem $[a,b]$. Zatem dla dowolnych $m,n,x,y\in\mathbb{N}$:

$$(x,y)\in[m,n] \iff (x,y)R(m,n) \iff x+n=m+y. \tag{2.2}$$

Stwierdzenie 2.2. *Dla dowolnych $m,n\in\mathbb{N}$:*
(i) $[n,n]=[1,1]=\{(a,a)\ :\ a\in\mathbb{N}\}$,

(ii) jeśli $n > m$, *to* $[n, m] = [(n - m) + 1, 1] = \{((n - m) + a, a) : a \in \mathbb{N}\}$,

(iii) jeśli $n < m$, *to* $[n, m] = [1, (m - n) + 1] = \{(a, (m - n) + a) : a \in \mathbb{N}\}$.

Dowód. Weźmy dowolne $a, b \in \mathbb{N}$. Na mocy wzoru (2.2), $(a, b) \in [1, 1] \iff a + 1 = 1 + b \iff a = b$. Stąd $[1, 1] = \{(a, a) : a \in \mathbb{N}\}$ i dla $n \in \mathbb{N}$ jest $(n, n) \in [1, 1]$, więc z własności klas abstrakcji, $[n, n] = [1, 1]$, co dowodzi (i).

Niech $n > m$. Ze wzoru (2.2) otrzymujemy, że (a, b) należy do klasy $[(n - m) + 1, 1]$ wtedy i tylko wtedy, gdy $a + 1 = (n - m) + 1 + b$, co jest równoważne temu, że $a + m = n + b \iff a = (n - m) + b$, skąd $[(n-m)+1, 1] = \{((n-m)+b, b) : b \in \mathbb{N}\}$ i $(n, m) \in [(n-m)+1, 1]$, więc z własności klas abstrakcji mamy, że $[n, m] = [(n - m) + 1, 1]$, co dowodzi (ii).

Niech $n < m$. Na mocy wzoru (2.2), $(a, b) \in [1, (m - n) + 1]$ wtedy i tylko wtedy, gdy $a + (m - n) + 1 = 1 + b$, czyli gdy $a + m = n + b$, a zatem jedynie dla $b = a + (m - n)$, skąd uzyskujemy, że $[1, (m-n)+ +1] = \{(a, (m - n) + a : a \in \mathbb{N}\}$ i $(n, m) \in [1, (m - n) + 1]$, więc z własności klas abstrakcji $[n, m] = [1, (m-n)+1]$, co dowodzi (iii). □

Ze Stwierdzeń 2.2 i 1.21 uzyskujemy od razu następujące

Stwierdzenie 2.3. *Wszystkimi parami różnymi klasami abstrakcji relacji* R *są klasy:* $[1, 1] = \{(a, a) : a \in \mathbb{N}\}$, $[n + 1, 1] = \{(n + a, a) : a \in \mathbb{N}\}$ *dla* $n \in \mathbb{N}$ *oraz* $[1, n + 1] = \{(a, n + a) : a \in \mathbb{N}\}$ *dla* $n \in \mathbb{N}$.

Ćwiczenie 2.4. Wyznacz wszystkie pary (a, b) liczb naturalnych takie, że $[a, 3] = [6, b]$.

2.2 Określenie i własności dodawania liczb całkowitych

Dodawanie liczb całkowitych określamy przyjmując, że dla dowolnych $a, b, c, d \in \mathbb{N}$:

$$[a, b] + [c, d] = [a + c, b + d]. \tag{2.3}$$

Udowodnimy, że dodawanie liczb całkowitych nie zależy od wyboru reprezentantów klas abstrakcji, to znaczy jeżeli $(a,b)R(a',b')$ i $(c,d)R(c',d')$, to $(a+c,b+d)R(a'+c',b'+d')$. Rzeczywiście, z naszych założeń wynika, że $a+b'=a'+b$ i $c+d'=c'+d$, więc po dodaniu stronami: $a+b'+c+d'=a'+b+c'+d$, skąd $(a+c,b+d)R(a'+c',b'+d')$.

Klasę $[1,1]$ będziemy oznaczali symbolem 0. Zatem na mocy stwierdzenia 2.3,

$$0=[1,1]=\{(a,a)\ : a\in\mathbb{N}\}.$$

Stwierdzenie 2.5. *(i) Dla dowolnych $x,y\in\mathbb{Z}$: $x+y=y+x$ (to znaczy dodawanie liczb całkowitych jest przemienne),*

(ii) dla dowolnych $x,y,z\in\mathbb{Z}$: $x+(y+z)=(x+y)+z$ (to znaczy dodawanie liczb całkowitych jest łączne),

(iii) dla każdego $x\in\mathbb{Z}$: $x+0=0+x=x$ (to znaczy 0 jest elementem neutralnym dodawania liczb całkowitych),

(iv) dla każdego $x\in\mathbb{Z}$ istnieje $x'\in\mathbb{Z}$ takie, że $x+x'=x'+x=0$,

(v) dla dowolnych $x,y,z\in\mathbb{Z}$: $x+y=x+z\Rightarrow y=z$,

(vi) dla dowolnych $k,l\in\mathbb{N}$: $[k+1,1]+[l+1,1]=[(k+l)+1,1]$,

(vii) dla dowolnych $k,l\in\mathbb{N}$: $[1,k+1]+[1,l+1]=[1,(k+l)+1]$.

Dowód. Weźmy dowolne $x,y,z\in\mathbb{Z}$. Wtedy istnieją $a,b,c,d,r,s\in\mathbb{N}$ takie, że $x=[a,b]$, $y=[c,d]$ i $z=[r,s]$. Ze wzoru (2.3) i z przemienności dodawania liczb naturalnych: $y+x=[c,d]+[a,b]=[c+a,d+b]=$ $=[a+c,b+d]=[a,b]+[c,d]=x+y$, co dowodzi (i).

Ze wzoru (2.3) i z łączności dodawania liczb naturalnych mamy: $x+(y+z)=[a,b]+([c,d]+[r,s])=[a,b]+[c+r,d+s]=$ $=[a+(c+r),b+(d+s)]$, a zatem $x+(y+z)=[(a+c)+r,(b+d)+s]=$ $=[a+c,b+d]+[r,s]=([a,b]+[c,d])+[r,s]=(x+y)+z$, co dowodzi (ii).

Ponadto, $x+0=0+x=[1,1]+[a,b]=[a,b]+[1,1]=[a+1,b+1]$ oraz $(a+1,b+1)R(a,b)$, bo $a+1+b=b+1+a$, więc $[a+1,b+1]=[a,b]$ i $0+x=x+0=x$, co dowodzi (iii).

Na mocy przemienności dodawania liczb całkowitych, wzoru (2.3), stwierdzenia 2.2 i przemienności dodawania liczb naturalnych mamy: $[b,a]+x=x+[b,a]=[a+b,b+a]=[a+b,a+b]=[1,1]=0$, więc w punkcie (iv) wystarczy przyjąć $x'=[b,a]$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

(v). Ponieważ $x + y = x + z$, więc $x' + (x + y) = x' + (x + z)$, gdzie $x' + x = 0$. Stąd na mocy (ii), $(x' + x) + y = (x' + x) + z$, czyli $0 + y = 0 + z$ i na mocy (iii), $y = z$.

(vi). Ze wzoru (2.3) i ze stwierdzenia 2.2: $[k + 1, 1] + [l + 1, 1] = [k + l + 2, 2] = [(k + l) + 1, 1]$.

(vii). Ze wzoru (2.3) i ze stwierdzenia 2.2: $[1, k + 1] + [1, l + 1] = [2, k + l + 2] = [1, (k + l) + 1]$. □

Ze stwierdzenia 2.5 wynika zatem, że dla dowolnego całkowitego x istnieje całkowite y takie, że $x + y = 0$. Jeśli także $x + z = 0$ dla pewnego całkowitego z, to na mocy stwierdzenia 2.5, $z = y$. Wobec tego dla każdego całkowitego x istnieje dokładnie jedno całkowite y takie, że $x + y = 0$. To jedyne y nazywamy **elementem przeciwnym** do x i oznaczamy symbolem $-x$. Ponieważ $(-x) + x = 0$, więc x jest elementem przeciwnym do $(-x)$, czyli

$$-(-x) = x \text{ dla każdego całkowitego } x. \tag{2.4}$$

Ponadto z dowodu stwierdzenia 2.4 mamy, że dla dowolnych liczb naturalnych a, b:

$$-[a, b] = [b, a]. \tag{2.5}$$

2.3 Określenie i własności mnożenia liczb całkowitych

Mnożenie liczb całkowitych określamy przyjmując, że dla dowolnych $a, b, c, d \in \mathbb{N}$:

$$[a, b] \cdot [c, d] = [ac + bd, ad + cb]. \tag{2.6}$$

Udowodnimy, że mnożenie liczb całkowitych nie zależy od wyboru reprezentantów klas abstrakcji, to znaczy jeżeli $(a, b)R(a', b')$ i $(c, d)R(c', d')$, to $(ac + bd, ad + cb)R(a'c' + b'd', a'd' + c'b')$. Z naszych założeń wynika, że $a + b' = a' + b$ i $c + d' = c' + d$. Najpierw udowodnimy, że $(ac + bd, ad + cb)R(a'c + b'd, a'd + cb')$. W tym celu wystarczy

pokazać, że $ac+bd+a'd+cb' = a'c+b'd+ad+cb$, ale $ac+bd+a'd+cb' = c(a+b')+d(a'+b) = c(a'+b)+d(a+b') = a'c+b'd+ad+cb$, więc rzeczywiście $(ac+bd, ad+cb)R(a'c+b'd, a'd+cb')$. Następnie pokazujemy, że $(a'c+b'd, a'd+cb')R(a'c'+b'd', a'd'+c'b')$. W tym celu wystarczy pokazać, że $a'c+b'd+a'd'+c'b' = a'c'+b'd'+a'd+cb'$, ale $a'c+b'd+a'd'+c'b' = a'(c+d')+b'(c'+d) = a'(c'+d)+b'(c+d') = a'c'+b'd'+a'd+cb'$, więc rzeczywiście $(a'c+b'd, a'd+cb')R(a'c'+b'd', a'd'+c'b')$. Ponadto, jak pokazaliśmy, $(ac+bd, ad+cb)R(a'c+b'd, a'd+cb')$, więc z przechodniości relacji R, $(ac+bd, ad+cb)R(a'c'+b'd', a'd'+c'b')$.

Klasę $[2,1]$ będziemy oznaczali symbolem 1. Zatem na mocy stwierdzenia 2.3,

$$1 = [2,1] = \{(a+1, a) \ : \ a \in \mathbb{N}\}.$$

Stwierdzenie 2.6. *(i) Dla dowolnych $x, y \in \mathbb{Z}$: $x \cdot y = y \cdot x$ (to znaczy mnożenie liczb całkowitych jest przemienne),*

(ii) dla dowolnych $x, y, z \in \mathbb{Z}$: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (to znaczy mnożenie liczb całkowitych jest łączne),

(iii) dla każdego $x \in \mathbb{Z}$: $x \cdot 1 = 1 \cdot x = x$ (to znaczy 1 jest elementem neutralnym mnożenia liczb całkowitych),

(iv) dla dowolnych $x, y, z \in \mathbb{Z}$: $x \cdot (y + z) = x \cdot y + x \cdot z$ (to znaczy mnożenie liczb całkowitych jest rozdzielne względem dodawania),

(v) dla każdego $x \in \mathbb{Z}$: $0 \cdot x = x \cdot 0 = 0$,

(vi) dla dowolnych $k, l \in \mathbb{N}$: $[k+1, 1] \cdot [l+1, 1] = [kl+1, 1]$,

(vii) dla dowolnych $k, l \in \mathbb{N}$: $[k+1, 1] \cdot [1, l+1] = [1, l+1] \cdot [k+1, 1] = [1, kl+1]$,

(viii) dla dowolnych $k, l \in \mathbb{N}$: $[1, k+1] \cdot [1, l+1] = [kl+1, 1]$.

Dowód. Weźmy dowolne $x, y, z \in \mathbb{Z}$. Wtedy istnieją $a, b, c, d, r, s \in \mathbb{N}$ takie, że $x = [a, b]$, $y = [c, d]$ i $z = [r, s]$. Ze wzoru (2.6) i z przemienności mnożenia liczb naturalnych: $y \cdot x = [c, d] \cdot [a, b] = [ca+db, da+bc] = [ac+bd, ad+cb] = [a, b] \cdot [c, d] = x \cdot y$, co dowodzi (i).

Ze wzoru (2.6) i z własności dodawania i mnożenia liczb naturalnych: $x \cdot (y \cdot z) = [a, b] \cdot ([c, d] \cdot [r, s]) = [a, b] \cdot [cr+ds, cs+rd] = [a(cr+ds)+b(cs+rd), a(cs+rd)+(cr+ds)b]$, co oznacza, że $x \cdot (y \cdot z) = [acr+ads+bcs+bdr, acs+adr+bcr+bds]$ oraz $(x \cdot y) \cdot z = ([a, b] \cdot [c, d]) \cdot [r, s] = [ac+bd, ad+cb] \cdot [r, s]$, czyli $(x \cdot y) \cdot z =$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$= [(ac+bd)r+(ad+cb)s, (ac+bd)s+r(ad+cb)] = [acr+bdr+ads+$ $+bcs, acs+bds+adr+bcr]$, skąd $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, co dowodzi (ii).

Ponadto, na mocy (i), wzoru (2.6) i stwierdzenia 2.2, $x \cdot 1 = 1 \cdot x =$ $= [2,1] \cdot [a,b] = [2a+1 \cdot b, 2b+a \cdot 1] = [2a+b, 2b+a] = [a+(a+b), b+$ $+(a+b)] = [a,b] = x$, co dowodzi (iii).

(iv). Na mocy własności dodawania i mnożenia liczb całkowitych, wzorów (2.3) i (2.6) oraz stwierdzenia 2.2: $x \cdot (y+z) = [a,b] \cdot [c+r, d+s] =$ $= [a(c+r)+b(d+s), a(d+s)+(c+r)b] = [ac+ar+bd+bs, ad+as+bc+br]$ oraz $x \cdot y + x \cdot z = [a,b] \cdot [c,d] + [a,b] \cdot [r,s] = [ac+bd, ad+cb] + [ar+bs, as+$ $+rb] = [ac+bd+ar+bs, ad+cb+as+rb]$, więc $x \cdot (y+z) = x \cdot y + x \cdot z$.

(v). Na mocy (i), wzoru (2.6) i stwierdzenia 2.2: $x \cdot 0 = 0 \cdot x =$ $= [1,1] \cdot [a,b] = [1 \cdot a + 1 \cdot b, 1 \cdot b + a \cdot 1] = [a+b, a+b] = [1,1] = 0$.

(vi). Ze wzoru (2.6), z własności dodawania i mnożenia liczb naturalnych i ze stwierdzenia 2.2 mamy, że $[k+1,1] \cdot [l+1,1] =$ $= [(k+1)(l+1)+1 \cdot 1, (k+1) \cdot 1 + (l+1) \cdot 1] = [kl+k+l+2, k+l+2] =$ $= [(kl+1)+(k+l+1), 1+(k+l+1)] = [kl+1, 1]$.

(vii). Ze wzoru (2.6), z (i), z własności dodawania i mnożenia liczb naturalnych i ze stwierdzenia 2.2: $[k+1,1] \cdot [1,l+1] = [1,l+1] \cdot [k+1,1] =$ $= [1 \cdot (k+1) + (l+1) \cdot 1, 1 \cdot 1 + (k+1) \cdot (l+1)] = [k+l+2, kl+(k+l+2)] =$ $= [1, kl+1]$.

(viii). Ze wzoru (2.6), z własności dodawania i mnożenia liczb naturalnych i ze stwierdzenia 2.2 uzyskujemy, że $[k+1,1] \cdot [l+1,1] =$ $= [1 \cdot 1 + (k+1) \cdot (l+1), 1 \cdot (l+1) + 1 \cdot (k+1)] = [kl+(k+l+2), k+l+2] =$ $= [kl+1, 1]$. □

Stwierdzenie 2.7. *Dla dowolnych liczb całkowitych x, y, z takich, że $x \neq 0$:*

$$x \cdot y = x \cdot z \Rightarrow y = z.$$

Dowód. Weźmy dowolne $x, y, z \in \mathbb{Z}$ takie, że $x \neq 0$ oraz $x \cdot y = x \cdot z$. Wtedy na mocy stwierdzenia 2.3 istnieją liczby naturalne a, b, c, d, r, s takie, że $x = [a,b]$ i $a \neq b$ oraz $y = [c,d]$ i $z = [r,s]$. Zatem na mocy wzoru (2.6): $x \cdot y = [a,b] \cdot [c,d] = [ac+bd, ad+cb]$ i $x \cdot z =$ $= [a,b] \cdot [r,s] = [ar+bs, as+rb]$, więc $[ac+bd, ad+cb] = [ar+bs, as+rb]$, skąd $(ac+bd, ad+cb) R (ar+bs, as+rb)$. Zatem z definicji relacji R: $ac+bd+as+br = ad+bc+ar+bs$. Wobec tego, $a(c+s)+b(d+r) =$

$= b(c+s) + a(d+r)$, ale $a \neq b$, więc $a < b$ lub $b < a$. W pierwszym przypadku $(b-a)(d+r) = (b-a)(c+s)$, skąd po skróceniu przez $b - a \in \mathbb{N}$, $d + r = c + s$, więc $[c, d] = [r, s]$, czyli $y = z$. Natomiast w drugim przypadku, $(a-b)(c+s) = (a-b)(d+r)$, skąd po skróceniu przez $a - b \in \mathbb{N}$, $c + s = d + r$, więc $[c, d] = [r, s]$, czyli też $y = z$. □

Wniosek 2.8. *Dla dowolnych liczb całkowitych x i y mamy: jeżeli $x \neq 0$ i $y \neq 0$, to $x \cdot y \neq 0$. Równoważnie, jeżeli $x \cdot y = 0$, to $x = 0$ lub $y = 0$.*

Dowód. Załóżmy, że istnieją liczby całkowite $x \neq 0$ i $y \neq 0$ takie, że $x \cdot y = 0$. Wtedy na mocy stwierdzenia 2.6 (v), $x \cdot y = x \cdot 0$. Zatem ze stwierdzenia 2.7, $y = 0$ i mamy sprzeczność. Wobec tego dla dowolnych $x, y \in \mathbb{Z} \setminus \{0\}$ jest $x \cdot y \neq 0$. □

Stwierdzenie 2.9. *Dla dowolnych liczb całkowitych x i y:*
(i) $(-1) \cdot x = -x$,
(ii) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$,
(iii) $(-x) \cdot (-y) = x \cdot y$,
(iv) $-(x + y) = (-x) + (-y)$.

Dowód. Weźmy dowolne $x, y \in \mathbb{Z}$. Wtedy istnieją $a, b \in \mathbb{N}$ takie, że $x = [a, b]$. Ponieważ $1 = [2, 1]$, więc ze wzoru (2.5) oraz ze stwierdzenia 2.2, $-1 = [1, 2]$ i $(-1) \cdot x = [2, 1] \cdot [a, b] = [2a + 1 \cdot b, 2b + a \cdot 1] = [2a + b, a + 2b] = [a + (a + b), b + (a + b)] = [a, b] = x$, co dowodzi (i).

(ii) Na mocy (i), $-x = (-1) \cdot x$, więc na mocy stwierdzenia 2.6 oraz na mocy (i), $(-x) \cdot y = [(-1) \cdot x] \cdot y = (-1) \cdot (x \cdot y) = -(x \cdot y)$ oraz $-y = (-1) \cdot y$, więc podobnie, $x \cdot (-y) = x \cdot [(-1) \cdot y] = [x \cdot (-1)] \cdot y = [(-1) \cdot x] \cdot y = (-x) \cdot y$, co dowodzi (ii).

(iii). Podstawiając w (ii) $(-y)$ w miejsce elementu y uzyskujemy, że $(-x) \cdot (-y) = -[x \cdot (-y)]$, ale na mocy (ii), $x \cdot (-y) = -(x \cdot y)$, więc $(-x) \cdot (-y) = -[-(x \cdot y)] = x \cdot y$ na mocy wzoru (2.4).

(iv). Zauważmy, że $(x+y)+[(-x)+(-y)] = [x+(-x)]+[y+(-y)] = 0 + 0 = 0$, a to oznacza, że $(-x) + (-y)$ jest elementem przeciwnym do elementu $x + y$, czyli $-(x + y) = (-x) + (-y)$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

2.4 Określenie i własności odejmowania liczb całkowitych

Odejmowanie liczb całkowitych określamy przyjmując, że dla dowolnych $x, y \in \mathbb{Z}$:

$$x - y = x + (-y). \tag{2.7}$$

W szczególności, dla każdego $x \in \mathbb{Z}$ jest $x - x = 0$, bo $x - x = x + (-x) = 0$. Ponadto dla $a, b, c, d \in \mathbb{N}$ na mocy (2.5) i (2.3) mamy, że $[a, b] - [c, d] = [a, b] + (-[c, d]) = [a, b] + [d, c] = [a + d, b + c]$, czyli

$$[a, b] - [c, d] = [a + d, b + c]. \tag{2.8}$$

Zauważmy, że dla $n, m \in \mathbb{N}$ mamy następujące wzory:

$$n > m \Rightarrow [n + 1, 1] - [m + 1, 1] = [(n - m) + 1, 1], \tag{2.9}$$

$$n < m \Rightarrow [n + 1, 1] - [m + 1, 1] = [1, (m - n) + 1]. \tag{2.10}$$

Rzeczywiście, ze wzoru (2.8) i ze stwierdzenia 2.3 w przypadku, gdy $n > m$, $[n+1, 1]-[m+1, 1] = [n+2, m+2] = [(n-m)+(m+2), m+2] = [(n-m)+1, 1]$, zaś w przypadku, gdy $n < m$: $[n+1, 1]-[m+1, 1] = [n + 2, m + 2] = [n + 2, (m - n) + (n + 2)] = [1, (m - n) + 1]$.

Stwierdzenie 2.10. *Dla dowolnych liczb całkowitych x, y zachodzi wzór:*

$$x \cdot (y - z) = x \cdot y - x \cdot z.$$

Dowód. Na mocy (2.7), stwierdzenia 2.6 (iv), stwierdzenia 2.8 (ii) i wzoru (2.7) mamy, że $x \cdot (y - z) = x \cdot [y + (-z)] = x \cdot y + x \cdot (-z) = x \cdot y + [-(x \cdot z)] = x \cdot y - x \cdot z$. □

2.5 Określenie i własności uporządkowania liczb całkowitych

Relację mniejszości $<$ w zbiorze liczb całkowitych określamy przyjmując dla dowolnych $a, b, c, d \in \mathbb{N}$, że:

$$[a, b] < [c, d] \iff a + d < b + c. \tag{2.11}$$

Udowodnimy, że wzór (2.11) nie zależy od wyboru reprezentantów klas abstrakcji, to znaczy jeżeli $(a,b)R(a',b')$ i $(c,d)R(c',d')$, to $a+d<b+c$ wtedy i tylko wtedy, gdy $a'+d'<b'+c'$. Z naszych założeń wynika, że $a+b'=a'+b$ i $c+d'=c'+d$. Jeżeli $a+d<b+c$, to $(a+d)+(a'+c')<$ $<(b+c)+(a'+c')$, czyli $a+a'+(c'+d)<(b+a')+c+c'$, skąd $a+a'+c+d'<a+b'+c+c'$, więc $a'+d'<b'+c'$. Analogicznie dowodzi się, że jeśli $a'+d'<b'+c'$, to $a+d<b+c$.

Stwierdzenie 2.11. *Dla dowolnych liczb całkowitych x,y,z:*
(i) $\sim(x<x)$,
(ii) $[x<y \text{ i } y<z]\Rightarrow x<z$,
(iii) $x=y$ *albo* $x<y$ *albo* $y<x$,
(iv) $x<y \iff x-y<0$,
(v) $x<y \iff x+z<y+z$.

Dowód. Weźmy dowolne $x,y,z\in\mathbb{Z}$. Wtedy istnieją $a,b,c,d,r,s\in\mathbb{N}$ takie, że $x=[a,b]$, $y=[c,d]$ i $z=[r,s]$. Ponieważ nie jest prawdą, że $a+b<b+a$, więc ze wzoru (2.11) mamy, że $\sim(x<x)$, co dowodzi (i).

Dla dowodu (ii) załóżmy, że $x<y$ i $y<z$. Wtedy z (2.11), $a+d<$ $<b+c$ i $c+s<d+r$, skąd $a+d+s<b+c+s$ i $c+s+b<d+r+b$. Zatem z przechodniości relacji $<$ w zbiorze $\mathbb{N}$ mamy, że $a+s+d<b+r+d$, skąd $a+s<b+r$, a to wobec (2.11) oznacza, że $x<z$.

(iii). Jeśli $x=y$, to na mocy (i), $\sim(x<y)$ i $\sim(y<x)$. Jeśli $x<y$ i $y<x$, to na mocy (ii), $x<x$, co przeczy (i). Wobec tego warunki: $x=y$, $x<y$ i $y<x$ wykluczają się wzajemnie. Ponadto ze stwierdzenia 1.21 wiemy, że $a+d=b+c$ lub $a+d<b+c$ lub $b+c<a+d$, co wobec (2.11) oznacza, że $x=y$ lub $x<y$ lub $y<x$ i ostatecznie mamy, że $x=y$ albo $x<y$ albo $y<x$.

(iv). Ponieważ $0=[1,1]$ i na mocy wzoru (2.8), $x-y=[a+d,b+c]$, więc ze wzoru (2.11), $x-y<0 \iff [a+d,b+c]<[1,1]$, czyli $x-y<0 \iff a+d+1<b+c+1 \iff a+d<b+c \iff x<y$, co kończy dowód tego punktu.

(v). Ze wzoru (2.7) i ze stwierdzenia 2.9 (iv), $(x+z)-(y+z)=$ $=x+z+(-y)+(-z)=[x+(-y)]+[z+(-z)]=(x-y)+0=x-y$. Wobec tego na mocy (iv), $x<y \iff x+z<y+z$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Definicja 2.12. W zbiorze $\mathbb{Z}$ określamy przy użyciu relacji $<$ relacje: $>$, $\leqslant$ i $\geqslant$ przyjmując, że dla dowolnych $x, y \in \mathbb{Z}$:
(i) $x > y \iff y < x$,
(ii) $x \leqslant y \iff (x = y \text{ lub } x < y)$,
(iii) $x > y \iff (x = y \text{ lub } y < x)$.

Z definicji 2.12 i ze stwierdzenia 2.11 mamy od razu

Wniosek 2.13. *Dla dowolnych liczb całkowitych x, y, z:*
(i) $x \leqslant x$,
(ii) $(x \leqslant y \text{ i } y \leqslant z) \Rightarrow x \leqslant z$,
(iii) $x \leqslant y$ *lub* $y \leqslant x$,
(iv) $x \leqslant y \iff x - y \leqslant 0$,
(v) $(x \leqslant y \text{ i } y \leqslant x) \Rightarrow x = y$.

Stwierdzenie 2.14. *Dla dowolnych $a, b \in \mathbb{N}$:*
(i) $[a, b] > 0 \iff a > b$,
(ii) $[a, b] < 0 \iff a < b$,
(iii) $[a, b] = 0 \iff a = b$.

Dowód. Ponieważ $0 = [1, 1]$, więc na mocy (2.11) i definicji 2.12, $[a, b] > 0 \iff [1, 1] < [a, b] \iff 1 + b < 1 + a \iff b < a$, co dowodzi (i). Analogicznie, $[a, b] < 0 \iff [a, b] < [1, 1]$, czyli $[a, b] < 0 \iff a + 1 < b + 1 \iff a < b$, co dowodzi (ii). Ponadto, $[a, b] = 0 \iff [a, b] = [1, 1] \iff a + 1 = 1 + b \iff a = b$, co dowodzi (iii). □

Ze wzoru (2.5) i ze stwierdzenia 2.14 od razu wynika, że dla dowolnego $x \in \mathbb{Z}$:

$$[x < 0 \iff -x > 0] \text{ oraz } [x > 0 \iff -x < 0]. \tag{2.12}$$

Stwierdzenie 2.15. *Dla dowolnych $m, n \in \mathbb{N}$ zachodzą wzory:*
(i) $[n + 1, 1] > 0$,
(ii) $[n + 1, 1] < [m + 1, 1] \iff n < m$,
(iii) $[1, n + 1] < [1, m + 1] \iff m < n$,
(iv) $[1, n + 1] = -[n + 1, 1]$ *i* $[1, n + 1] < 0$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Punkt (i) wynika od razu ze stwierdzenia 2.14 (i) oraz stąd, że $n+1>1$ dla każdego $n\in\mathbb{N}$. Dla dowodu (ii), zauważmy, że ze wzoru (2.11), $[n+1,1]<[m+1,1] \iff n+1+1<1+m+1 \iff n+2<$ $<m+2 \iff n<m$. Dla dowodu wzoru (iii) zauważmy, że ze wzoru (2.11), $[1,n+1]<[1,m+1] \iff 1+m+1<n+1+1 \iff m+2<$ $<n+2 \iff m<n$.

(iv). Ze wzoru (2.5), $-[n+1,1]=[1,n+1]$ i $0=[1,1]$ oraz $1+1<$ $<n+1+1$, więc na mocy wzoru (2.11), $[1,n+1]<0$. □

Stwierdzenie 2.16. *Zbiory* $\{[1,n+1] : n\in\mathbb{N}\}$, $\{[n+1,1] : n\in\mathbb{N}\}$ *i* $\{0\}$ *są parami rozłączne i ich suma jest równa* $\mathbb{Z}$. *Ponadto* $\{x\in\mathbb{Z} : x>0\}=\{[n+1,1] : n\in\mathbb{N}\}$ *i* $\{x\in\mathbb{Z} : x<0\}=$ $=\{[1,n+1] : n\in\mathbb{N}\}$.

Dowód. Ponieważ $0=[1,1]$, więc na mocy stwierdzenia 2.3, $\mathbb{Z}$ jest sumą zbiorów $\{[1,n+1] : n\in\mathbb{N}\}$, $\{0\}$ i $\{[n+1,1] : n\in\mathbb{N}\}$. Ponadto ze stwierdzenia 2.3 te zbiory są parami rozłączne.

Natomiast ze Stwierdzeń 2.3, 2.15 i 2.11 (i) od razu wynika, że $\{x\in\mathbb{Z} : x>0\}=\{[n+1,1] : n\in\mathbb{N}\}$ i $\{x\in\mathbb{Z} : x<0\}=$ $=\{[1,n+1] : n\in\mathbb{N}\}$. □

Liczby całkowite mniejsze od 0 będziemy nazywali **ujemnymi liczbami całkowitymi**, zaś liczby całkowite większe od 0 będziemy nazywali **dodatnimi liczbami całkowitymi**.

Ze Stwierdzeń 2.16 i 2.6 (vi)-(viii) od razu wynika następujące

Stwierdzenie 2.17. *Dla dowolnych liczb całkowitych* x,y:
(i) jeżeli $x>0$ *i* $y>0$, *to* $x\cdot y>0$,
(ii) jeżeli $x>0$ *i* $y<0$, *to* $x\cdot y<0$,
(iii) jeżeli $x<0$ *i* $y<0$, *to* $x\cdot y>0$.

Stwierdzenie 2.18. *Dla dowolnych liczb całkowitych* x,y,z:
(i) jeżeli $x<y$ *i* $z>0$, *to* $x\cdot z<y\cdot z$,
(ii) jeżeli $x<y$ *i* $z<0$, *to* $x\cdot z>y\cdot z$.

Dowód. (i). Z naszych założeń i ze stwierdzenia 2.11 (iv) wynika, że $x-y<0$. Zatem ze stwierdzenia 2.17 (ii), $z\cdot(x-y)<0$, skąd na mocy

stwierdzenia 2.10, $z \cdot x - z \cdot y < 0$. Wobec tego na mocy stwierdzenia 2.11 (iv), $z \cdot x < z \cdot y$.

(ii). Z naszych założeń i ze stwierdzenia 2.11 (iv), $x - y < 0$. Zatem ze stwierdzenia 2.17 (iii), $z \cdot (x - y) > 0$, skąd na mocy stwierdzenia 2.10, $z \cdot x - z \cdot y > 0$. Wobec tego na mocy stwierdzenia 2.11 (iv), $z \cdot x > z \cdot y$. □

Stwierdzenie 2.19. *Dla dowolnych liczb całkowitych x, y, z:*
(i) jeżeli $x \cdot z < y \cdot z$ i $z > 0$, to $x < y$,
(ii) jeżeli $x \cdot z < y \cdot z$ i $z < 0$, to $x > y$.

Dowód. (i). Załóżmy, że $x \cdot z < y \cdot z$ i $z > 0$. Wtedy $z \neq 0$ i ze stwierdzenia 2.11 (iii), $x = y$ lub $y < x$ lub $x < y$. W pierwszym przypadku, $x \cdot z = y \cdot z$, co prowadzi do sprzeczności, gdyż $x \cdot z < y \cdot z$. W drugim przypadku, na mocy stwierdzenia 2.18 (i), $y \cdot z < x \cdot x$, co prowadzi do sprzeczności, bo $x \cdot z < y \cdot z$. Wobec tego musi być $x < y$.

(ii). Załóżmy, że $x \cdot z < y \cdot z$ i $z < 0$. Wtedy $z \neq 0$ i ze stwierdzenia 2.11 (iii), $x = y$ lub $x < y$ lub $x > y$. W pierwszym przypadku, $x \cdot z = y \cdot z$, co prowadzi do sprzeczności, gdyż $x \cdot z < y \cdot z$. W drugim przypadku, na mocy stwierdzenia 2.18 (ii), $y \cdot z < x \cdot z$, co prowadzi do sprzeczności, bo $x \cdot z < y \cdot z$. Wobec tego musi być $x > y$. □

Stwierdzenie 2.20. *Dla dowolnych liczb całkowitych x, y:*
(i) jeżeli $x < y$, to $x + 1 \leqslant y$,
(ii) nie istnieje liczba całkowita z taka, że $x < z < x + 1$.

Dowód. Istnieją $a, b, c, d \in \mathbb{N}$ takie, że $x = [a, b]$ i $y = [c, d]$. Załóżmy, że $x < y$. Wtedy ze wzoru (2.11), $a+d < b+c$. Zatem z własności liczb naturalnych $a+d+1 \leqslant b+c$. Dalej, $x+1 = [a, b]+[2, 1] = [a+2, b+1] = [a+1, b]$, bo $(a+2, b+1)R(a+1, b)$, gdyż $(a+2)+b = (a+1)+(b+1)$. Stąd jeśli $a + d + 1 = b + c$, to $x + 1 = y$, a jeśli zaś $a + d + 1 < b + c$, to $x + 1 < y$. Zatem $x + 1 \leqslant y$, co dowodzi (i).

(ii). Załóżmy, że $x < z < x+1$ dla pewnego $z \in \mathbb{Z}$. Wtedy $z = [r, s]$ dla pewnych $r, s \in \mathbb{N}$. Ponadto, $x + 1 = [a + 1, b]$ i ze wzoru (2.11), $a + s < r + b$ oraz $r + b < a + 1 + s$, więc $a + s < r + b < (a + s) + 1$, co przeczy stwierdzeniu 1.20. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 2.21. *Dla dowolnych liczb całkowitych x, y, u, v:*

$$[x < y \text{ i } u < v] \Rightarrow x + u < y + v.$$

Dowód. Załóżmy, że $x < y$ i $u < v$. Wtedy na mocy stwierdzenia 2.11 (v), po dodaniu do obu stron pierwszej nierówności liczby u oraz po dodaniu do obu stron drugiej nierówności liczby y uzyskamy, że $x + u < y + u$ i $y + u < y + v$. Stąd na mocy stwierdzenia 2.11 (iii), $x + u < y + v$. □

2.6 Liczby naturalne jako dodatnie liczby całkowite

Z przeprowadzonych przez nas rozważań wynika, że dla dowolnych liczb naturalnych m, n:

$$[m + 1, 1] = [n + 1, 1] \iff m = n,$$

$$[m + 1, 1] + [n + 1, 1] = [(m + n) + 1, 1],$$
$$[m + 1, 1] \cdot [n + 1, 1] = [m \cdot n + 1, 1],$$
$$[m + 1, 1] < [n + 1, 1] \iff m < n.$$

W związku z tym możemy utożsamić klasę $[n+1, 1]$ z liczbą naturalną n:

$$[n + 1, 1] \equiv n \text{ dla } n \in \mathbb{N}. \tag{2.13}$$

Wtedy $[1, n + 1] = -[n + 1, 1]$, czyli

$$[1, n + 1] \equiv -n \text{ dla } n \in \mathbb{N}. \tag{2.14}$$

Wynika stąd, że wszystkim i liczbami całkowitymi są:

$$0, 1, -1, 2, -2, \ldots$$

oraz zbiór $\mathbb{N}$ zawiera się w zbiorze $\mathbb{Z}$ wszystkich liczb całkowitych, zaś relacja $<$ w zbiorze $\mathbb{Z}$ jest przedłużeniem relacji $<$ określonej w zbiorze

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$\mathbb{N}$ i podobne uwagi dotyczą dodawania i mnożenia. Wobec tego nasza formalna konstrukcja spełnia wszystkie warunki, o których pisaliśmy w rozdziale 1. Dalej nie będziemy traktowali liczb całkowitych jako klasy, lecz będziemy dla nich stosowali normalne, standardowe oznaczenia, znane ze szkoły. Będziemy też korzystali (czasami bez stosowania szczegółowych odnośników) z udowodnionych przez nas własności liczb całkowitych.

2.7 Pewne szczególne własności liczb całkowitych

Stwierdzenie 2.22. (aksjomat Archimedesa). *Niech $m \in \mathbb{N}$ i $a \in \mathbb{Z}$. Wówczas istnieje liczba naturalna k taka, że $m \cdot k > a$ oraz dla dowolnego naturalnego $t \geqslant k$ jest $m \cdot t > a$.*

Dowód. Jeżeli $k, t \in \mathbb{N}$, $t \geqslant k$ i $m \cdot k > a$, to $m \cdot t \geqslant m \cdot k$, skąd $m \cdot t > a$. Wystarczy zatem pokazać istnienie k. Jeżeli $a \leqslant 0$, to wystarczy przyjąć $k = 1$. Jeżeli zaś $a > 0$, to $a \in \mathbb{N}$ i dla $k = a + 1$ jest $m \cdot k = m \cdot (a + 1) = m \cdot a + m \geqslant a + m > a$, bo $m \geqslant 1$. □

Definicja 2.23. Powiemy, że niepusty podzbiór X zbioru $\mathbb{Z}$ jest ograniczony z góry, jeżeli istnieje $a \in \mathbb{Z}$ takie, że $x \leqslant a$ dla wszystkich $x \in X$.

Zauważmy, że zbiór wszystkich liczb całkowitych ujemnych jest ograniczony z góry, gdyż każda liczba ujemna jest mniejsza od 0. Natomiast zbiór $\mathbb{N}$ nie jest ograniczony z góry, gdyż dla każdej liczby naturalnej n mamy $n < n + 1$.

Stwierdzenie 2.24. (zasada maksimum). *Każdy niepusty ograniczony z góry podzbiór zbioru liczb całkowitych posiada liczbę największą, czyli liczbę większą lub równą od każdej liczby tego podzbioru.*

Dowód. Niech X będzie niepustym podzbiorem zbioru $\mathbb{Z}$ ograniczonym z góry. Wówczas istnieje liczba całkowita a taka, że $x \leqslant a$ dla każdego $x \in X$. Załóżmy najpierw, że $X \cap \mathbb{N} \neq \emptyset$. Wtedy podzbiór $X \cap \mathbb{N}$ zbioru

$\mathbb{N}$ jest ograniczony z góry przez liczbę a, więc z zasady maksimum dla liczb naturalnych uzyskujemy, że w zbiorze $X \cap \mathbb{N}$ istnieje liczba największa y. Wtedy $y > x$ dla wszystkich całkowitych $x \leqslant 0$, skąd wynika, że $x \leqslant y$ dla wszystkich $x \in X$. Wobec tego y jest największą liczbą w zbiorze X.

Pozostaje zatem do rozważenia przypadek, gdy do X nie należy żadna liczba naturalna, czyli gdy $X \subseteq \{0\} \cup \{-n \ : \ n \in \mathbb{N}\}$. Jeśli $0 \in X$, to 0 jest największą liczbą w zbiorze X. Niech dalej, $X \subseteq$ $\subseteq \{-n \ : \ n \in \mathbb{N}\}$. Wówczas istnieje niepusty podzbiór A zbioru $\mathbb{N}$ taki, że $X = \{-a \ : \ a \in A\}$. Z zasady minimum w zbiorze liczb naturalnych wynika, że w zbiorze A istnieje liczba najmniejsza b. Wtedy $b \leqslant a$ dla każdego $a \in A$, skąd $-b \geqslant -a$ dla każdego $a \in A$. Wobec tego $-b$ jest największą liczbą w zbiorze X. □

2.8 Twierdzenie o dzieleniu z resztą

Twierdzenie 2.25. (o dzieleniu z resztą). *Niech $m \in \mathbb{N}$. Wówczas dla każdego $a \in \mathbb{Z}$ istnieje dokładnie jedna para (q, r) liczb całkowitych taka, że $a = q \cdot m + r$ i $0 \leqslant r < m$.*

Dowód. Niech X będzie zbiorem wszystkich liczb całkowitych q takich, że $q \cdot m \leqslant a$. Jeśli $a \geqslant 0$, to $0 \in X$, a jeśli $a < 0$, to $a \in X$, bo wtedy $m \geqslant 1$, skąd $am \leqslant a$. Zatem $X \neq \emptyset$. Z Aksjomatu Archimedesa wynika, że zbiór X jest ograniczony z góry. Wobec tego na mocy zasady maksimum istnieje w X liczba największa q. Zatem $q \cdot m \leqslant a$, więc ponieważ $q+1 > q$, to $q+1 \notin X$ i $(q+1) \cdot m > a$. Stąd $r = a - q \cdot m \geqslant 0$, $r \in \mathbb{Z}$ i $r < m$ oraz $a = q \cdot m + r$.

Niech teraz $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ będą takie, że $a = q_1 \cdot m + r_1 = q_2 \cdot m + r_2$ oraz $0 \leqslant r_1, r_2 < m$. Wtedy $q_1 \cdot m - q_2 \cdot m = r_2 - r_1$, skąd $(q_1 - q_2) \cdot m =$ $= r_2 - r_1$. Ponadto $-m < r_2 - r_1 < m$, więc $-m < (q_1 - q_2) \cdot m < m$, skąd $-1 < q_1 - q_2 < 1$. Zatem $q_1 - q_2 = 0$ i wobec tego $r_2 - r_1 = 0$, czyli $q_1 = q_2$ i $r_1 = r_2$, a więc $(q_1, r_1) = (q_2, r_2)$. □

Uwaga 2.26. Liczbę r podaną w sformułowaniu twierdzenia 2.25 nazywamy **resztą z dzielenia** liczby całkowitej a przez liczbę naturalną m i oznaczamy symbolem $[a]_m$. Natomiast liczbę q nazywamy

niepełnym ilorazem z dzielenia liczby całkowitej a przez liczbę naturalną m.

Ponieważ $-1 = (-1) \cdot 5 + 4$ i $0 \leqslant 4 < 5$, więc $[-1]_5 = 4$. Jeżeli $0 \leqslant r < m$ i $r \in \mathbb{Z}$, to oczywiście $[r]_m = r$, bo $r = 0 \cdot m + r$ i $0 \leqslant r < m$. Zatem na przykład $[1]_5 = 1$ oraz $[5]_7 = 5$. Aby obliczyć $[101]_7$, wykonujemy pisemne dzielenie liczby 101 przez 7 i uzyskujemy, że $101 = 14 \cdot 7 + 3$, więc $[101]_7 = 3$.

Uwaga 2.27. Zauważmy, że twierdzenie o dzieleniu z resztą możemy wypowiedzieć równoważnie innymi słowami: Niech $m \in \mathbb{N} \setminus \{1\}$. Wówczas każda liczba całkowita jest dokładnie jednej z m postaci: $mk, mk+1, \ldots, mk+(m-1)$ dla $k \in \mathbb{Z}$, czyli zbiór $\mathbb{Z}$ jest sumą m parami rozłącznych podzbiorów: $A_0, A_1, \ldots, A_{m-1}$, gdzie $A_j = \{km + j : k \in \mathbb{Z}\}$ dla $j = 0, 1, \ldots, m-1$.

W szczególności dla $m = 2$ mamy, że każda liczba całkowita jest postaci $2k$ (to znaczy jest parzysta) albo jest postaci $2k+1$ (to znaczy jest nieparzysta), czyli zbiór $\mathbb{Z}$ jest sumą rozłącznych podzbiorów: $\{2k : k \in \mathbb{Z}\}$ i $\{2k+1 : k \in \mathbb{Z}\}$.

Dla $m = 3$ mamy, że każda liczba całkowita jest postaci $3k$ albo $3k+1$ albo $3k+2$, a więc zbiór $\mathbb{Z}$ jest sumą trzech parami rozłącznych zbiorów: $\{3k : k \in \mathbb{Z}\}$, $\{3k+1 : k \in \mathbb{Z}\}$ i $\{3k+2 : k \in \mathbb{Z}\}$.

Wartością bezwzględną (modułem) liczby całkowitej x nazywamy nieujemną liczbę całkowitą $|x|$ określoną wzorem:

$$|x| = \begin{cases} x & \text{dla } x \geqslant 0 \\ -x & \text{dla } x < 0 \end{cases} . \tag{2.15}$$

Możemy teraz podać uogólnienie twierdzenia 2.25 nazywane przez niektórych twierdzeniem o dzieleniu z resztą:

Twierdzenie 2.28. *Niech b będzie niezerową liczbą całkowitą. Wówczas dla każdego $a \in \mathbb{Z}$ istnieje dokładnie jedna para (q, r) liczb całkowitych taka, że $a = q \cdot b + r$ i $0 \leqslant r < |b|$.*

Dowód. Jeżeli $b > 0$, to teza wynika od razu z twierdzenia 2.25. Niech $b < 0$. Wtedy $m = -b \in \mathbb{N}$. Weźmy dowolne $a \in \mathbb{Z}$. Wtedy z twierdzenia 2.25 istnieją liczby całkowite x i r takie, że $0 \leqslant r < m = |b|$

i $a = xm+r = (-x)\cdot b+r$. Niech $q, s \in \mathbb{Z}$ będą takie, że $0 \leqslant s < |b| = m$ i $a = qb+s$. Wtedy $a = (-q)\cdot m+s$. Zatem z twierdzenia 2.25, $-q = x$ i $s = r$, więc $q = -x$. Kończy to nasz dowód. □

Przykład 2.29. Załóżmy, że $m^2 = 2n^2$ dla pewnych $m, n \in \mathbb{N}$. Wówczas z zasady minimum istnieje najmniejsza liczba naturalna k taka, że $k^2 = 2s^2$ dla pewnego $s \in \mathbb{N}$. Ponieważ $2s^2 > s^2$, więc stąd $k > s$. Z twierdzenia o dzieleniu z resztą wynika, że $k = 2l$ lub $k = 2l+1$ dla pewnego $l \in \mathbb{N}_0$. W drugim przypadku $[k^2]_2 = [4l^2 + 4l + 1]_2 = 1$ i $[2s^2]_2 = 0$, co prowadzi do sprzeczności. Natomiast w pierwszym przypadku $4l^2 = 2s^2$, skąd $s^2 = 2l^2$, ale $s < k$, więc mamy sprzeczność z minimalnością liczby k.

Uzyskana sprzeczność pokazuje, że nie istnieją $m, n \in \mathbb{N}$ takie, że $m^2 = 2n^2$. Stąd natomiast wynika, że nie istnieją niezerowe liczby całkowite x i y takie, że $x^2 = 2y^2$.

W następnym twierdzeniu podajemy podstawowe własności obliczania reszt.

Twierdzenie 2.30. *Niech $m, n \in \mathbb{N}$ i niech $a_i, b_i \in \mathbb{Z}$ oraz $[a_i]_m = [b_i]_m$ dla $i = 1, \ldots, n$. Wówczas:*
(i) $[a_1 + \ldots + a_n]_m = [b_1 + \ldots + b_n]_m$,
(ii) $[a_1 \cdot \ldots \cdot a_n]_m = [b_1 \cdot \ldots \cdot b_n]_m$.

Dowód. (i). Z założenia mamy, że $a_i = q_i m + r_i$ oraz $b_i = p_i m + r_i$, gdzie $p_i, q_i \in \mathbb{Z}$ oraz $r_i \in \{0, 1, \ldots, m-1\}$ dla $i = 1, \ldots, n$. Z twierdzenia 2.25, $r_1 + \ldots + r_n = qm + r$ dla pewnych $q, r \in \mathbb{Z}$ takich, że $0 \leqslant r < m$. Wobec tego $a_1 + \ldots + a_n = (q + q_1 + \ldots + q_n)m + r$ oraz $b_1 + \ldots + b_n = (q + p_1 + \ldots + p_n)m + r$. Zatem z twierdzenia 2.25, $r = [a_1 + \ldots + a_n]_m = [b_1 + \ldots + b_n]_m$.

(ii). Zastosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista. Przypuśćmy teraz, że teza zachodzi dla pewnego $n \in \mathbb{N}$ i niech $a_i, b_i \in \mathbb{Z}$ będą takie, że $[a_i]_m = [b_i]_m$ dla $i = 1, \ldots, n, n+1$. Wtedy z założenia indukcyjnego wynika, że $a_1 \cdot \ldots \cdot a_n = pm + r$ i $b_1 \cdot \ldots \cdot b_n = qm + r$ dla pewnych $p, q, r \in \mathbb{Z}$. Ponadto $a_{n+1} = xm + s$ i $b_{n+1} = ym + s$ dla pewnych $x, y, s \in \mathbb{Z}$, więc $a_1 \cdot \ldots \cdot a_n \cdot a_{n+1} = (pm + r)(xm + s) = (pmx + rx + ps)m +$

$+rs$ oraz $b_1 \cdot \ldots \cdot b_n \cdot b_{n+1} = (qm+r)(ym+s) = (qmy+ry+qs)m+rs$. Z twierdzenia 2.25, $rs = Qm + R$ dla pewnych $Q, R \in \mathbb{Z}$ takich, że $0 \leqslant R < m$. Zatem $a_1 \cdot \ldots \cdot a_n \cdot a_{n+1} = (pmx + rx + ps + Q)m + R$ i $b_1 \cdot \ldots \cdot b_n \cdot b_{n+1} = (qmy+ry+qs+Q)m+R$. Stąd na mocy twierdzenia 2.25, $R = [a_1 \cdot \ldots \cdot a_{n+1}]_m = [b_1 \cdot \ldots \cdot b_{n+1}]_m$, czyli teza zachodzi dla liczby $n+1$. □

Podstawiając $a = a_1 = \ldots = a_n$ i $b = b_1 = \ldots = b_n$ w twierdzeniu 2.30 uzyskujemy od razu następujący

Wniosek 2.31. *Niech $m, n \in \mathbb{N}$ i niech $a, b \in \mathbb{Z}$ oraz $[a]_m = [b]_m$. Wówczas $[a^n]_m = [b^n]_m$.*

Wszędzie dalej zbiór $\mathbb{N} \cup \{0\}$ będziemy oznaczali symbolem $\mathbb{N}_0$.

Twierdzenie 2.32. *Niech $m \in \mathbb{N}$ oraz niech $a, b \in \mathbb{Z}$ będą takie, że $[a]_m = [b]_m$. Wówczas $[f(a)]_m = [f(b)]_m$ dla każdej funkcji $f\colon \mathbb{Z} \to \mathbb{Z}$ postaci $f(x) = c_0 + c_1 x + \ldots + c_n x^n$, gdzie $n \in \mathbb{N}_0$ oraz $c_0, c_1, \ldots, c_n \in \mathbb{Z}$.*

Dowód. Na mocy wniosku 2.31, $[a^k]_m = [b^k]_m$ dla $k = 0, 1, \ldots, n$. Stąd i z twierdzenia 2.30 (ii), $[c_k a^k]_m = [c_k b^k]_m$ dla $k = 0, 1, \ldots, n$. Zatem na mocy twierdzenia 2.30 (i),

$$[c_0 + c_1 a + \ldots + c_n a^n]_m = [c_0 + c_1 b + \ldots + c_n b^n]_m,$$

czyli $[f(a)]_m = [f(b)]_m$. □

Przykład 2.33. Obliczymy resztę z dzielenia liczby 5^{1994} przez 3. Ponieważ $[5]_3 = 2$ i $[-1]_3 = 2$, gdyż $5 = 1 \cdot 3 + 2$ oraz $-1 = (-1) \cdot 3 + 2$, więc na mocy wniosku 2.31 mamy, że $[5^{1994}]_3 = [(-1)^{1994}]_3 = [1]_3 = 1$.

Ćwiczenie 2.34. Udowodnij, że liczba 4444^{4444} przy dzieleniu przez 9 daje resztę 7.

Przykład 2.35. Udowodnimy, że ciąg reszt z dzielenia przez 31 liczb postaci 10^n jest okresowy. Mamy, $[10]_{31} = 10$, $[10^2]_{31} = [100]_{31} = 7$, więc stosując wielokrotnie twierdzenie 2.30 uzyskujemy $[10^3]_{31} = [10 \cdot 7]_{31} = 8$, $[10^4]_{31} = [7 \cdot 7]_{31} = 18$, $[10^5]_{31} = [7 \cdot 8]_{31} = 25$, $[10^6]_{31} = [8 \cdot 8]_{31} = 2$, $[10^7]_{31} = [2 \cdot 10]_{31} = 20$, $[10^8]_{31} = [7 \cdot 2]_{31} = 14$,

$[10^9]_{31} = [8 \cdot 2]_{31} = 16$, $[10^{10}]_{31} = [18 \cdot 2]_{31} = 5$, $[10^{11}]_{31} = [10 \cdot 5]_{31} = 19$, $[10^{12}]_{31} = [2 \cdot 2]_{31} = 4$, $[10^{13}]_{31} = [10 \cdot 4]_{31} = 9$, $[10^{14}]_{31} = [2 \cdot 14]_{31} = 28$, $[10^{15}]_{31} = [2 \cdot 16]_{31} = 1$, więc na mocy wniosku 2.31 dla każdego $k \in \mathbb{N}_0$ mamy, że $[10^{15k}]_{31} = 1$, a stąd na mocy twierdzenia 2.30: $[10^{15k+1}]_{31} = 10$, $[10^{15k+2}]_{31} = 7$, $[10^{15k+3}]_{31} = 8$, $[10^{15k+4}]_{31} = 18$, $[10^{15k+5}]_{31} = 25$, $[10^{15k+2}]_{31} = 2$, $[10^{15k+7}]_{31} = 20$, $[10^{15k+8}]_{31} = 14$, $[10^{15k+9}]_{31} = 16$, $[10^{15k+10}]_{31} = 5$, $[10^{15k+11}]_{31} = 19$, $[10^{15k+12}]_{31} = 4$, $[10^{15k+13}]_{31} = 9$, $[10^{15k+14}]_{31} = 28$, czyli ciąg $([10^n]_{31})$ jest okresowy o podstawowym okresie 10, 7, 8, 18, 25, 2, 20, 14, 16, 5, 19, 4, 8, 28, 1 długości 15. W szczególności wynika stąd, że $[10^n + a]_{31} \neq 0$ dla $a \in \{1, 2, 4, 5, 7, 8, 9\}$ i dla każdego $n \in \mathbb{N}$.

Obliczmy na przykład $[10^{2022}]_{31}$. Najpierw dzielimy liczbę 2022 z resztą przez 15 uzyskując, że $2022 = 134 \cdot 15 + 12$. Wobec tego z wcześniejszych wyliczeń mamy, że $[10^{2022}]_{31} = [10^{12}]_{31} = 4$.

Ćwiczenie 2.36. Udowodnij, że ciąg reszt z dzielenia przez 11 liczb postaci 2^n jest okresowy i oblicz reszty $[2^{2022}]_{11}$ oraz $[2^{2023}]_{11}$.

Ćwiczenie 2.37. Dany jest ciąg liczbowy

$$(a_n) = (1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, 1, \ldots).$$

Wyznacz a_{2021}.

Ćwiczenie 2.38. W koszu jest 56 kamieni. Każdy z dwóch graczy bierze na przemian po k kamieni, gdzie $k \in \{1, 2, 3, 4, 5\}$. Wygrywa ten gracz, który zabiera ostatnie kamienie. Wyznacz strategię wygrywania dla gracza, który zaczyna jako pierwszy brać kamienie.

Rozdział 3

Liczby wymierne

Najpierw zostaną przedstawione niezbyt formalnie idee związane z prezentowaną dalej konstrukcją ciała liczb wymiernych. W pierścieniu liczb całkowitych $\mathbb{Z}$ nie jest wykonalne odwracanie wszystkich niezerowych elementów (na przykład nie istnieje $x \in \mathbb{Z}$ takie, że $2 \cdot x = 1$). W związku z tym powstaje naturalny problem: jak powiększyć zbiór $\mathbb{Z}$ za pomocą zbioru X rozłącznego z $\mathbb{Z}$ do zbioru $\mathbb{Z} \cup X$, w którym wykonalne będzie odwracanie wszystkich niezerowych elementów? Chodzi nam też o to, aby w nowym zbiorze było określone dodawanie i mnożenie, które mają te same własności, co dodawanie i mnożenie liczb całkowitych, to znaczy, aby dodawanie i mnożenie były przemienne, łączne, posiadały elementy neutralne oraz aby mnożenie było rozdzielne względem dodawania. Zależy nam także na tym, aby nowe dodawanie pokrywało się na zbiorze $\mathbb{Z}$ z naturalnym dodawaniem i aby nowe mnożenie pokrywało się na zbiorze $\mathbb{Z}$ z naturalnym mnożeniem. Pożądane jest też znalezienie minimalnego zbioru X, który spełnia te wszystkie warunki. Przyjęte założenia implikują wiele zależności, które muszą być spełnione w zbiorze $\mathbb{Z} \cup X$. Na przykład $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$, bo $2 \cdot 2 = 1 \cdot 4$ oraz $2 \cdot 6 = 4 \cdot 3$, itd. Ponadto $\frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \ldots$. Dalej, dla $a, b, c, d \in \mathbb{Z}$, gdzie $b, d \neq 0$: $\frac{a}{b} = \frac{c}{d} \iff a \cdot d = b \cdot c$. Nasuwa to pomysł zastosowania zasady abstrakcji do formalnego uzasadnienia przedstawionych wyżej idei.

3.1 Liczby wymierne jako klasy abstrakcji relacji równoważności w zbiorze $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$

W zbiorze $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ wprowadzamy relację R przyjmując dla dowolnych elementów $(a, b), (c, d)$ tego zbioru, że:

$$(a, b)R(c, d) \iff a \cdot d = c \cdot b. \tag{3.1}$$

Pokażemy, że R jest relacją równoważności. Ponieważ $a \cdot b = a \cdot b$ dla dowolnych $a \in \mathbb{Z}$, $b \in \mathbb{Z}\setminus\{0\}$, więc $(a, b)R(a, b)$ i relacja R jest zwrotna.

Niech $(a, b), (c, d) \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ będą takie, że $(a, b)R(c, d)$. Wtedy z (3.1), $a \cdot d = c \cdot b$, więc $c \cdot b = a \cdot d$, a zatem na mocy (3.1), $(c, d)R(a, b)$ i relacja R jest symetryczna.

Niech $(a, b), (c, d), (r, s) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ będą takie, że $(a, b)R(c, d)$ i $(c, d)R(r, s)$. Wtedy na mocy (3.1), $a \cdot d = c \cdot b$ i $c \cdot s = r \cdot d$. Stąd po pomnożeniu pierwszej równości przez s i drugiej przez b uzyskamy, że $ads = bcs$ i $bcs = dbr$, więc $ads = dbr$. Ponadto $d \neq 0$, więc po skróceniu przez d mamy $a \cdot s = r \cdot b$, co wobec (3.1) oznacza, że $(a, b)R(r, s)$. Wobec tego R jest relacją przechodnią.

W takim razie relacja R jest zwrotna, symetryczna i przechodnia, a więc R jest relacją równoważności w zbiorze $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Klasę abstrakcji elementu $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ będziemy nazywali **liczbą wymierną** i będziemy ją oznaczali symbolem $[a, b]$. Natomiast zbiór ilorazowy $[\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})]/R$ będziemy oznaczali symbolem $\mathbb{Q}$ i nazywali **zbiorem liczb wymiernych**. Zatem na mocy (3.1):

$$[a, b] = \{(x, y) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \ : \ a \cdot y = x \cdot b\}. \tag{3.2}$$

Dla dowolnych $(a, b), (x, y) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ mamy zatem, że

$$(x, y) \in [a, b] \iff a \cdot y = x \cdot b. \tag{3.3}$$

Stwierdzenie 3.1. *Dla dowolnych $x \in \mathbb{Z}$, $y, d \in \mathbb{Z} \setminus \{0\}$ zachodzi wzór:*

$$[xd, yd] = [x, y]. \tag{3.4}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Ponieważ $y, d \in \mathbb{Z} \setminus \{0\}$, więc $y \cdot d \in \mathbb{Z} \setminus \{0\}$ i $(xd, yd) \in \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Ponadto $(xd)y = x(yd)$, więc $(xd, yd)R(x, y)$ i wobec tego $[xd, yd] = [x, y]$. □

Ze wzoru (3.3) dla dowolnego $s \in \mathbb{Z} \setminus \{0\}$ uzyskujemy następujące wzory:

$$[0, 1] = \{(0, k) \ : \ k \in \mathbb{Z} \setminus \{0\}\} = [0, s], \tag{3.5}$$

$$[1, 1] = \{(k, k) \ : \ k \in \mathbb{Z} \setminus \{0\}\} = [s, s]. \tag{3.6}$$

Liczbę wymierną $[0, 1]$ będziemy nazywali **zerem** i oznaczali dalej symbolem 0, zaś liczbę $[1, 1]$ będziemy nazywali **jedynką** i oznaczali symbolem 1.

Ze wzoru (3.3) uzyskujemy od razu, że dla dowolnych $a, b \in \mathbb{Z}$:

$$[a, 1] = [b, 1] \iff a = b. \tag{3.7}$$

W szczególności $0 \neq 1$.

3.2 Dodawanie liczb wymiernych i jego własności

Sumę liczb wymiernych $[a, b]$ i $[c, d]$ określamy wzorem:

$$[a, b] + [c, d] = [ad + cb, bd]. \tag{3.8}$$

Pokażemy poprawność wzoru (3.8). Po pierwsze, skoro $b, d \in \mathbb{Z} \setminus \{0\}$, więc też $bd \in \mathbb{Z}\setminus\{0\}$; ponadto oczywiście $ad+cb \in \mathbb{Z}$. Po drugie, należy wykazać, że wzór (3.8) nie zależy od wyboru reprezentantów klas, czyli, że jeśli $(a, b)R(r, s)$ i $(c, d)R(u, v)$, to $(ad+cb, bd)R(rv+us, sv)$, ale na mocy (3.1), $as = rb$ i $cv = ud$, więc $(rv+us)bd = (rb)(vd)+(ud)(bs) = = asdv + cvbs = (ad + cb)sv$, skąd na mocy (3.1) uzyskujemy, że $(ad + cb, bd)R(rv + us, sv)$.

Ze wzoru (3.8) wynika od razu, że dla dowolnych $a, b \in \mathbb{Z}$:

$$[a, 1] + [b, 1] = [a + b, 1]. \tag{3.9}$$

Stwierdzenie 3.2. *Dla dowolnych $a, c \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$:*

$$[a, b] + [c, b] = [a + c, b]. \tag{3.10}$$

Dowód. Ze wzorów (3.8) i (3.4) mamy, że $[a, b]+[c, b] = [ab+cb, b\cdot b] =$ $= [(a + c) \cdot b, b \cdot b] = [a + c, b]$. □

Stwierdzenie 3.3. *Dodawanie liczb wymiernych jest przemienne, łączne i 0 jest elementem neutralnym tego działania, to znaczy dla dowolnych liczb wymiernych w, u, v:*

(i) $w + u = u + w$,

(ii) $w + (u + v) = (w + u) + v$,

(iii) $w + 0 = 0 + w = w$.

Dowód. Oznaczmy $w = [a, b]$, $u = [c, d]$ i $v = [r, s]$.

(i). Ze wzoru (3.8) i z własności dodawania i mnożenia liczb całkowitych mamy, że $u + w = [c, d] + [a, b] = [cb + ad, db] = [ad + cb, bd] =$ $= [a, b] + [c, d] = w + u$.

(ii). Ze wzoru (3.4), $[a, b] = [ads, bds]$, $[c, d] = [cbs, bds]$ i $[r, s] =$ $= [rbd, bds]$. Stąd i na mocy (3.10) oraz własności dodawania liczb całkowitych: $w + (u + v) = [a, b] + ([c, d] + [r, s]) = [ads, bds] + [cbs +$ $+rbd, bds] = [ads+cbs+rbd, bds]$ i $(w+u)+v = ([a, b]+[c, d])+[r, s] =$ $= [ads + cbs, bds] + [rbd, bds] = [ads + cbs + rbd, bds]$, co dowodzi (ii).

(iii). Ze wzoru (3.5), $[0, 1] = [0, b]$. Zatem na mocy (i) oraz (3.10), $w + 0 = 0 + w = 0 + [a, b] = [0, 1] + [a, b] = [0, b] + [a, b] = [0 + a, b] =$ $= [a, b] = w$. □

Stwierdzenie 3.4. *Dla dowolnej liczby wymiernej $[a, b]$ liczba wymierna $[-a, b]$ jest jedynym rozwiązaniem równania $[a, b] + [x, y] = 0$ w liczbach wymiernych.*

Dowód. Ze wzorów (3.10) i (3.5), $[a, b] + [-a, b] = [a + (-a), b] =$ $= [0, b] = [0, 1] = 0$. Niech teraz $[x, y]$ będzie taką liczbą wymierną, że $[a, b] + [x, y] = 0$. Wtedy $[-a, b] + ([a, b] + [x, y]) = [-a, b] + 0$, więc na mocy stwierdzenia 3.3, $([-a, b] + [a, b]) + [x, y] = [-a, b]$ oraz $[0, 1] + [x, y] = [-a, b]$ i $[x, y] = [-a, b]$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Ten jedyny element ze stwierdzenia 3.4 nazywamy **liczbą przeciwną do liczby** $w = [a, b]$ i oznaczamy symbolem $-w$. Zatem dla dowolnej liczby wymiernej $[a, b]$:

$$-[a, b] = [-a, b]. \tag{3.11}$$

Ponadto, dla liczby wymiernej w jest $(-w) + w = 0$, więc w jest liczbą przeciwną do liczby $(-w)$, czyli:

$$-(-w) = w \text{ dla dowolnej liczby wymiernej } w. \tag{3.12}$$

Odejmowanie liczb wymiernych definiujemy za pomocą dodawania liczby przeciwnej. Mianowicie dla dowolnych liczb wymiernych w, u przyjmujemy, że:

$$w - u = w + (-u). \tag{3.13}$$

Ze wzorów (3.11) i (3.8) w prosty sposób można wyprowadzić, że dla dowolnych liczb wymiernych $[a, b], [c, d]$ zachodzi wzór:

$$[a, b] - [c, d] = [ab - cb, bd]. \tag{3.14}$$

Stwierdzenie 3.5. *Dla dowolnych liczb wymiernych* w, u, v*:*
(i) jeżeli $w + v = u + v$*, to* $w = u$*,*
(ii) $-(w + u) = (-w) + (-u)$*,*
(iii) $(w - u) + u = w$*,*
(iv) $w - (u - v) = (w - u) + v$*.*

Dowód. (i). Niech $w + v = u + v$. Wtedy po dodaniu do obu stron tej równości elementu $-v$ i wykorzystaniu stwierdzenia 5.5 uzyskamy, że $(w+v)+(-v) = (u+v)+(-v)$, skąd $w+(v+(-v)) = u+(v+(-v))$, czyli $w + 0 = u + 0$, a zatem $w = u$.

(ii). Zgodnie ze stwierdzeniem 3.5 mamy, że $[w+u]+[(-w)+(-u)] = = [w+(-w)]+[u+(-u)] = 0+0 = 0$, więc $(-w)+(-u)$ jest elementem przeciwnym do $w + u$, czyli $-(w + u) = (-w) + (-u)$.

(iii). Ze wzoru (3.14) i ze stwierdzenia 3.5 mamy, że $(w - u) + u = = [w + (-u)] + u = w + [(-u) + u] = w + 0 = w$.

(iv). Ze wzoru (3.14) i ze stwierdzenia 3.5 oraz z (ii) i ze wzoru (3.12) mamy, że $w - (u - v) = w + [-(u + (-v))] = w + [(-u) + (-(-v))] = = w + [(-u) + v] = [w + (-u)] + v = (w - u) + v$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

3.3 Mnożenie liczb wymiernych i jego własności

Iloczyn liczb wymiernych $[a, b], [c, d]$ określamy za pomocą wzoru:

$$[a, b] \cdot [c, d] = [ac, bd]. \tag{3.15}$$

Pokażemy poprawność wzoru (3.15). Po pierwsze, skoro $b, d \in \mathbb{Z} \setminus \{0\}$, więc też $bd \in \mathbb{Z}\setminus\{0\}$; ponadto oczywiście $ac \in \mathbb{Z}$. Po drugie, należy wykazać, że wzór (3.15) nie zależy od wyboru reprezentantów klas, czyli, że jeśli $(a, b)R(r, s)$ i $(c, d)R(u, v)$, to $(ac, bd)R(ru, sv)$. Ponadto na mocy (3.1), $as = rb$ i $cv = ud$, więc $(ac)(sv) = (as)(cv) = (rb)(ud) = = (ru)(bd)$, skąd na mocy (3.1), $(ac, bd)R(ru, sv)$.

Stwierdzenie 3.6. *Mnożenie liczb wymiernych jest przemienne, łączne,* 1 *jest elementem neutralnym tego mnożenia i mnożenie liczb wymiernych jest rozdzielne względem dodawania liczb wymiernych, to znaczy dla dowolnych liczb wymiernych* w, u, v*:*

(i) $w \cdot u = u \cdot w$,
(ii) $w \cdot (u \cdot v) = (w \cdot u) \cdot v$,
(iii) $1 \cdot w = w \cdot 1 = w$,
(iv) $w \cdot (u + v) = w \cdot u + w \cdot v$.

Dowód. Oznaczmy: $w = [a, b]$, $u = [c, d]$ i $v = [r, s]$.

(i). Ze wzoru (3.15) i z przemienności mnożenia liczb całkowitych mamy, że $u \cdot w = [c, d] \cdot [a, b] = [ca, db] = [ac, bd] = [a, b] \cdot [c, d] = w \cdot u$.

(ii). Ze wzoru (3.15) i z łączności mnożenia liczb całkowitych mamy, że $w \cdot (u \cdot v) = [a, b] \cdot ([c, d] \cdot [r, s]) = [a, b] \cdot [cr, ds] = [a(cr), b(ds)] = = [(ac)r, (bd)s] = [ac, bd] \cdot [r, s] = ([a, b] \cdot [c, d]) \cdot [r, s] = (w \cdot u) \cdot v$.

(iii). Ze wzoru (3.15) i z (i) mamy, że $1 \cdot w = w \cdot 1 = [a, b] \cdot [1, 1] = = [a \cdot 1, b \cdot 1] = [a, b] = w$.

(iv). Ze wzoru (3.4), $u = [c, d] = [cs, ds]$ i $v = [r, s] = [rd, ds]$. Stąd i ze wzoru (3.10), $u + v = [c, d] + [r, s] = [cs + rd, ds]$, więc ze wzoru (3.15), $w \cdot (u + v) = [a, b] \cdot ([c, d] + [r, s]) = [a(cs + rd), bds] = [acs + +ard, bds]$. Podobnie, $w \cdot u + w \cdot v = [a, b] \cdot [c, d] + [a, b] \cdot [r, s] = [acs, bds] + +[ard, bds] = [acs + ard, bds]$. Zatem $w \cdot (u + v) = w \cdot u + w \cdot v$. □

Stwierdzenie 3.7. *Dla dowolnych liczb wymiernych* w, u, v*:*
(i) $w \cdot 0 = 0 \cdot w = 0$,
(ii) $(-w) \cdot u = w \cdot (-u) = -(w \cdot u)$,
(iii) $(-w) \cdot (-u) = w \cdot u$,
(iv) $w \cdot (u - v) = w \cdot u - w \cdot v$.

Dowód. Oznaczmy: $w = [a, b]$, $u = [c, d]$ i $v = [r, s]$. (i). Na mocy stwierdzenia 3.5 (i) oraz (3.15) i (3.5), $0 \cdot w = w \cdot 0 = [a, b] \cdot [0, 1] = [a \cdot 0, b \cdot 1] = [0, b] = [0, 1] = 0$.

(ii). Ze wzorów (3.11) i (3.15) mamy, że $(-w) \cdot u = [-a, b] \cdot [c, d] = [(-a) \cdot c, b \cdot d] = [-(a \cdot c), b \cdot d] = -[ac, bd] = -(w \cdot u)$ oraz $w \cdot (-u) = [a, b] \cdot [-c, d] = [a \cdot (-c), b \cdot d] = [-(ac), bd] = -[ac, bd] = -(w \cdot u$, co kończy dowód (ii).

(iii). Ze wzorów (3.11) i (3.15), $(-w) \cdot (-u) = [-a, b] \cdot [-c, d] = [(-a)(-b), cd] = [ac, bd] = w \cdot u$.

(iv). Z (3.14), $u - q = u + (-q)$. Stąd i ze stwierdzenia 3.5 (iv), $w \cdot (u - v) = w \cdot u + w \cdot (-v)$. Ponadto z (ii), $w \cdot (-v) = -(w \cdot v)$, więc $w \cdot (u - v) = w \cdot u + [-(w \cdot v)] = w \cdot u - w \cdot v$, na mocy (3.14). □

Stwierdzenie 3.8. *Dla dowolnej liczby wymiernej* $[a, b] \neq 0$ *liczba wymierna* $[b, a]$ *jest jedynym rozwiązaniem równania* $[a, b] \cdot [x, y] = 1$ *w liczbach wymiernych.*

Dowód. Jeśli $a = 0$, to na mocy wzoru (3.5), $[a, b] = [0, 1]$. Zatem $a \neq 0$. Stąd $[b, a]$ jest liczbą wymierną i na mocy wzoru (3.15), $[a, b] \cdot [b, a] = [ab, ba] = [ab, ab]$, skąd na mocy (3.4), $[a, b] \cdot [b, a] = [1, 1] = 1$. Jeśli $[x, y]$ jest liczbą wymierną taką, że $[a, b] \cdot [x, y] = 1$, to na mocy stwierdzenia 3.5 i pierwszej części naszego dowodu, $[b, a] \cdot ([a, b] \cdot [x, y]) = [b, a] \cdot 1 = [b, a]$ oraz $([b, a] \cdot [a, b]) \cdot [x, y] = 1 \cdot [x, y] = [x, y]$, czyli $[x, y] = [b, a]$. □

Liczbę wymierną $u = [x, y]$ ze stwierdzenie 3.6 nazywamy **liczbą odwrotną** do liczby $w = [a, b] \neq 0$. Zauważmy, że wtedy $u \neq 0$, bo inaczej $w \cdot u = [0, b] \neq [1, 1] = 1$. Liczbę u oznaczamy zazwyczaj symbolem w^{-1}. Ponieważ $u \cdot w = [1, 1]$ i $u \neq 0$, więc ze stwierdzenia 3.6 wynika, że w jest liczbą odwrotną do u, a zatem mamy wzór:

$$(w^{-1})^{-1} = w \text{ dla dowolnej liczby wymiernej } w \neq 0. \tag{3.16}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 3.9. *Iloczyn dwóch niezerowych liczb wymiernych jest liczbą wymierną niezerową. Ponadto dla dowolnych liczb wymiernych w, u, v:*

$$\text{jeśli } v \neq 0 \text{ i } w \cdot v = u \cdot v, \text{to } w = u, \tag{3.17}$$

$$\text{jeśli } w, u \neq 0, \text{ to } (w \cdot u)^{-1} = w^{-1} \cdot u^{-1}. \tag{3.18}$$

Dowód. Weźmy dowolne liczby wymierne $w, u \neq 0$ i załóżmy, że $w \cdot u = 0$. Wtedy wykorzystując założenie $u \neq 0$ możemy obie strony tej równości pomnożyć przez u^{-1} i na mocy stwierdzenia 3.5 uzyskamy, że $w = 0$, co prowadzi do sprzeczności. Zatem $w \cdot u \neq 0$.

Niech teraz $w \cdot v = u \cdot v$ i $v \neq 0$. Wtedy istnieje v^{-1} i $(w \cdot v) \cdot v^{-1} = (u \cdot v) \cdot v^{-1}$, więc z łączności mnożenia liczb wymiernych, $w \cdot (v \cdot v^{-1}) = u \cdot (v \cdot v^{-1})$, czyli $w \cdot 1 = u \cdot 1$ i $w = u$.

Niech $w, u \neq 0$. Wtedy, jak wiemy $w \cdot u \neq 0$. Ponadto ze stwierdzenia 3.6, $(w \cdot u) \cdot (w^{-1} \cdot u^{-1}) = (w \cdot w^{-1}) \cdot (u \cdot u^{-1}) = 1 \cdot 1 = 1$. Zatem na mocy stwierdzenia 3.8, $w^{-1} \cdot u^{-1}$ jest elementem odwrotnym do $w \cdot u$, czyli $(w \cdot u)^{-1} = w^{-1} \cdot u^{-1}$. □

Iloraz liczb wymiernych w i $u \neq 0$ określamy wzorem:

$$w : u = w \cdot u^{-1}. \tag{3.19}$$

Często zamiast $w : u$ piszemy $\frac{w}{u}$, a zatem $\frac{w}{u} = w \cdot u^{-1} = w \cdot \frac{1}{u}$, gdyż $\frac{1}{u} = 1 : u = 1 \cdot u^{-1} = u^{-1}$.

Stwierdzenie 3.10. *Dla dowolnych liczb wymiernych w, u, x, y, r takich, że $u, y \neq 0$ zachodzą wzory:*

(i) $\frac{w}{u} = \frac{x}{y} \iff w \cdot y = u \cdot x$,
(ii) jeżeli $r \neq 0$, *to* $\frac{w}{u} = \frac{w \cdot r}{u \cdot r}$,
(iii) $\frac{w}{u} + \frac{x}{u} = \frac{w+x}{u}$,
(iv) $\frac{w}{u} - \frac{x}{u} = \frac{w-x}{u}$,
(v) $r \cdot \frac{w}{u} = \frac{r \cdot w}{u}$,
(vi) $\frac{w}{u} + \frac{x}{y} = \frac{w \cdot y + x \cdot u}{u \cdot y}$,
(vii) $\frac{w}{u} - \frac{x}{y} = \frac{w \cdot y - x \cdot u}{u \cdot y}$,
(viii) $\frac{w}{u} \cdot \frac{x}{y} = \frac{w \cdot x}{u \cdot y}$,
(ix) jeśli $x \neq 0$, *to* $(\frac{x}{y})^{-1} = \frac{y}{x}$ *i* $\frac{w}{u} : \frac{x}{y} = \frac{w}{u} \cdot \frac{y}{x} = \frac{w \cdot y}{u \cdot x}$.

Dowód. (i). Jeśli $\frac{w}{u} = \frac{x}{y}$, to $w \cdot u^{-1} = x \cdot y^{-1}$, skąd po pomnożeniu obu stron tej równości przez $u \cdot y$ i wykorzystaniu wcześniej udowodnionych własności liczb wymiernych uzyskamy, że $w \cdot (u^{-1} \cdot u) \cdot y = x \cdot (y^{-1} \cdot y) \cdot u$, czyli $w \cdot 1 \cdot y = x \cdot 1 \cdot u$, a zatem $w \cdot y = u \cdot x$. Na odwrót, załóżmy, że $w \cdot y = u \cdot x$. Wykorzystując założenie, że $u, y \neq 0$ możemy obie strony tej równości pomnożyć przez $u^{-1} \cdot y^{-1}$ i podobnie jak wcześniej uzyskujemy, że $w \cdot (y \cdot y^{-1}) \cdot u^{-1} = (u \cdot u^{-1}) \cdot x \cdot y^{-1}$, czyli $w \cdot 1 \cdot u^{-1} = 1 \cdot x \cdot y^{-1}$, skąd $w \cdot u^{-1} = x \cdot y^{-1}$ a to oznacza, że $\frac{w}{u} = \frac{x}{y}$.

(ii). Ze stwierdzenia 3.8 mamy, że $u \cdot r \neq 0$. Ponadto $w \cdot (u \cdot r) = u \cdot (w \cdot r)$, więc z (i), $\frac{w}{u} = \frac{w \cdot r}{u \cdot r}$.

(iii). Z (3.19) i ze stwierdzenia 3.6 uzyskujemy, że $\frac{w}{u} + \frac{x}{u} = w \cdot u^{-1} + x \cdot u^{-1} = (w + x) \cdot u^{-1} = \frac{w+x}{u}$.

(iv). Na mocy (iii) i stwierdzenia 3.5, $\frac{w-x}{u} + \frac{x}{u} = \frac{(w-x)+x}{u} = \frac{w}{u}$, skąd $\frac{w}{u} - \frac{x}{u} = \frac{w-x}{u}$.

(v). Z (3.19) i ze stwierdzenia 3.6 mamy, że $r \cdot \frac{w}{u} = r \cdot (w \cdot u^{-1}) = (r \cdot w) \cdot u^{-1} = \frac{r \cdot w}{u}$.

(vi). Z (ii), $\frac{w}{u} = \frac{w \cdot y}{u \cdot y}$ i $\frac{x}{y} = \frac{x \cdot u}{u \cdot y}$, więc na mocy (iii), $\frac{w}{u} + \frac{x}{y} = \frac{w \cdot y + x \cdot u}{u \cdot y}$.

(vii). Z (ii), $\frac{w}{u} = \frac{w \cdot y}{u \cdot y}$ i $\frac{x}{y} = \frac{x \cdot u}{u \cdot y}$, więc na mocy (iv), $\frac{w}{u} - \frac{x}{y} = \frac{w \cdot y - x \cdot u}{u \cdot y}$.

(viii). Ze stwierdzenia 3.8, $u \cdot y \neq 0$ oraz $(u \cdot y)^{-1} = u^{-1} \cdot y^{-1}$. Zatem z (3.19) i ze stwierdzenia 3.6, $\frac{w}{u} \cdot \frac{x}{y} = w \cdot u^{-1} \cdot x \cdot y^{-1} = (w \cdot x) \cdot (u^{-1} \cdot y^{-1}) = (w \cdot u) \cdot (u \cdot y)^{-1} = \frac{w \cdot x}{u \cdot y}$.

(ix). Z (3.19) oraz ze stwierdzenia 3.6 uzyskujemy, że $\frac{x}{y} \cdot \frac{y}{x} = x \cdot y^{-1} \cdot y \cdot x^{-1} = [x \cdot x^{-1}] \cdot [y \cdot y^{-1}] = 1 \cdot 1$, więc na mocy stwierdzenia 3.8, $\frac{y}{x}$ jest elementem odwrotnym do $\frac{x}{y}$, czyli $(\frac{x}{y})^{-1} = \frac{y}{x}$. Stąd i ze wzoru (3.19), $\frac{w}{u} : \frac{x}{y} = \frac{w}{u} \cdot \frac{y}{x} = \frac{w}{u} \cdot (\frac{x}{y})^{-1} = \frac{w}{u} \cdot \frac{y}{x} = \frac{w \cdot y}{u \cdot x}$, na mocy (viii). □

3.4 Uporządkowanie liczb wymiernych

Relację mniejszości $<$ w zbiorze liczb wymiernych określamy przyjmując, że dla dowolnych $[a, b], [c, d] \in \mathbb{Q}$:

$$[a, b] < [c, d] \iff abd^2 < cb^2d. \tag{3.20}$$

Udowodnimy, że wzór (3.20) nie zależy od wyboru reprezentantów klas abstrakcji, to znaczy jeżeli $(a,b)R(r,s)$ i $(c,d)R(u,v)$ i $abd^2 < cb^2d$, to $rsv^2 < us^2v$. Z naszych założeń mamy, że, $as = rb$ i $cv = ud$ i $v^2s^2 > 0$, gdyż $v, s \in \mathbb{Z}\setminus\{0\}$, więc po pomnożeniu nierówności $abd^2 < cb^2d$ przez v^2s^2 uzyskamy, że $(as)sv^2bd^2 < (cv)s^2vb^2d$, skąd $rb^2sv^2d^2 < ud^2s^2vb^2$. Dalej, $b, d \in \mathbb{Z}\setminus\{0\}$, więc $b^2d^2 > 0$ i po skróceniu przez b^2d^2 uzyskujemy, że $rsv^2 < us^2v$.

Stwierdzenie 3.11. *Dla dowolnych liczb wymiernych x, y, z:*
(i) $\sim (x < x)$,
(ii) $[x < y \text{ i } y < z] \Rightarrow x < z$,
(iii) $x = y$ *albo* $x < y$ *albo* $y < x$,
(iv) $x < y \iff x - y < 0$,
(v) $x < y \iff x + z < y + z$.

Dowód. Weźmy dowolne $x, y, z \in \mathbb{Q}$. Wtedy istnieją $a, b, c, d, r, s \in \mathbb{Z}$ takie, że $x = [a,b]$, $y = [c,d]$ i $z = [r,s]$ oraz $b, d, s \neq 0$. Ponieważ nie jest prawdą, że $abb^2 < ab^2b$, więc ze wzoru (3.20) mamy, że $\sim (x < x)$, co dowodzi (i).

Dla dowodu (ii) załóżmy, że $x < y$ i $y < z$. Wtedy z (3.20), $abd^2 < cb^2d$ i $cds^2 < rd^2s$, skąd po pomnożeniu pierwszej nierówności przez $s^2 > 0$ i drugiej przez $b^2 > 0$ uzyskamy, że $abd^2s^2 < cb^2ds^2$ i $cb^2ds^2 < rb^2d^2s$, więc $abd^2s^2 < rb^2d^2s$. Ponadto $d \neq 0$, więc $d^2 > 0$ i po skróceniu przez d^2, $abs^2 < rb^2s$, co oznacza, że $x < z$.

(iii). Jeśli $x = y$, to na mocy (i), $\sim (x < y)$ i $\sim (y < x)$. Jeśli $x < y$ i $y < x$, to na mocy (ii), $x < x$, co przeczy (i). Wobec tego warunki: $x = y$, $x < y$ i $y < x$ wykluczają się wzajemnie. Ponadto ze stwierdzenia 2.11 wiemy, że $abd^2 < cb^2d$ lub $cb^2d < abd^2$ lub $abd^2 = cb^2d$, co wobec (3.20) i tego, że $b, d \neq 0$ oznacza, że $x < y$ lub $y < x$ lub $ad = cb$, czyli $x = y$, więc ostatecznie mamy, że $x = y$ albo $x < y$ albo $y < x$.

(iv). Ponieważ $0 = [0,1]$ i na mocy wzoru (3.14), $x - y = [ad - cb, bd]$, więc ze wzoru (3.20), $x - y < 0 \iff [ad - cb, bd] < [0,1]$, czyli $x - y < 0 \iff (ad - cb)bd \cdot 1^2 < 0 \cdot b^2d^2 \cdot 1$, skąd $x - y < 0$ wtedy i tylko wtedy, gdy $(ad - cb)bd < 0 \iff abd^2 - cb^2d < 0 \iff x < y$, co kończy dowód.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

(v). Ze wzoru (3.13) i ze stwierdzenia 3.5 (iv), $(x+z)-(y+z) = x+z+(-y)+(-z) = [x+(-y)]+[z+(-z)] = (x-y)+0 = x-y$. Wobec tego na mocy (iv), $x < y \iff x+z < y+z$. □

Definicja 3.12. W zbiorze $\mathbb{Q}$ określamy przy użyciu relacji $<$ relacje: $>$, $\leqslant$ i $\geqslant$ przyjmując dla dowolnych $x, y \in \mathbb{Q}$, że:
(i) $x > y \iff y < x$,
(ii) $x \leqslant y \iff (x = y \text{ lub } x < y)$,
(iii) $x > y \iff (x = y \text{ lub } y < x)$.

Z definicji 3.12 i ze stwierdzenia 3.11 mamy od razu

Wniosek 3.13. *Dla dowolnych liczb wymiernych x, y, z:*
(i) $x \leqslant x$,
(ii) $(x \leqslant y \text{ i } y \leqslant z) \Rightarrow x \leqslant z$,
(iii) $x \leqslant y$ *lub* $y \leqslant x$,
(iv) $x \leqslant y \iff x - y \leqslant 0$,
(v) $(x \leqslant y \text{ i } y \leqslant x) \Rightarrow x = y$.

Stwierdzenie 3.14. *Dla dowolnych $a, b \in \mathbb{Z}$, $b \neq 0$:*
(i) $[a, b] > 0 \iff ab > 0$,
(ii) $[a, b] < 0 \iff ab < 0$,
(iii) $[a, b] = 0 \iff a = 0$.

Dowód. Ponieważ $0 = [0, 1]$, więc na mocy (3.20) i definicji 3.12, $[a, b] > 0 \iff [0, 1] < [a, b] \iff 0 < ab \iff ab > 0$, co dowodzi (i). Analogicznie, $[a, b] < 0 \iff [a, b] < [0, 1] \iff ab < 0$, co dowodzi (ii). Ponadto, $[a, b] = 0 \iff [a, b] = [0, 1] \iff a \cdot 1 = 0 \cdot b \iff a = 0$, co dowodzi (iii). □

Ze wzoru (3.11) i ze stwierdzenia 3.14 od razu wynika, że dla dowolnego $x \in \mathbb{Q}$:

$$[x < 0 \iff -x > 0] \text{ oraz } [x > 0 \iff -x < 0]. \tag{3.21}$$

Liczby wymierne mniejsze od 0 będziemy nazywali **ujemnymi liczbami wymiernymi**, zaś liczby wymierne większe od 0 będziemy nazywali **dodatnimi liczbami wymiernymi**.

Stwierdzenie 3.15. *Dla dowolnych liczb wymiernych x, y:*
(i) jeżeli $x > 0$ i $y > 0$, to $x \cdot y > 0$,
(ii) jeżeli $x > 0$ i $y < 0$, to $x \cdot y < 0$,
(iii) jeżeli $x < 0$ i $y < 0$, to $x \cdot y > 0$.

Dowód. Istnieją $a, b, c, d \in \mathbb{Z}$ takie, że $b, d \neq 0$ i $x = [a, b]$ oraz $y = [c, d]$. Wtedy ze wzoru (3.15), $x \cdot y = [ac, bd]$.

(i). Ze stwierdzenia 3.14 (i) mamy, że $ab > 0$ i $cd > 0$, skąd $abcd > 0$, więc znowu ze stwierdzenie 3.14 (i), $x \cdot y > 0$.

(ii). Ze stwierdzenia 3.14 mamy, że $ab > 0$ i $cd < 0$, skąd $abcd < 0$, więc znowu ze stwierdzenie 3.14, $x \cdot y < 0$.

(iii). Ze stwierdzenia 3.14 mamy, że $ab < 0$ i $cd < 0$, skąd $abcd > 0$, więc znowu ze stwierdzenie 3.14, $x \cdot y > 0$. □

Stwierdzenie 3.16. *Dla dowolnych liczb wymiernych x, y, z:*
(i) jeżeli $x < y$ i $z > 0$, to $x \cdot z < y \cdot z$,
(ii) jeżeli $x < y$ i $z < 0$, to $x \cdot z > y \cdot z$.

Dowód. (i). Z naszych założeń i ze stwierdzenia 3.11 (iv) mamy, że $x - y < 0$. Zatem ze stwierdzenia 3.15 (ii), $z \cdot (x - y) < 0$, skąd na mocy stwierdzenia 3.7, $z \cdot x - z \cdot y < 0$. Wobec tego na mocy stwierdzenia 3.11 (iv), $z \cdot x < z \cdot y$.

(ii) Z naszych założeń i ze stwierdzenia 3.11 (iv), $x - y < 0$. Zatem ze stwierdzenia 3.15 (iii), $z \cdot (x - y) > 0$, skąd na mocy stwierdzenia 3.7, $z \cdot x - z \cdot y > 0$. Wobec tego na mocy stwierdzenia 3.11 (iv), $z \cdot x > z \cdot y$. □

Stwierdzenie 3.17. *Dla dowolnych liczb wymiernych x, y, z:*
(i) jeżeli $x \cdot z < y \cdot z$ i $z > 0$, to $x < y$,
(ii) jeżeli $x \cdot z < y \cdot z$ i $z < 0$, to $x > y$.

Dowód. (i). Załóżmy, że $x \cdot z < y \cdot z$ i $z > 0$. Wtedy $z \neq 0$ i ze stwierdzenia 3.11 (iii), $x = y$ lub $y < x$ lub $x < y$. W pierwszym przypadku, $x \cdot z = y \cdot z$, co prowadzi do sprzeczności, gdyż $x \cdot z < y \cdot z$. W drugim przypadku, na mocy stwierdzenia 3.16 (i), $y \cdot z < x \cdot x$, co prowadzi do sprzeczności, bo $x \cdot z < y \cdot z$. Wobec tego musi być $x < y$.

(ii). Załóżmy, że $x \cdot z < y \cdot z$ i $z < 0$. Wtedy $z \neq 0$ i ze stwierdzenia 3.11 (iii), $x = y$ lub $x < y$ lub $x > y$. W pierwszym przypadku, $x \cdot z = y \cdot z$, co prowadzi do sprzeczności, gdyż $x \cdot z < y \cdot z$. W drugim przypadku, na mocy stwierdzenia 3.16 (ii), $y \cdot z < x \cdot z$, co prowadzi do sprzeczności, bo $x \cdot z < y \cdot z$. Wobec tego musi być $x > y$. □

Stwierdzenie 3.18. *Dla dowolnych liczb wymiernych x, y, u, v:*

$$[x < y \text{ i } u < v] \Rightarrow x + u < y + v.$$

Dowód. Załóżmy, że $x < y$ i $u < v$. Wtedy na mocy stwierdzenia 3.11 (v), po dodaniu do obu stron pierwszej nierówności liczby u oraz po dodaniu do obu stron drugiej nierówności liczby y uzyskamy, że $x + u < y + u$ i $y + u < y + v$. Stąd na mocy stwierdzenia 3.11 (ii), $x + u < y + v$. □

3.5 Liczby całkowite jako szczególne liczby wymierne

Z podanej przez nas konstrukcji liczb wymiernych wynika, że dla dowolnych liczb całkowitych a i b:

$$[a, 1] = [b, 1] \iff a = b,$$

$$[a, 1] + [b, 1] = [a + b, 1],$$

$$-[a, 1] = [-a, 1],$$

$$[a, 1] - [b, 1] = [a - b, 1],$$

$$[a, 1] \cdot [b, 1] = [ab, 1],$$

$$[a, 1] < [b, 1] \iff a < b.$$

Wobec tego liczbę wymierną $[a, 1]$ możemy utożsamić z liczbą całkowitą a:

$$[a, 1] \equiv a. \tag{3.22}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Przy tym utożsamieniu zbiór liczb całkowitych $\mathbb{Z}$ jest podzbiorem zbioru $\mathbb{Q}$ liczb wymiernych. Ponadto relacja mniejszości $<$ w $\mathbb{Q}$ jest rozszerzeniem relacji mniejszości w $\mathbb{Z}$ oraz dodawanie i mnożenie liczb wymiernych są rozszerzeniami dodawania i mnożenia liczb całkowitych. Dodatkowo dodawanie i mnożenie liczb wymiernych spełniają wszystkie warunki postawione przez nas we wstępie do tego rozdziału (z algebraicznego punktu widzenia możemy powiedzieć, że $\mathbb{Q}$ z dodawaniem i mnożeniem tworzy **ciało**, zaś $\mathbb{Z}$ jest jego **podpierścieniem**). Nietrudno jest też zauważyć, że tak skonstruowany zbiór $\mathbb{Q}$ jest „minimalny". Rzeczywiście, dowolna liczba wymierna $w = [a, b]$ dla pewnych $a, b \in \mathbb{Z}$ takich, że $b \neq 0$, więc na mocy wzoru (3.15) i stwierdzenia 3.8, $[a, b] = [a, 1] \cdot [1, b] = [a, 1] \cdot [b, 1]^{-1} \equiv a \cdot b^{-1}$. Wobec tego:

$$[a, b] \equiv a \cdot b^{-1}. \tag{3.23}$$

A zatem jeżeli S jest ciałem zawierającym $\mathbb{Z}$ jako podpierścień, to dla dowolnych $a, b \in \mathbb{Z}$ takich, że $b \neq 0$ musi być $b^{-1} \in S$ oraz $a \cdot b^{-1} \in S$, skąd $\mathbb{Q} \subseteq S$.

W naszych dalszych rozważaniach nie będziemy stosowali zapisu $[a, b]$ dla liczb wymiernych, lecz będziemy go zastępowali ułamkiem $\frac{a}{b}$. Wszystkie udowodnione przez nas rezultaty można teraz zapisać w tej nowej, znanej ze szkoły, notacji. Zauważmy, że $[a, b] = [-a, -b]$, przy czym $b > 0$ lub $-b > 0$ na mocy (3.21), więc uwzględniając (3.23) mamy następujący

Wniosek 3.19. *Każdą liczbę wymierną można zapisać w postaci* $\frac{a}{b}$*, gdzie* $a \in \mathbb{Z}$ *i* $b \in \mathbb{N}$.

Stwierdzenie 3.20. *Między każdymi dwiema różnymi liczbami wymiernymi leży zawsze pewna liczba wymierna. Mianowicie, jeśli* x, y *są liczbami wymiernymi i* $x < y$*, to* $x < \frac{x+y}{2} < y$.

Dowód. Z udowodnionych własności liczb wymiernych mamy, że $x < \frac{x+y}{2} \iff 2x < x + y \iff x < y$ oraz $\frac{x+y}{2} < y \iff x + y < 2y \iff x < y$. Wobec tego $x < \frac{x+y}{2} < y$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 4

Ciała abstrakcyjne

4.1 Działanie w zbiorze

Z dowolnych przedmiotów a i b (niekoniecznie różnych) można utworzyć **parę uporządkowaną** $(a, b) = \{\{a\}, \{a, b\}\}$ o poprzedniku a i następniku b. Pary (a, b) i (c, d) uważamy za równe wtedy i tylko wtedy, gdy $a = c$ i $b = d$, to znaczy gdy mają równe poprzedniki i równe następniki. Mając dwa zbiory A i B możemy utworzyć zbiór $A \times B$ złożony ze wszystkich par uporządkowanych (a, b) o poprzedniku $a \in A$ i następniku $b \in B$.

Definicja 4.1. Działaniem w niepustym zbiorze A nazywamy każde odwzorowanie zbioru $A \times A$ w zbiór A. Jeżeli $\circ$ jest działaniem w zbiorze A i $a, b \in A$, to $\circ((a, b))$ oznaczamy przez $a \circ b$ i nazywamy **wynikiem działania** $\circ$ na parze (a, b).

Zatem w niepustym zbiorze A jest określone działanie $\circ$, jeśli dowolnej parze uporządkowanej (a, b), gdzie $a, b \in A$, został przyporządkowany w jakiś sposób (na przykład wzorem) za pomocą odwzorowania (funkcji, przekształcenia) $\circ$ dokładnie jeden element zbioru A oznaczany symbolem $a \circ b$.

Definicja 4.2. Niech $\circ$ będzie działaniem w zbiorze A. Mówimy, że

(1) działanie $\circ$ jest **łączne**, jeżeli $(a \circ b) \circ c = a \circ (b \circ c)$ dla dowolnych $a, b, c \in A$,
(2) działanie $\circ$ jest **przemienne**, jeżeli $a \circ b = b \circ a$ dla dowolnych $a, b \in A$,
(3) $e \in A$ jest **elementem neutralnym** działania $\circ$, jeżeli $e \circ a = a \circ e = a$ dla każdego $a \in A$.

Zauważmy, że jeśli $e, f \in A$ są elementami neutralnymi działania $\circ$ w zbiorze A, to $e = f$. Rzeczywiście, $a \circ e = a$ dla $a \in A$, więc $f \circ e = f$ oraz $f \circ a = a$ dla $a \in A$, więc $f \circ e = e$. Stąd $f = e$. Wobec tego **każde działanie w zbiorze A posiada co najwyżej jeden element neutralny**.

Twierdzenie 4.3. *Jeżeli $\circ$ jest działaniem łącznym w zbiorze A, to wynik tego działania na dowolnym układzie elementów $a_1, a_2, \ldots, a_n$ należących do zbioru A nie zależy od sposobu rozstawienia nawiasów.*

Dowód. Zastosujemy indukcję względem n przy dowolnych elementach $a_1, \ldots, a_n \in A$. Dla $n = 1$ przyjmijmy formalnie, że wynik działania $\circ$ na układzie a_1 jest równy a_1. Dla $n = 2$ teza też zachodzi, bo mamy tylko jedną możliwość: $a_1 \circ a_2$. Dla $n = 3$ mamy dwie możliwości rozstawienia nawiasów w układzie a_1, a_2, a_3: $a_1 \circ (a_2 \circ a_3)$ i $(a_1 \circ a_2) \circ a_3$, które prowadzą do tego samego wyniku na mocy łączności działania $\circ$ i ten wynik oznaczymy przez $a_1 \circ a_2 \circ a_3$.

Niech teraz $n > 3$ będzie taką liczbą naturalną, że dla każdego naturalnego $k < n$ wynik działania $\circ$ na dowolnych elementach $x_1, \ldots, x_k \in A$ nie zależy od sposobu rozstawienia nawiasów i jego wartość oznaczmy symbolem $x_1 \circ \ldots \circ x_k$. Weźmy dowolne $a_1, a_2, \ldots, a_n \in A$. Niech a będzie wynikiem działania $\circ$ na układzie elementów $a_1, a_2, \ldots, a_n$ przy pewnym rozstawieniu nawiasów. Jeśli w tym rozstawieniu nawiasów za elementem a_n z prawej strony stoi nawias), to $a = b \circ (\ldots \circ a_n)\ldots)$, gdzie b jest wynikiem działania $\circ$ na układzie $a_1, \ldots, a_k$ dla pewnego naturalnego $k < n - 1$, zaś $c = (\ldots \circ a_n)\ldots)$ jest wynikiem działania $\circ$ na układzie $a_{k+1}, \ldots, a_n$. Zatem na mocy założenia indukcyjnego i łączności działania $\circ$ mamy, że $a = b \circ ((a_{k+1} \circ \ldots \circ a_{n-1}) \circ a_n) = (b \circ (a_{k+1} \circ \ldots \circ a_{n-1})) \circ a_n = (a_1 \circ \ldots \circ a_{n-1}) \circ a_n$. Jeśli zaś za elementem

a_n nie ma nawiasu), to $a = c \circ a_n$, gdzie c jest wynikiem działania $\circ$ na układzie $a_1, \ldots, a_{n-1}$ przy pewnym rozstawieniu nawiasów. Zatem z założenia indukcyjnego c nie zależy od sposobu rozstawienia nawiasów, więc $c = a_1 \circ \ldots \circ a_{n-1}$ i $a = (a_1 \circ \ldots \circ a_{n-1}) \circ a_n$. Kończy to dowód tego, że wynik działania $\circ$ na układzie elementów $a_1, a_2, \ldots, a_n$ nie zależy od sposobu rozstawienia nawiasów. □

Twierdzenie 4.3 pozwala na pomijanie nawiasów dla działania łącznego $\circ$ i używanie zapisu $a_1 \circ a_2 \circ \ldots \circ a_n$ dla dowolnej liczby naturalnej n. Ponadto wówczas dla $a \in A$ i $n \in \mathbb{N}$ możemy stosować zapis $a^n = \underbrace{a \circ a \circ \ldots \circ a}_{n}$ (oczywiście $a^1 = a$).

Wniosek 4.4. *Jeżeli $\circ$ jest działaniem łącznym w zbiorze A, to dla dowolnego $a \in A$ i dla dowolnych $n, m \in \mathbb{N}$:*
(i) $a^n \circ a^m = a^{n+m}$ oraz (ii) $(a^n)^m = a^{nm}$.

Dowód. (i). W zapisie $a^n \circ a^m$ element a występuje dokładnie $n + m$ razy, więc na mocy twierdzenia 4.3, $a^n \circ a^m = a^{n+m}$.

(ii). W zapisie $(a^n)^m$ element a^n występuje dokładnie m razy, zaś w zapisie a^n element a występuje dokładnie n razy. Zatem w zapisie $(a^n)^m$ element a występuje dokładnie nm razy, więc na mocy twierdzenia 4.3, $(a^n)^m = a^{nm}$. □

Wniosek 4.5. *Niech $\circ$ będzie działaniem łącznym w zbiorze A i niech $a, b \in A$ będą takie, że $a \circ b = b \circ a$. Wtedy dla dowolnych $m, n \in \mathbb{N}$:*
(i) $a \circ b^m = b^m \circ a$, (ii) $a^n \circ b^m = b^m \circ a^n$, (iii) $(a \circ b)^n = a^n \circ b^n$.

Dowód. (i). Stosujemy indukcję względem m. Dla $m = 1$ teza wynika wprost z założenia. Załóżmy, że dla pewnego $m \in \mathbb{N}$ jest $a \circ b^m = b^m \circ a$. Wtedy na mocy wniosku 4.4, $b^{m+1} = b^m \circ b$, więc na mocy łączności $\circ$ i założenia indukcyjnego, $a \circ b^{m+1} = (a \circ b^m) \circ b = (b^m \circ a) \circ b = b^m \circ (a \circ b) = b^m \circ (b \circ a) = (b^m \circ b) \circ a = b^{m+1} \circ a$. Zatem teza zachodzi dla liczby $m + 1$.

Podpunkt (ii) wynika od razu z (i). W dowodzie (iii) stosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista. Załóżmy, że teza

zachodzi dla pewnego $n \in \mathbb{N}$. Wtedy na mocy twierdzenia 4.3 i założenia indukcyjnego oraz (i), $(a \circ b)^{n+1} = (a \circ b)^n \circ (a \circ b) = a^n \circ b^n \circ a \circ b = a^n \circ a \circ b^n \circ b = a^{n+1} \circ b^{n+1}$, czyli teza zachodzi dla liczby $n+1$. □

Twierdzenie 4.6. *Jeżeli $\circ$ jest działaniem łącznym i przemiennym w zbiorze A, to wynik tego działania na dowolnym układzie elementów $a_1, \ldots, a_n$ należących do zbioru A nie zależy od kolejności tych elementów.*

Dowód. Indukcja względem n. Dla $n = 1$ teza jest oczywista, a dla $n = 2$ teza wynika z przemienności działania $\circ$. Niech teraz teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ i niech $a_1, \ldots, a_n, a_{n+1} \in A$. Niech $b_1, \ldots, b_{n+1}$ będzie dowolną permutacją ciągu $a_1, \ldots, a_n, a_{n+1}$. Załóżmy najpierw, że $a_1 = b_i$ dla pewnego $i > 1$. Wtedy z przemienności i łączności działania $\circ$: $b_1 \circ \ldots \circ b_{i-1} \circ b_i \circ b_{i+1} \circ \ldots \circ b_{n+1} = b_i \circ (b_1 \circ \ldots \circ b_{i-1} \circ b_{i+1} \circ \ldots \circ b_{n+1})$. Ponadto $b_i = a_1$ oraz ciąg $b_2, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{n+1}$ jest permutacją ciągu $a_2, \ldots, a_{n+1}$, więc z założenia indukcyjnego $b_1 \circ \ldots \circ b_{i-1} \circ b_{i+1} \circ \ldots \circ b_{n+1} = a_2 \circ \ldots \circ a_{n+1}$. Zatem w tym przypadku $b_1 \circ b_2 \circ \ldots \circ b_{n+1} = a_1 \circ a_2 \circ \ldots \circ a_{n+1}$. Jeżeli zaś $b_1 = a_1$, to z założenia indukcyjnego $b_2 \circ \ldots \circ b_{n+1} = a_2 \circ \ldots \circ a_{n+1}$, więc też $b_1 \circ b_2 \circ \ldots \circ b_{n+1} = a_1 \circ a_2 \circ \ldots \circ a_{n+1}$.

Stąd na mocy zasady indukcji teza zachodzi dla każdego $n \in \mathbb{N}$. □

4.2 Określenie ciała

Definicja 4.7. Niech K będzie zbiorem posiadającym **co najmniej dwa elementy**. Niech $+$ i $\cdot$ będą działaniami w zbiorze K zwanymi odpowiednio **dodawaniem** i **mnożeniem** oraz niech będą wyróżnione w zbiorze K dwa elementy nazywane **zerem** i **jedynką**, i oznaczane symbolami 0 i 1 odpowiednio. Powiemy, że K z tymi działaniami i wyróżnionymi elementami 0, 1 jest **ciałem**, jeżeli spełnione są następujące warunki (aksjomaty ciała):

A1. $a + b = b + a$ dla dowolnych $a, b \in K$.

A2. $(a + b) + c = a + (b + c)$ dla dowolnych $a, b, c \in K$.

A3. $a + 0 = a$ dla każdego $a \in K$.

A4. Dla każdego $a \in K$ istnieje $x \in K$ takie, że $a + x = 0$.
A5. $a \cdot b = b \cdot a$ dla dowolnych $a, b \in K$.
A6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dla dowolnych $a, b, c \in K$.
A7. $a \cdot 1 = a$ dla każdego $a \in K$.
A8. $a \cdot (b + c) = a \cdot b + a \cdot c$ dla dowolnych $a, b, c \in K$.
A9. Dla każdego $a \in K$, $a \neq 0$, istnieje $y \in K$ takie, że $a \cdot y = 1$.

Zatem, ciało jest uporządkowanym układem $(K, +, \cdot, 0, 1)$, w którym K jest zbiorem o co najmniej dwóch elementach, $0, 1 \in K$ są wyróżnionymi elementami zbioru K (nie muszą to być liczby całkowite 0 i 1), zaś $+$ i $\cdot$ są działaniami w K spełniającymi aksjomaty **A1-A9**. Zauważmy, że aksjomaty **A1** i **A5** mówią, że dodawanie oraz mnożenie są działaniami przemiennymi. Aksjomaty **A2** i **A6** oznajmiają, że dodawanie i mnożenie są łączne. Z aksjomatów **A2** i **A3** wynika, że 0 jest elementem neutralnym dodawania, zaś z aksjomatów **A5** i **A7** wnioskujemy, że 1 jest elementem neutralnym mnożenia. Aksjomat **A8** mówi, że mnożenie jest rozdzielne względem dodawania. Ostatni aksjomat **A9**, można wypowiedzieć tak: w ciele każdy niezerowy element jest odwracalny. Wobec tego dodawanie i mnożenie w dowolnym ciele są formalnym uogólnieniem zwykłego dodawania i mnożenia liczb rzeczywistych. Ta uwaga może pomóc przy zapamiętywaniu aksjomatów ciała!

Jeśli znane są działania $+$ i $\cdot$ w ciele $(K, +, \cdot, 0, 1)$ i nie prowadzi to do nieporozumień, to takie ciało będziemy oznaczali symbolem K. Należy jednak pamiętać, że ciało, to coś więcej niż sam zbiór K!

Podstawowym i jednocześnie wzorcowym przykładem ciała jest **ciało liczb wymiernych** (ze zwykłym dodawaniem i mnożeniem liczb). Oznaczamy je przez $\mathbb{Q}$.

Zbiór wszystkich liczb całkowitych $\mathbb{Z}$ ze zwykłym dodawaniem i mnożeniem liczb nie tworzy ciała, bo nie spełnia aksjomatu **A9**, gdyż na przykład $2 \cdot y \neq 1$ dla każdego $y \in \mathbb{Z}$.

Uwaga 4.8. Niech $(K, +, \cdot, 0, 1)$ będzie dowolnym ciałem. Wówczas na mocy **A2** i twierdzeń 4.3 i 4.6, dla dowolnego $n \in \mathbb{N}$ i dla dowolnych $a_1, a_2, \ldots, a_n$ wynik dodawania na tym układzie elementów

nie zależy od sposobu rozstawienia nawiasów i od kolejności składników. Ten wspólny wynik będziemy oznaczali przez $a_1 + a_2 + \ldots + a_n$ i nazywali **sumą** elementów $a_1, a_2, \ldots, a_n$. Ponadto, dla $a \in K$ i $n \in \mathbb{N}$, zamiast $\underbrace{a + a + \ldots + a}_{n}$ będziemy pisali na.

Podobnie, na mocy **A6** i twierdzeń 4.3 i 4.6, wynik mnożenia na układzie elementów $a_1, a_2, \ldots, a_n$ nie zależy od sposobu rozstawienia nawiasów i kolejności czynników; będzie on oznaczany symbolem $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ i nazywany **iloczynem** elementów $a_1, a_2, \ldots, a_n$. Ponadto, dla $a \in K$ i $n \in \mathbb{N}$, zamiast $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n}$ będziemy pisali a^n.

Następująca własność nazywana jest prawami skracania równości w ciele :

Własność 4.9. *Dla dowolnych elementów a, b, c ciała K:*
(a) jeśli $a + c = b + c$, to $a = b$,
(b) jeśli $a \cdot c = b \cdot c$ i $c \neq 0$, to $a = b$.

Dowód. (a). Z **A4** istnieje $t \in K$ takie, że $c + t = 0$, więc $(a + c) + t = (b + c) + t$, skąd z **A2**: $a + (c + t) = b + (c + t)$, czyli $a + 0 = b + 0$ i z **A3**: $a = b$.
(b). Z **A9** istnieje $y \in K$ takie, że $c \cdot y = 1$, więc $(a \cdot c) \cdot y = (b \cdot c) \cdot y$, skąd z **A6**, $a \cdot (c \cdot y) = b \cdot (c \cdot y)$, czyli $a \cdot 1 = b \cdot 1$, a więc z **A7**, $a = b$. □

Uwaga 4.10. Zauważmy, że element x z **A4** jest wyznaczony jednoznacznie przez element a. Rzeczywiście, jeśli $y \in K$ i $a + y = 0$, to $a + y = a + x$, skąd z **A1** i własności 4.9 (a) mamy, że $y = x$. Ten jedyny element x z **A4** nazywamy **elementem przeciwnym** do a i oznaczamy przez $(-a)$. Zatem $a + (-a) = 0$ i $(-a)$ jest jedynym rozwiązaniem równania $a + x = 0$. Ponieważ z **A1**: $(-a) + a = 0$, więc a jest elementem przeciwnym do $(-a)$ i mamy wzór:

$$-(-a) = a. \tag{4.1}$$

Ponadto, z **A3**, $0 + 0 = 0$, więc $0 = -0$.

Własność 4.11. *Dla każdego elementu a ciała K:*

(i) $a \cdot 0 = 0$,
(ii) $-a = 0 \iff a = 0$,
(iii) $-a = (-1) \cdot a$.
W szczególności: $1 \neq 0$ *i* $-1 \neq 0$.

Dowód. (i). Z **A3**: $0 = 0 + 0$, więc $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, na mocy **A8**. Stąd z **A3** i **A1**: $0 + a \cdot 0 = a \cdot 0 + a \cdot 0$ i z własności 4.9 (a), $a \cdot 0 = 0$.

(ii). Jeśli $-a = 0$, to $-(-a) = -0 = 0$, więc na mocy (4.1), $a = 0$. Jeśli zaś $a = 0$, to $-a = -0 = 0$.

(iii). Z **A7** i **A5**, $a = 1 \cdot a$. Stąd i z **A8** oraz z **A5**: $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = [1 + (-1)] \cdot a = 0 \cdot a = 0$ na mocy (i). Zatem z uwagi 4.10, $(-1) \cdot a = -a$.

Ponieważ zbiór K ma co najmniej dwa elementy, więc istnieje $a \in K$ takie, że $a \neq 0$ i wtedy z **A7**: $a = a \cdot 1$ oraz : $a \cdot 0 = 0 \neq a$, więc $1 \neq 0$ i na mocy (ii), $-1 \neq 0$. □

Uwaga 4.12. Zauważmy, że element y z **A9** jest wyznaczony jednoznacznie przez element a. Rzeczywiście, niech $z \in K$ będzie taki, że $a \cdot z = 1$. Wtedy na mocy **A5**, $z \cdot a = y \cdot a$ i $a \neq 0$, więc na mocy własności 4.9 (b), $z = y$. Ten jedyny element y z **A9** nazywamy **elementem odwrotnym** do elementu $a \neq 0$ i oznaczamy przez a^{-1} lub $\frac{1}{a}$. Zatem $a \cdot \frac{1}{a} = 1$ i $\frac{1}{a}$ jest jedynym rozwiązaniem równania $a \cdot y = 1$ (dla $a \neq 0$). Jeśli $a^{-1} = 0$, to $1 = a \cdot a^{-1} = a \cdot 0 = 0$, na mocy własności 4.11, skąd $0 = 1$ wbrew własności 4.11. Zatem $a^{-1} \neq 0$ oraz z **A5**, $a^{-1} \cdot a = 1$, czyli a jest elementem odwrotnym do elementu a^{-1} i dla dowolnego $a \neq 0$ mamy wzór:

$$(a^{-1})^{-1} = a. \tag{4.2}$$

Z **A7** mamy, że $1 \cdot 1 = 1$, więc $1^{-1} = \frac{1}{1} = 1$.

W dowolnym ciele $(K, +, \cdot, 0, 1)$ można określić **odejmowanie** przyjmując, że dla dowolnych $a, b \in K$:

$$a - b \stackrel{def}{=} a + (-b). \tag{4.3}$$

Zauważmy, że sumę dowolnych elementów $a, b \in K$ można wyrazić za pomocą odejmowania:

$$a + b = a - (-b). \tag{4.4}$$

Rzeczywiście, $a - (-b) = a + [-(-b)] = a + b$ na mocy (4.3) i (4.1).

Stwierdzenie 4.13. *Niech $(L, +, \cdot, 0, 1)$ będzie ciałem. Dla podzbioru K zbioru L równoważne są warunki:*

(i) K tworzy ciało ze względu na dodawanie i mnożenie ciała L obcięte do $K \times K$,

(ii) $1 \in K$ i $a - b, a \cdot b \in K$ dla $a, b \in K$ oraz $\frac{1}{b} \in K$ dla każdego $b \in K \setminus \{0\}$.

Dowód. $(i) \Rightarrow (ii)$. Z założenia wynika, że zbiór K ma co najmniej dwa elementy. Istnieje zatem $x \in K$ takie, że $x \neq 0$. Dalej, $x \cdot e = x$ dla pewnego $e \in K$, a ponieważ $x \neq 0$ i $x = x \cdot 1$, więc z własności 4.9 (b), $e = 1$. Zatem $1 \in K$. Na mocy naszego założenia, $a + b \in K$ i $a \cdot b \in K$ dla dowolnych $a, b \in K$. Dalej, istnieje $f \in K$ takie, że $x + f = x$. Ale $x = x + 0$, więc z własności 4.9 (a), $f = 0$, czyli $0 \in K$. Weźmy dowolne $a, b \in K$. Wtedy $b + y = 0$ dla pewnego $y \in K$, skąd $y = -b$ i $-b \in K$. Ale $a - b = a + (-b)$, więc $a - b \in K$. W końcu dla $b \in K \setminus \{0\}$ istnieje $t \in K$ takie, że $b \cdot t = 1$, skąd $t = \frac{1}{b}$, czyli $\frac{1}{b} \in K$.

$(ii) \Rightarrow (i)$. Ponieważ $1 \in K$, więc $0 = 1 + (-1) = 1 - 1 \in K$, czyli $0 \in K$. Ale $0 \neq 1$ w L, więc zbiór K ma co najmniej dwa elementy. Dalej, dla każdego $a \in K$ jest $-a \in K$, bo $-a = 0 - a$. Ponadto dla dowolnych $a, b \in K$ na mocy (4.4): $a + b = a - (-b)$, więc $a + b \in K$, bo jak wykazaliśmy $-b \in K$. Wobec tego: $a + b = b + a$, $a + 0 = a$, $a + (b + c) = (a + b) + c$ i $a + (-a) = 0$ dla dowolnych $a, b, c \in K$.

Weźmy dowolne $a, b, c \in K$. Wtedy $a, b, c \in L$. Z własności mnożenia i dodawania w ciele L wynika, że $a \cdot 1 = a$, $a \cdot b = b \cdot a$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ i $a \cdot (b + c) = a \cdot b + a \cdot c$ dla dowolnych $a, b, c \in K$. Ponadto, dla każdego $a \in K \setminus \{0\}$ jest $a \cdot \frac{1}{a} = 1$ i $\frac{1}{a} \in K$.

Widzimy zatem, że zbiór K tworzy ciało ze względu na dodawanie i mnożenie ciała L (obcięte do $K \times K$). □

Ciało K spełniające podpunkt (ii) stwierdzenia 4.13 nazywamy **podciałem ciała** $(L, +, \cdot, 0, 1)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

4.3 Własności działań w ciele

Własność 4.14. *Dla dowolnych elementów a, b, c ciała K:*
(i) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$ *oraz* $(-a)\cdot(-b) = a\cdot b$,
(ii) $a - b$ *jest jedynym rozwiązaniem równania* $b + x = a$,
(iii) $a\cdot(b-c) = a\cdot b - a\cdot c$ *oraz* $(b-c)\cdot a = b\cdot a - c\cdot a$.

Dowód. (i). Z własności 4.11 (iii) i z uwagi 4.8 mamy, że $(-a)\cdot b = = (-1)\cdot(a\cdot b) = -(a\cdot b)$ oraz $a\cdot(-b) = a\cdot(-1)\cdot b = (-1)\cdot(a\cdot b) = -(a\cdot b)$. Stąd $(-a)\cdot(-b) = -[(-a)\cdot b] = -[-(a\cdot b)] = a\cdot b$, na mocy (4.1).

(ii). Ponieważ na mocy wzoru (4.3) i **A2**, $b + (a-b) = b + [a + +(-b)] = b + [(-b) + a] = [b + (-b)] + a = 0 + a = a$, więc $a - b$ spełnia równanie $b + x = a$. Jeżeli zaś $u, v \in K$ są takie, że $b + u = a$ i $b + v = a$, to $b + u = b + v$ i na mocy własności 4.9 (a), $u = v$. Wobec tego $a - b$ jest jedynym rozwiązaniem równania $b + x = a$ w ciele K.

(iii). Z (4.3), **A8** i z (i) mamy, że $a\cdot(b-c) = a\cdot(b + (-c)) = = a\cdot b + a\cdot(-c) = a\cdot b + [-(a\cdot c)] = a\cdot b - a\cdot c$.

Stąd i z **A6**, $(b-c)\cdot a = a\cdot(b-c) = a\cdot b - a\cdot c = b\cdot a - c\cdot a$. □

Dzielenie przez niezerowe elementy b w ciele $(K, +, \cdot, 0, 1)$ określamy następująco:

$$a : b = \frac{a}{b} = a\cdot b^{-1}, \quad b \neq 0. \tag{4.5}$$

Dla $a \neq 0$: $\frac{a}{a} = a\cdot a^{-1} = 1$, więc mamy wzór:

$$\frac{a}{a} = 1 \text{ dla każdego } a \neq 0. \tag{4.6}$$

Własność 4.15. *Dla dowolnych elementów a i b ciała K takich, że $b \neq 0$ element $\frac{a}{b}$ jest jedynym rozwiązaniem równania $b\cdot x = a$. W szczególności dla każdego $c \in K$: $\frac{a}{b} = c \iff a = b\cdot c$.*

Dowód. Z **A6** i ze wzoru (4.5) oraz z **A5**, $b\cdot\frac{a}{b} = \frac{a}{b}\cdot b = [a\cdot b^{-1}]\cdot b = = a\cdot[b^{-1}\cdot b] = a\cdot 1 = a$ na mocy **A7**. Zatem $\frac{a}{b}$ jest rozwiązaniem równania $b\cdot x = a$. Niech $u, v \in K$ będą takie, że $b\cdot u = a$ i $b\cdot v = a$. Wtedy $b\cdot u = b\cdot v$, więc z własności 4.9 (b), $u = v$. Zatem $\frac{a}{b}$ jest jedynym rozwiązaniem równania $b\cdot x = a$.

Z pierwszej części dowodu, $\frac{a}{b} = c$ wtedy i tylko wtedy, gdy c jest rozwiązaniem równania $b \cdot x = a$, czyli, gdy $a = b \cdot c$. □

Własność 4.16. *Dla dowolnego $n = 2, 3, \ldots$ i dla dowolnych niezerowych elementów $a_1, a_2, \ldots, a_n$ ciała $(K, +, \cdot, 0, 1)$:*
(i) $a_1 \cdot a_2 \cdot \ldots \cdot a_n \neq 0$,
(ii) $\frac{1}{a_1 \cdot a_2 \cdot \ldots \cdot a_n} = \frac{1}{a_1} \cdot \frac{1}{a_2} \cdot \ldots \cdot \frac{1}{a_n}$.

Dowód. (i). Niech a i b będą niezerowymi elementami ciała K. Jeżeli $a \cdot b = 0$, to na mocy **A5** i własności 4.11, $a \cdot b = 0 \cdot b$, skąd $a = 0$ na mocy własności 4.9 (b) i mamy sprzeczność. Zatem $a \cdot b \neq 0$.

Niech teraz $n \geqslant 2$ będzie taką liczbą naturalną, że w ciele K iloczyn dowolnych n niezerowych elementów jest elementem niezerowym. Weźmy dowolne niezerowe elementy $a_1, \ldots, a_{n+1} \in K$. Wtedy $a_1 \cdot \ldots \cdot a_n \neq 0$ na mocy założenia indukcyjnego, więc z pierwszej części dowodu $(a_1 \cdot \ldots \cdot a_n) \cdot a_{n+1} \neq 0$, czyli $a_1 \cdot \ldots \cdot a_n \cdot a_{n+1} \neq 0$. Stąd na mocy zasady indukcji matematycznej mamy tezę.

(ii). Na mocy uwagi 4.8 mamy, że $(\frac{1}{a_1} \cdot \frac{1}{a_2} \cdot \ldots \cdot \frac{1}{a_n}) \cdot (a_1 \cdot a_2 \cdot \ldots \cdot a_n) = (\frac{1}{a_1} \cdot a_1) \cdot (\frac{1}{a_2} \cdot a_2) \cdot \ldots \cdot (\frac{1}{a_n} \cdot a_n) = 1 \cdot 1 \cdot \ldots \cdot 1 = 1$. Zatem na mocy uwagi 4.12 oraz podpunktu (i) mamy, że $\frac{1}{a_1} \cdot \frac{1}{a_2} \cdot \ldots \cdot \frac{1}{a_n}$ jest elementem odwrotnym do elementu $a_1 \cdot a_2 \cdot \ldots \cdot a_n$, co kończy dowód. □

Własność 4.17. *Jeżeli a i b są niezerowymi elementami ciała $(K, +, \cdot, 0, 1)$, to $a \cdot b \neq 0$, $\frac{a}{b} \neq 0$ i $(\frac{a}{b})^{-1} = \frac{b}{a}$ oraz $\frac{1}{a \cdot b} = \frac{1}{a} \cdot \frac{1}{b}$.*

Dowód. Z uwagi 4.12, $\frac{1}{b} \neq 0$, a ponieważ $a \neq 0$, więc z własności 4.16, $a \cdot \frac{1}{b} \neq 0$, czyli $\frac{a}{b} \neq 0$. Ponadto, $\frac{a}{b} \cdot \frac{b}{a} = a \cdot b^{-1} \cdot b \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1$, więc na mocy uwagi 4.12, $\frac{b}{a}$ jest elementem odwrotnym do $\frac{a}{b}$, czyli $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Dalej, z własności 4.16, $a \cdot b \neq 0$ i na mocy uwagi 4.8, $(a \cdot b) \cdot \frac{1}{a} \cdot \frac{1}{b} = [a \cdot \frac{1}{a}] \cdot [b \cdot \frac{1}{b}] = 1 \cdot 1 = 1$, więc na mocy uwagi 4.12, $\frac{1}{a} \cdot \frac{1}{b}$ jest elementem odwrotnym do elementu $a \cdot b$, czyli $\frac{1}{a \cdot b} = \frac{1}{a} \cdot \frac{1}{b}$. □

Własność 4.18. *Dla dowolnych elementów a, b, c ciała K takich, że $b \neq 0$: $c \cdot \frac{a}{b} = \frac{c \cdot a}{b}$.*

Dowód. Z (4.5) i z **A6**, $c \cdot \frac{a}{b} = c \cdot a \cdot b^{-1} = (c \cdot a) \cdot b^{-1} = \frac{c \cdot a}{b}$. □

Własność 4.19. *Niech a, b, c, d będą elementami ciała K takimi, że $b \neq 0$ i $d \neq 0$. Wtedy: $\frac{a}{b} = \frac{c}{d} \iff a \cdot d = b \cdot c$.*

Dowód. Jeśli $\frac{a}{b} = \frac{c}{d}$, to z własności 4.15, $a = b \cdot \frac{c}{d}$. Stąd i z uwagi 4.8, $a \cdot d = b \cdot (\frac{c}{d} \cdot d) = b \cdot c$, na mocy własności 4.15.

Jeżeli zaś $a \cdot d = b \cdot c$, to $a \cdot d \cdot d^{-1} = b \cdot c \cdot d^{-1}$, skąd $a \cdot 1 = b \cdot \frac{c}{d}$, więc z **A7** i **A6**, $a = \frac{c}{d} \cdot b$. Zatem z własności 4.15 i z **A6**, $\frac{c}{d} = \frac{a}{b}$. □

Własność 4.20. *Niech a, b, c będą elementami ciała K takimi, że $b \neq 0$ i $c \neq 0$. Wówczas: $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$.*

Dowód. Z własności 4.16 mamy, że $b \cdot c \neq 0$. Ponieważ $a \cdot (b \cdot c) = (a \cdot b) \cdot c = (b \cdot a) \cdot c = b \cdot (a \cdot c)$, więc na mocy własności 4.19, $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$. □

Własność 4.21. *Niech a, b, c będą elementami ciała K takimi, że $c \neq 0$. Wówczas: $\frac{a+b}{c} = \frac{a}{c} + \frac{b}{c}$ i $\frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}$.*

Dowód. Ze wzoru (4.5) i z **A8** oraz **A5** mamy kolejno: $\frac{a+b}{c} = (a + b) \cdot c^{-1} = a \cdot c^{-1} + b \cdot c^{-1} = \frac{a}{c} + \frac{b}{c}$. Wobec tego $\frac{a-b}{c} + \frac{b}{c} = \frac{(a-b)+b}{c} = \frac{a+(-b)+b}{c} = \frac{a+0}{c} = \frac{a}{c}$, skąd z własności 4.14, $\frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}$. □

Własność 4.22. *Niech a, b, c, d będą elementami ciała K takimi, że $b \neq 0$ i $d \neq 0$. Wtedy: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$, $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ i $\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d}$.*

Dowód. Z **A5** i wzoru (4.5) mamy, że $\frac{a}{b} \cdot \frac{c}{d} = a \cdot \frac{1}{b} \cdot c \cdot \frac{1}{d} = (a \cdot c) \cdot (\frac{1}{b} \cdot \frac{1}{d}) = (a \cdot c) \cdot \frac{1}{b \cdot d}$, na mocy własności 4.17, więc ze wzoru (4.5), $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.

Z własności 4.20 i **A5**, $\frac{a}{b} = \frac{a \cdot d}{b \cdot d}$ i $\frac{c}{d} = \frac{b \cdot c}{b \cdot d}$. Stąd i na mocy własności 4.21, $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ i $\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d}$. □

Własność 4.23. *Niech a, b, c będą elementami ciała K takimi, że $b \neq 0$ i $c \neq 0$. Wtedy $a : \frac{b}{c} = a \cdot \frac{c}{b}$.*

Dowód. Ze wzoru (4.5) i z własności 4.17, $a : \frac{b}{c} = a \cdot (\frac{b}{c})^{-1} = a \cdot \frac{c}{b}$. □

Własność 4.24. *Dla dowolnego $n = 2, 3, \ldots$ i dla dowolnych elementów $a_1, a_2, \ldots, a_n$ ciała K:*
$-(a_1 + a_2 + \ldots + a_n) = (-a_1) + (-a_2) + \ldots + (-a_n)$.

Dowód. Na mocy uwagi 4.8, $(a_1 + \ldots + a_n) + [(-a_1) + \ldots + (-a_n)] = [a_1 + (-a_1)] + \ldots + [a_n + (-a_n)] = 0 + \ldots + 0 = 0$, więc na mocy uwagi 4.10, $(-a_1) + (-a_2) + \ldots + (-a_n)$ jest elementem przeciwnym do $a_1 + \ldots + a_n$, skąd mamy tezę. □

Własność 4.25. *Dla dowolnego $n = 2, 3, \ldots$ i dla dowolnych elementów $a, a_1, a_2, \ldots, a_n$ ciała K zachodzą wzory:*

(i) $a \cdot (a_1 + a_2 + \ldots + a_n) = a \cdot a_1 + a \cdot a_2 + \ldots + a \cdot a_n$,

(ii) $(a_1 + a_2 + \ldots + a_n) \cdot a = a_1 \cdot a + a_2 \cdot a + \ldots + a_n \cdot a$.

Dowód. (i). Zastosujemy indukcję względem n. Dla $n = 2$ teza wynika z **A8**. Załóżmy, że teza zachodzi dla pewnego naturalnego $n \geqslant 2$ i weźmy dowolne $a, a_1, \ldots, a_n, a_{n+1} \in K$. Wtedy $a_1 + a_2 + \ldots + a_{n+1} = (a_1 + \ldots + a_n) + a_{n+1}$, więc z **A8**, $a \cdot (a_1 + \ldots + a_n + a_{n+1}) = a \cdot (a_1 + \ldots + a_n) + a \cdot a_{n+1}$. Ale z założenia indukcyjnego $a \cdot (a_1 + a_2 + \ldots + a_n) = a \cdot a_1 + a \cdot a_2 + \ldots + a \cdot a_n$, więc $a \cdot (a_1 + \ldots + a_n + a_{n+1}) = a \cdot a_1 + \ldots + a \cdot a_n + a \cdot a_{n+1}$, czyli teza zachodzi dla liczby $n+1$. Wobec tego na mocy zasady indukcji dowodzony wzór zachodzi dla każdego naturalnego $n \geqslant 2$.

(ii). Z **A5** oraz z podpunktu (i) mamy, że $(a_1 + a_2 + \ldots + a_n) \cdot a = a \cdot (a_1 + a_2 + \ldots + a_n) = a \cdot a_1 + a \cdot a_2 + \ldots + a \cdot a_n = a_1 \cdot a + a_2 \cdot a + \ldots + a_n \cdot a$. □

Własność 4.26. *Dla dowolnego $n = 2, 3, \ldots$ i dla dowolnych elementów $b, a_1, a_2, \ldots, a_n$ ciała K takich, że $b \neq 0$ zachodzi wzór:*

$$\frac{a_1 + a_2 + \ldots + a_n}{b} = \frac{a_1}{b} + \frac{a_2}{b} + \ldots + \frac{a_n}{b}.$$

Dowód. Ze wzoru (4.5) i z własności 4.25 mamy, że $\frac{a_1+a_2+\ldots+a_n}{b} = (a_1 + a_2 + \ldots + a_n) \cdot b^{-1} = a_1 \cdot b^{-1} + a_2 \cdot b^{-1} + \ldots + a_n \cdot b^{-1} = \frac{a_1}{b} + \frac{a_2}{b} + \ldots + \frac{a_n}{b}$. □

Własność 4.27. *Dla dowolnych $n, m = 2, 3, \ldots$ i dla dowolnych elementów $a_1, a_2, \ldots, a_n, b_1, \ldots, b_m$ ciała K:*

$$(a_1 + a_2 + \ldots + a_n) \cdot (b_1 + b_2 + \ldots + b_m) =$$

$$= (a_1 \cdot b_1 + \ldots + a_1 \cdot b_m) + \ldots + (a_n \cdot b_1 + \ldots + a_n \cdot b_m).$$

Dowód. Z własności 4.25 mamy, że $(a_1 + \ldots + a_n) \cdot (b_1 + \ldots + b_m) = a_1 \cdot (b_1 + \ldots + b_m) + \ldots + a_n \cdot (b_1 + \ldots + b_m)$. Teraz stosując n-krotnie własność 4.25 uzyskamy tezę. □

W ciele $(K, +, \cdot, 0, 1)$ określamy całkowitą nieujemną potęgę dowolnego elementu $a \in K$ przyjmując, że $a^0 = 1$, $a^1 = 1$ oraz $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}$ dla $n = 2, 3, \ldots$.

Z **A5** i **A6** oraz z wniosków 4.4 i 4.5 mamy od razu następującą:

Własność 4.28. *Dla dowolnych $m, n \in \mathbb{N}_0$ oraz dla dowolnych elementów a i b ciała K:*
(i) $a^n \cdot a^m = a^{n+m}$, *(ii)* $(a^n)^m = a^{nm}$, *(iii)* $(a \cdot b)^n = a^n \cdot b^n$.

Własność 4.29. *Dla dowolnych elementów a i b ciała K zachodzą wzory:*
(i) $a^2 - b^2 = (a - b)(a + b)$,
(ii) $(a + b)^2 = a^2 + 2ab + b^2$.

Dowód. Z własności 4.25, $(a - b) \cdot (a + b) = (a - b) \cdot a + (a - b) \cdot b$. Z własności 4.14 i **A6** mamy, że $(a - b) \cdot a = a \cdot a - b \cdot a = a^2 - a \cdot b$ oraz $(a - b) \cdot b = a \cdot b - b \cdot b = a \cdot b - b^2$, Zatem $(a - b) \cdot (a + b) = a^2 - a \cdot b + a \cdot b - b^2 = a^2 + [-(a \cdot b) + a \cdot b] - b^2 = a^2 + 0 - b^2 = a^2 - b^2$, co kończy dowód (i).

(ii). Na mocy własności 4.27 mamy, że $(a + b)^2 = (a + b) \cdot (a + b) = a^2 + a \cdot b + b \cdot a + b^2$. Ale $b \cdot a = a \cdot b$, więc $b \cdot a + a \cdot b = 2ab$, skąd $(a + b)^2 = a^2 + 2ab + b^2$. □

Własność 4.30. *Dla dowolnych elementów a i b ciała K i dla każdego naturalnego $n \geqslant 2$ zachodzi wzór:*

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}). \tag{4.7}$$

Dowód. Z własności 4.14 (iii) oraz aksjomatu **A5** uzyskujemy, że $(a-b)\cdot(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1}) = a\cdot(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1}) - (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) \cdot b$. Następnie z własności 4.25 dostajemy, że $a \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) = a^n + a^{n-1}b + \ldots + a^2b^{n-2} + ab^{n-1}$ i $(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) \cdot b = a^{n-1}b + a^{n-2}b^2 + \ldots + ab^{n-1} + b^n$. Wobec tego na mocy własności 4.24 i uwagi 4.8 mamy tezę. □

Własność 4.31. *Niech $n \in \mathbb{N}$ i niech a będzie elementem ciała K. Wówczas:*
(i) $(-a)^n = a^n$, *gdy n jest parzyste,*
(ii) $(-a)^n = -a^n$, *gdy n jest nieparzyste.*

Dowód. Jeśli n jest parzyste, to $n = 2k$ dla pewnego $k \in \mathbb{N}$. Z własności 4.25 mamy, że $(-a)^n = [(-a)^2]^k$. Ale na mocy własności 4.14 (i), $(-a)^2 = (-a) \cdot (-a) = a \cdot a = a^2$, więc znowu z własności 4.25, $(-a)^n = (a^2)^k = a^{2k} = a^n$. Ponadto, $(-a)^1 = -a = -a^1$ oraz dla nieparzystych $n > 1$ mamy, że $n = 2k + 1$ dla pewnego $k \in \mathbb{N}$, więc $(-a)^n = (-a)^{2k} \cdot (-a) = a^{2k} \cdot (-a)$ i z własności 4.14 (i), $(-a)^n = -(a^{2k} \cdot a) = -a^{2k+1} = -a^n$. □

Podstawiając we wzorze (4.7): $n = 2m + 1$ dla $m \in \mathbb{N}$ oraz $(-b)$ w miejsce b i wykorzystując własność 4.31, uzyskujemy wzór:

$$a^{2m+1} + b^{2m+1} = (a+b)(a^{2m} - a^{2m-1}b + \ldots + a^2b^{2m-2} - ab^{2m-1} + b^{2m}). \tag{4.8}$$

W ciele $(K, +, \cdot, 0, 1)$ można określić całkowitą wielokrotność $k \cdot a$ elementu $a \in K$ przez liczbę $k \in \mathbb{Z}$ przyjmując, że

$$k \cdot a \stackrel{def}{=} \begin{cases} \underbrace{a + a + \ldots + a}_{k} & , \text{ gdy } k > 0 \\ 0 & , \text{ gdy } k = 0 \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{|k|} & , \text{ gdy } k < 0 \end{cases} . \tag{4.9}$$

Pokażemy, że wówczas zachodzi następujące

Stwierdzenie 4.32. *Dla dowolnych $m, n \in \mathbb{Z}$ i dla dowolnych elementów a i b ciała K:*
(i) $(-n) \cdot a = n \cdot (-a) = -(n \cdot a)$,
(ii) $n \cdot (a + b) = n \cdot a + n \cdot b$.
(iii) $(n + m) \cdot a = n \cdot a + m \cdot a$,
(iv) $(n - m) \cdot a = n \cdot a - m \cdot a$,
(v) $n \cdot (m \cdot a) = (nm) \cdot a$,
(vi) $n \cdot (a \cdot b) = (n \cdot a) \cdot b = a \cdot (n \cdot b)$,
(vii) $(n \cdot a) \cdot (m \cdot b) = (nm) \cdot (a \cdot b)$.

Dowód. (i). Dla $n = 0$ mamy, że $(-n) \cdot a = 0 \cdot a = 0$, $n \cdot (-a) = 0 \cdot (-a) = 0$ i $-(n \cdot a) = -(0 \cdot a) = -0 = 0$, więc wzór nasz zachodzi. Jeśli $n \in \mathbb{N}$, to $(-n) \cdot a = n \cdot (-a)$ i $n \cdot a + n \cdot (-a) = n \cdot [a + (-a)] = n \cdot 0 = 0 + \ldots + 0 = 0$, więc $n \cdot (-a) = -(n \cdot a)$. Pozostaje rozpatrzeć $n < 0$. Wtedy $n = -k$ dla pewnego $k \in \mathbb{N}$, skąd $(-n) \cdot a = k \cdot a$, $n \cdot (-a) = (-k) \cdot (-a) = k \cdot [-(-a)] = k \cdot a$ i $-(n \cdot a) = -[(-k) \cdot a] = -[k \cdot (-a)] = -[-(k \cdot a)] = k \cdot a$, co kończy dowód (i).

(ii). Z wniosku 4.5 i z przemienności dodawania w ciele K wynika, że $n \cdot (a + b) = n \cdot a + n \cdot b$ dla wszystkich $n \in \mathbb{N}$. Ponadto dla $n = 0$: $n \cdot (a + b) = 0 = 0 + 0 = n \cdot a + n \cdot b$. Jeśli zaś $n < 0$, to $n = -k$ dla pewnego $k \in \mathbb{N}$, więc $n \cdot (a + b) = k \cdot [-(a + b)] = k \cdot [(-a) + (-b)] = k \cdot (-a) + k \cdot (-b) = n \cdot a + n \cdot b$.

(iii). Jeśli $n = 0$, to $(n+m) \cdot a = m \cdot a$ i $n \cdot a + m \cdot a = 0 + m \cdot a = m \cdot a$, czyli wzór (iii) wtedy zachodzi. Podobnie, jeśli $m = 0$, to $(n + m) \cdot a = n \cdot a = n \cdot a + 0 = n \cdot a + m \cdot a$. Niech dalej $m, n \neq 0$. Jeżeli $m, n > 0$, to teza zachodzi na mocy wniosku 4.5. Niech teraz $m, n < 0$. Wtedy $n = -k$ i $m = -l$ dla pewnych $k, l \in \mathbb{N}$, więc $n + m = -(k + l)$, czyli $(n + m) \cdot a = (k + l) \cdot (-a) = k \cdot (-a) + l \cdot (-a) = n \cdot a + m \cdot a$.

Pozostają do rozpatrzenia przypadki, gdy n, m są liczbami całkowitymi różnych znaków. Wtedy ze względu na przemienność dodawania w K i przemienność dodawania liczb całkowitych możemy zakładać, że $n > 0$ i $m < 0$, więc $m = -k$ dla pewnego $k \in \mathbb{N}$. Jeśli $n + m = 0$, to $(n+m) \cdot a = 0$ i $m = -n$, więc na mocy (i), $n \cdot a + m \cdot a = n \cdot a + n \cdot (-a) = n \cdot [a + (-a)] = n \cdot 0 = 0$, czyli $(n+m) \cdot a = n \cdot a + m \cdot a$. Jeśli $n + m > 0$, to $n + m = n - k > 0$, więc $(n + m) \cdot a = k \cdot a$ oraz $n \cdot a + m \cdot a = n \cdot a + k \cdot (-a) = (n-k) \cdot a + k \cdot a + k \cdot (-a) = (n-k) \cdot a + 0 = (n-k) \cdot a$, czyli $(n+m) \cdot a = n \cdot a + m \cdot a$. W końcu, niech $n + m < 0$. Wtedy $n - k < 0$, skąd $k - n \in \mathbb{N}$ oraz $(n+m) \cdot a = (k-n) \cdot (-a)$ i $n \cdot a + m \cdot a = n \cdot a + k \cdot (-a) = n \cdot a + n \cdot (-a) + (k - n) \cdot (-a) = 0 + (n - k) \cdot a = (n - k) \cdot a$, więc $(n + m) \cdot a = n \cdot a + m \cdot a$, co kończy dowód (iii).

(iv). Na mocy (iii) mamy, że $(n - m) \cdot a + m \cdot a = [(n - m) + m] \cdot a = n \cdot a$, skąd $(n - m) \cdot a = n \cdot a - m \cdot a$.

(v). Jeśli $n = 0$, to $n \cdot (m \cdot a) = 0$ i $(nm) \cdot a = 0 \cdot a = 0$, czyli

$n \cdot (m \cdot a) = (nm) \cdot a$. Podobnie będzie dla $m = 0$. Niech dalej $m, n \neq 0$. Na mocy wniosku 4.4, $n \cdot (m \cdot a) = (nm) \cdot a$ dla dowolnych $m, n \in \mathbb{N}$.

Jeżeli $m, n < 0$, to $n = -k$ i $m = -l$ dla pewnych $k, l \in \mathbb{N}$, więc $nm = kl$, czyli $(nm) \cdot a = (kl) \cdot a$ oraz $n \cdot (m \cdot a) = n \cdot [l \cdot (-a)] = (-k) \cdot [l \cdot (-a)]$. Ale na mocy (i), $l \cdot (-a) = -(l \cdot a)$, więc $n \cdot (m \cdot a) = (-k) \cdot [-(l \cdot a)] = k \cdot [-(-(l \cdot a))] = k \cdot (l \cdot a) = (kl) \cdot a = (nm) \cdot a$, na mocy pierwszej części dowodu punktu (iv).

Pozostaje do rozpatrzenia przypadek, gdy liczby m, n są różnych znaków. Jeśli $n > 0$ i $m < 0$, to $m = -k$ dla pewnego $k \in \mathbb{N}$, więc $n \cdot (m \cdot a) = n \cdot [k \cdot (-a)] = (nk) \cdot (-a) = (-nk) \cdot a = (nm) \cdot a$. Jeśli zaś $n < 0$ i $m > 0$, to $n = -k$ dla pewnego $k \in \mathbb{N}$, więc $n \cdot (m \cdot a) = k \cdot [-(m \cdot a)]$. Ale z (i), $m \cdot (-a) = (-m) \cdot a = -(m \cdot a)$, zatem $n \cdot (m \cdot a) = k \cdot [m \cdot (-a)] = (km) \cdot (-a) = (-km) \cdot a = (nm) \cdot a$.

(vi). Ponieważ $0 \cdot (a \cdot b) = 0$, $(0 \cdot a) \cdot b = 0 \cdot b = 0$ oraz $a \cdot (0 \cdot b) = a \cdot 0 = 0$ na podstawie definicji mnożenia elementu pierścienia przez liczbę całkowitą 0 oraz na mocy własności 4.11 (i), więc dla $n = 0$ wzór (vi) zachodzi. Załóżmy, że wzór (vi) zachodzi dla pewnego $k \in \mathbb{N}_0$. Wtedy $(k + 1) \cdot (a \cdot b) = k \cdot (a \cdot b) + a \cdot b = (k \cdot a) \cdot b + a \cdot b = (k \cdot a + a) \cdot b = [(k + 1) \cdot a] \cdot b$ oraz $(k + 1) \cdot (a \cdot b) = k \cdot (a \cdot b) + a \cdot b = a \cdot (k \cdot b) + a \cdot b = a \cdot (k \cdot b + b) = a \cdot [(k + 1) \cdot b]$, więc wzór (vi) zachodzi wówczas także dla liczby $k + 1$. Wobec tego na mocy zasady indukcji wzór (vi) zachodzi dla każdego $n \in \mathbb{N}_0$.

Niech teraz $n = -k$, gdzie $k \in \mathbb{N}$. Wtedy $n \cdot (a \cdot b) = k \cdot [-(a \cdot b)] = k \cdot [(-a) \cdot b] = [k \cdot (-a))] \cdot b = (n \cdot a) \cdot b$ oraz $n \cdot (a \cdot b) = k \cdot [-(a \cdot b)] = k \cdot [a \cdot (-b)] = a \cdot [k \cdot (-b)] = a \cdot (n \cdot b)$, na mocy pierwszej części dowodu i własności całkowitej wielokrotności elementu ciała. Wobec tego wzór (vi) zachodzi także dla dowolnej ujemnej liczby całkowitej n, co kończy dowód punktu (vi).

(vii). Na mocy (vi) i (v), $(n \cdot a) \cdot (m \cdot b) = a \cdot [n \cdot (m \cdot b)] = a \cdot [(nm) \cdot b] = (nm) \cdot (a \cdot b)$. □

Przypomnijmy, że dla $a \in K$ i $n \in \mathbb{N}$: $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}$ oraz $a^1 = a$ i dodatkowo przyjmujemy, że $a^0 = 1$ (a więc także $0^0 = 1$). Jeżeli $a \neq 0$, to definiujemy $a^{-n} = (\frac{1}{a})^n$, czyli $a^{-n} = \frac{1}{a^n}$ dla $n \in \mathbb{N}$. W ten sposób mamy określoną potęgę niezerowego elementu ciała

o wykładniku całkowitym. Własność 4.28 można teraz uogólnić w postaci następującego stwierdzenia, którego dowód pominiemy ze względu na jego podobieństwo do dowodu stwierdzenia 4.32.

Stwierdzenie 4.33. *Dla dowolnych $m, n \in \mathbb{Z}$ i dla dowolnych niezerowych elementów a i b ciała K:*
(i) $(a \cdot b)^n = a^n \cdot b^n$,
(ii) $(\frac{a}{b})^n = \frac{a^n}{b^n}$,
(iii) $a^n \cdot a^m = a^{n+m}$,
(iv) $a^n : a^m = a^{n-m}$,
(v) $(a^n)^m = a^{nm}$.

Podamy teraz uogólnienie własności 4.29 (ii) zwane **wzorem dwumianowym Newtona**. Przypomnijmy wcześniej pewne wiadomości dotyczące współczynnika dwumianowego $\binom{n}{k}$ dla $n, k \in \mathbb{N}_0$. Mianowicie $\binom{n}{k}$ jest liczbą wszystkich podzbiorów k-elementowych zbioru n-elementowego. Wobec tego $\binom{n}{k} \in \mathbb{N}_0$. Wprost z definicji mamy, że $\binom{n}{k} = 0$ dla $k > n$ oraz $\binom{n}{0} = 1$ i $\binom{n}{n} = 1$.

Lemat 4.34. *Dla każdego $n \in \mathbb{N}$ i dla dowolnego $j = 0, 1, \ldots, n-1$ zachodzi wzór:*

$$\binom{n}{j+1} + \binom{n}{j} = \binom{n+1}{j+1}. \tag{4.10}$$

Dowód. Niech X będzie zbiorem $(n+1)$-elementowym o elementach $a, a_1, \ldots, a_n$. Podzbiory $(j+1)$-elementowe zbioru X są dokładnie dwóch rodzajów: są to podzbiory zawierające a lub nie zawierające a. W pierwszym przypadku są one postaci $\{a\} \cup B$, gdzie B jest podzbiorem j-elementowym zbioru n-elementowego $\{a_1, \ldots, a_n\}$, więc takich podzbiorów jest dokładnie $\binom{n}{j}$. W drugim przypadku są one $(j+1)$-elementowymi podzbiorami zbioru n-elementowego $\{a_1, \ldots, a_n\}$, więc takich podzbiorów jest dokładnie $\binom{n}{j+1}$. Zatem $\binom{n+1}{j+1} = \binom{n}{j+1} + \binom{n}{j}$. □

Z lematu 4.34 w prosty sposób można wykazać, że dla dowolnych $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ takich, że $k \leqslant n$ zachodzi wzór:

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}, \tag{4.11}$$

gdzie $0! = 1! = 1$ oraz $m! = 1 \cdot 2 \cdot \ldots \cdot m$ dla $m = 2, 3, \ldots$.

Własność 4.35. (Wzór dwumianowy Newtona). *Dla dowolnych elementów a i b ciała K i dla dowolnego $n \in \mathbb{N}$ zachodzi wzór:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{4.12}$$

Dowód. Stosujemy indukcję względem n. Dla $n = 1$, $L = (a+b)^1 = a+b$, $P = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a \cdot 1 + 1 \cdot b = a+b$, czyli $L = P$ i teza zachodzi dla $n = 1$.

Załóżmy, że wzór (4.12) zachodzi dla pewnej liczby naturalnej n. Wtedy mamy $(a+b)^{n+1} = (a+b) \cdot (a+b)^n = a \cdot (a+b)^n + b \cdot (a+b)^n = a \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k + b \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} = a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k} b^k + b^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1}$, czyli $(a+b)^{n+1} = a^{n+1} + b^{n+1} + \sum_{j=0}^{n-1} \binom{n}{j+1} a^{n-j} b^{j+1} + \sum_{j=0}^{n-1} \binom{n}{j} a^{n-j} b^{j+1}$. Ale na mocy (4.10): $\binom{n}{j+1} + \binom{n}{j} = \binom{n+1}{j+1}$ dla $j = 0, 1, \ldots, n-1$, więc uzyskujemy stąd, że $(a+b)^{n+1} = a^{n+1} + b^{n+1} + \sum_{j=0}^{n-1} \binom{n+1}{j+1} a^{n-j} b^{j+1} = a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k = \sum_{j=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k$. Zatem wzór (4.12) jest wówczas prawdziwy także dla liczby $n+1$.

Wobec tego na mocy zasady indukcji wzór (4.12) jest prawdziwy dla dowolnego $n \in \mathbb{N}$. □

Rozdział 5

Ciała uporządkowane

5.1 Pojęcie i własności ciała uporządkowanego

Mówimy, że ciało $(K, +, \cdot, 0, 1)$ jest **ciałem uporządkowanym**, jeżeli istnieje relacja dwuargumentowa $<$ w zbiorze K spełniająca następujące warunki:

P1. Dla dowolnych $a, b \in K$ zachodzi dokładnie jedna z trzech możliwości:

$$a < b, \quad a = b, \quad b < a.$$

P2. Dla dowolnych $a, b, c \in K$: jeśli $a < b$ i $b < c$, to $a < c$.

P3. Dla dowolnych $a, b, c \in K$:

(a) jeżeli $a < b$, to $a + c < b + c$,

(b) jeżeli $a < b$ i $0 < c$, to $a \cdot c < b \cdot c$.

Przykładem ciała uporządkowanego jest ciało $\mathbb{Q}$ liczb wymiernych z naturalną relacją mniejszości.

Niech K będzie ciałem uporządkowanym z relacją mniejszości $<$. Udowodnimy, że wówczas zachodzą następujące własności.

Własność 5.1. *$0 < a^2$ dla każdego $a \in K$, $a \neq 0$.*

Dowód. Ponieważ $a \neq 0$, więc z **P1** wynika, że $0 < a$ lub $a < 0$. W pierwszym przypadku na mocy **P3** (b), $0 \cdot a < a \cdot a$, czyli $0 < a^2$.

W drugim przypadku na mocy **P3** (a), $a + (-a) < 0 + (-a)$, skąd $0 < -a$ i znowu z **P3** (b), $0 \cdot (-a) < (-a) \cdot (-a)$. Stąd $0 < a^2$, bo $(-a)^2 = a^2$. □

Własność 5.2. $0 < 1$.

Dowód. Ponieważ $1 \neq 0$, więc z własności 5.1, $0 < 1^2$, ale $1^2 = 1$, więc $0 < 1$. □

Własność 5.3. $0 < n \cdot 1$ *dla każdego* $n \in \mathbb{N}$.

Dowód. Zastosujemy indukcję ze względu na n. Dla $n = 1$ teza wynika z własności 5.2 i z tego, że $1 \cdot 1 = 1$. Załóżmy, że $0 < n \cdot 1$ dla pewnego $n \in \mathbb{N}$. Wtedy z **P3** (a), $0+1 < n \cdot 1+1$. Ale $0+1 = 1$ i $n \cdot 1+1 = (n+1) \cdot 1$, więc $0 < (n+1) \cdot 1$. Zatem dowodzona nierówność zachodzi wówczas dla liczby $n+1$. Na mocy zasady indukcji matematycznej mamy zatem, że $0 < n \cdot 1$ dla każdego $n \in \mathbb{N}$. □

Z własności 5.2 i **P1** wynika od razu, że $n \cdot 1 \neq 0$ dla każdego $n \in \mathbb{N}$.

Własność 5.4. $-1 < 0$.

Dowód. Ponieważ $0 < 1$ na mocy własności 5.2, więc z **P3** (a) mamy, że $0 + (-1) < 1 + (-1)$, czyli $-1 < 0$. □

Własność 5.5. $n \cdot (-1) < 0$ *dla każdego* $n \in \mathbb{N}$.

Dowód. Z własności 5.3 wynika, że $0 < n \cdot 1$. Zatem na mocy **P3** (a) jest $0+n \cdot (-1) < n \cdot 1+n \cdot (-1)$, ale $n \cdot (-1)+n \cdot 1 = n \cdot [1+(-1)] = n \cdot 0 = 0$, więc $n \cdot (-1) < 0$. □

Własność 5.6. *Jeżeli* $0 < a$, *to* $0 < a^{-1}$.

Dowód. Niech $0 < a$. Wtedy z **P1**, $a \neq 0$, skąd $\frac{1}{a} = a^{-1} \neq 0$. Zatem $0 < (\frac{1}{a})^2$ z własności 5.1. Stąd $0 < \frac{1}{a^2}$, ale $0 < a$, więc $0 \cdot \frac{1}{a^2} < a \cdot \frac{1}{a^2}$ na mocy **P3** (b), skąd $0 < \frac{1}{a}$. □

Własność 5.7. *Jeżeli* $a < b$, *to* $a < \frac{a+b}{1+1} < b$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Z **P3** (a) mamy, że $a + a < a + b$. Dalej, $a + a = (1 + 1) \cdot a$ i na mocy własności 5.3, $0 < 1 + 1$, więc $0 < \frac{1}{1+1}$ z własności 5.6. Ponadto $a \cdot (1+1) < a+b$, więc z **P3** (b) dostajemy, że $a \cdot (1+1) \cdot \frac{1}{1+1} < (a + b) \cdot \frac{1}{1+1}$, skąd $a < \frac{a+b}{1+1}$.

Ponadto, $a < b$, więc z **P3** (a), $a + b < b + b$ i $b + b = b \cdot (1 + 1)$, więc $a + b < b \cdot (1 + 1)$ i z **P3** (b) jest $(a + b) \cdot \frac{1}{1+1} < b \cdot (1 + 1) \cdot \frac{1}{1+1}$, a zatem $\frac{a+b}{1+1} < b$. □

Własność 5.8. *Jeżeli* $0 < a_i$ *dla* $i = 1, 2, \ldots, n$, *to* $0 < a_1 \cdot a_2 \cdot \ldots \cdot a_n$ *oraz* $0 < a_1 + a_2 + \ldots + a_n$.

Dowód. Zastosujemy indukcję ze względu na n. Dla $n = 1$ teza jest oczywista. Rozważmy $n = 2$. Wtedy mamy $0 < a_1$ i $0 < a_2$, więc z **P3** (b), $0 \cdot a_2 < a_1 \cdot a_2$, skąd $0 < a_1 \cdot a_2$. Ponadto z **P3** (a), $0 + a_2 < a_1 + a_2$, czyli $a_2 < a_1 + a_2$. Ale $0 < a_2$, więc z **P2**, $0 < a_1 + a_2$.

Załóżmy, że dla pewnego naturalnego $n \geqslant 2$ nasze nierówności zachodzą i weźmy dowolne $a_1, \ldots, a_{n+1} \in K$ takie, że $0 < a_i$ dla każdego $i = 1, 2, \ldots, n + 1$. Wtedy z założenia indukcyjnego $0 < a_1 \cdot \ldots \cdot a_n$ i $0 < a_1 + \ldots + a_n$. Stąd na mocy **P3** (b), $0 \cdot a_{n+1} < (a_1 \cdot \ldots \cdot a_n) \cdot a_{n+1}$, czyli $0 < a_1 \cdot a_n \cdot a_{n+1}$. Ponadto z **P3** (a), $0 + a_{n+1} < a_1 + \ldots + a_n + a_{n+1}$, czyli $a_{n+1} < a_1 + \ldots + a_n + a_{n+1}$. Ponadto $0 < a_{n+1}$, więc z **P2**, $0 < a_1 + \ldots + a_n + a_{n+1}$. Zatem teza zachodzi dla liczby $n + 1$.

Stąd na mocy zasady indukcji matematycznej teza zachodzi dla dowolnego $n \in \mathbb{N}$. □

Własność 5.9. *Dla dowolnego* $a \in K$: $a < 0 \iff 0 < -a$.

Dowód. Jeżeli $a < 0$, to $a + (-a) < 0 + (-a)$ na mocy **P3** (a), skąd $0 < -a$. Na odwrót, niech $0 < -a$. Wtedy $0 + a < (-a) + a$ na mocy **P3** (a), czyli $a < 0$. □

Własność 5.10. *Dla dowolnych* $a, b \in K$: $a < b \iff a - b < 0$.

Dowód. Niech $a < b$. Wtedy $a + (-b) < b + (-b)$ na mocy **P3**, skąd $a - b < 0$. Na odwrót, niech $a - b < 0$. Wtedy $(a - b) + b < 0 + b$ z **P3** (a), ale $(a - b) + b = a$, więc $a < b$. □

Własność 5.11. *Jeżeli* $a < b$ *i* $c < 0$, *to* $b \cdot c < a \cdot c$.

Dowód. Z własności 5.9 mamy, że $0 < -c$, więc $a \cdot (-c) < b \cdot (-c)$ z **P3** (b), skąd $-(a \cdot c) < -(b \cdot c)$. Stąd z **P3** (a) po dodaniu do obu stron elementu $a \cdot c + b \cdot c$ uzyskamy, że $b \cdot c < a \cdot c$. □

Własność 5.12. *Dla dowolnych $a, b \in K$:*
(i) jeżeli $a < 0$ i $b < 0$, to $0 < a \cdot b$,
(ii) jeżeli $a < 0$ i $0 < b$, to $a \cdot b < 0$,
(iii) $0 < a \cdot b \iff [(0 < a \text{ i } 0 < b) \text{ lub } (a < 0 \text{ i } b < 0)]$.

Dowód. (i). Z własności 5.9 mamy, że $0 < -b$, więc na mocy **P3** (b), $a \cdot (-b) < 0 \cdot (-b)$, czyli $-(a \cdot b) < 0$. Zatem $0 < -(-(a \cdot b))$ z własności 5.9, czyli $0 < a \cdot b$.

(ii). Wynika od razu z **P3**.

(iii). Implikacja $\Leftarrow$ wynika od razu z (i) oraz z własności 5.8. Załóżmy, że $0 < a \cdot b$. Wtedy na mocy **P1**, $a \neq 0$ i $b \neq 0$, bo $0 \cdot x = x \cdot 0 = 0$ dla każdego $x \in K$. Z **P1** wynika, że możliwe są tylko następujące przypadki: (1) $0 < a$ i $0 < b$; (2) $0 < a$ i $b < 0$; (3) $a < 0$ i $b < 0$; (4) $a < 0$ i $0 < b$. Ale na mocy (ii) przypadki (2) i (4) nie mogą zajść, co kończy nasz dowód. □

Własność 5.13. *Jeżeli $b \neq 0$, to:* $0 < \frac{a}{b} \iff 0 < a \cdot b$.

Dowód. Niech $0 < \frac{a}{b}$. Ponieważ $b \neq 0$, więc z własności 5.1, $0 < b^2$. Stąd na mocy **P3** (b), $0 \cdot b^2 < \frac{a}{b} \cdot b^2$, a zatem $0 < a \cdot b$, bo $\frac{a}{b} \cdot b^2 = a \cdot b$. Na odwrót, niech $0 < a \cdot b$. Ponieważ $b \neq 0$, więc $\frac{1}{b} \neq 0$ i z własności 5.1, $0 < (\frac{1}{b})^2$. Zatem $0 \cdot \frac{1}{b^2} < (a \cdot b) \cdot \frac{1}{b^2}$ z **P3** (b), czyli $0 < \frac{a}{b}$. □

Własność 5.14. *Jeżeli $a_i < b_i$ dla $i = 1, 2, \ldots, n$, to $a_1 + a_2 + \ldots + a_n < b_1 + b_2 + \ldots + b_n$.*

Dowód. Na mocy własności 5.10 mamy, że $a_i - b_i < 0$, skąd na mocy własności 5.9, $0 < -(a_i - b_i)$, czyli $0 < b_i - a_i$ dla $i = 1, 2, \ldots, n$. Stąd na mocy własności 5.8 jest $0 < (b_1 - a_1) + \ldots + (b_n - a_n)$, czyli $0 < (b_1 + \ldots + b_n) - (a_1 + \ldots + a_n)$ i na mocy własności 5.10 otrzymujemy, że $a_1 + \ldots + a_n < b_1 + \ldots + b_n$. □

Własność 5.15. *Jeżeli $0 < a_i < b_i$ dla $i = 1, 2, \ldots, n$, to $0 < a_1 \cdot a_2 \cdot \ldots \cdot a_n < b_1 \cdot b_2 \cdot \ldots \cdot b_n$.*

Dowód. Z własności 5.8 mamy, że $0 < a_1 \cdot \ldots \cdot a_n$. Ponadto $a_1 < b_1$. Załóżmy, że dla pewnego naturalnego n oraz dla dowolnych $a_i, b_i \in K$ takich, że $0 < a_i < b_i$ dla każdego $i = 1, 2, \ldots, n$ jest $a_1 \cdot a_2 \cdot \ldots \cdot a_n < b_1 \cdot b_2 \cdot \ldots \cdot b_n$. Weźmy dowolne $a_1, \ldots, a_{n+1}, b_1, \ldots, b_{n+1} \in K$ takie, że $0 < a_i < b_i$ dla każdego $i = 1, 2, \ldots, n+1$. Wtedy z założenia indukcyjnego $a_1 \cdot \ldots \cdot a_n < b_1 \cdot \ldots \cdot b_n$. Zatem na mocy **P3** (b) mamy, że $a_1 \cdot \ldots \cdot a_n \cdot a_{n+1} < b_1 \cdot \ldots \cdot b_n \cdot a_{n+1}$. Ale $a_{n+1} < b_{n+1}$ i $0 < b_1 \cdot \ldots \cdot b_n$, więc z **P3** (b), $b_1 \cdot \ldots \cdot b_n \cdot a_{n+1} < b_1 \cdot \ldots \cdot b_n \cdot b_{n+1}$ i na mocy **P2**, $a_1 \cdot \ldots \cdot a_{n+1} < b_1 \cdot \ldots \cdot b_{n+1}$, czyli teza zachodzi dla liczby $n+1$. Na mocy zasady indukcji matematycznej nasza własność jest zatem prawdziwa dla dowolnego $n \in \mathbb{N}$. □

Własność 5.16. *Jeżeli* $0 < a$ *i* $0 < b$, *to dla dowolnego* $n \in \mathbb{N}$*:* $a^n < b^n \iff a < b$.

Dowód. Jeżeli $a < b$, to $a^n < b^n$ na mocy własności 5.15. Na odwrót, niech dla pewnego $n \in \mathbb{N}$ będzie: $a^n < b^n$. Jeśli $a = b$, to $a^n = b^n$ i mamy sprzeczność z **P2**. Zatem $a \neq b$ i na mocy **P2**, $a < b$ lub $b < a$. Ale jeśli $b < a$, to na mocy własności 5.15, $b^n < a^n$, co wobec $a^n < b^n$ przeczy **P2**. Wobec tego musi być $a < b$. □

Własność 5.17. *Jeżeli* $0 < a, b$ *i* $n \in \mathbb{N}$ *oraz* $a^n = b^n$, *to* $a = b$.

Dowód. Jeśli $a < b$, to z własności 5.16, $a^n < b^n$, czyli na mocy **P1** mamy sprzeczność. Podobnie, jeśli $b < a$, to z własności 5.16, $b^n < a^n$ i też mamy sprzeczność. Stąd na mocy **P1**, $a = b$. □

W zbiorze K wprowadzamy jeszcze relacje: $>$, $\leqslant$, $\geqslant$, przyjmując, że dla dowolnych $a, b \in K$:

$$a > b \iff b < a,$$

$$a \leqslant b \iff [a < b \text{ lub } a = b],$$

$$a \geqslant b \iff [b < a \text{ lub } a = b].$$

Własność 5.18. (nierówność Bernoulliego). *Jeżeli* $a > -1$, *to dla każdego* $n \in \mathbb{N}$*:*

$$(1 + a)^n \geqslant 1 + n \cdot a. \tag{5.1}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Zastosujemy indukcję względem n przy dowolnym ustalonym $a > -1$. Dla $n = 1$: $(1+a)^n = (1+a)^1 = 1+a$ i $1+n\cdot a = 1+a$, więc nierówność (5.1) zachodzi.

Załóżmy, że dla pewnego $n \in \mathbb{N}$ mamy, że $(1+a)^n \geqslant 1+n\cdot a$. Ponieważ $a > -1$, więc $1+a > 0$ z własności 5.10. Zatem z **P3** (b), $(1+a)\cdot(1+a)^n \geqslant (1+a)\cdot(1+n\cdot a)$. Ponadto $(1+a)\cdot(1+a)^n = (1+a)^{n+1}$ i $(1+a)\cdot(1+n\cdot a) = 1+n\cdot a+a+n\cdot a^2 = 1+(n+1)\cdot a+n\cdot a^2 \geqslant 1+(n+1)a$, bo $a^2 \geqslant 0$ na mocy własności 5.1, skąd z własności 5.15, $n\cdot a^2 \geqslant 0$. Wobec tego na mocy **P2**, $(1+a)^{n+1} \geqslant 1+(n+1)\cdot a$, czyli nierówność (5.1) zachodzi wówczas dla liczby $n+1$.

Wobec tego na mocy zasady indukcji matematycznej $(1+a)^n \geqslant$ $\geqslant 1+n\cdot a$ dla każdego $n \in \mathbb{N}$. □

Własność 5.19. *Jeżeli $a \geqslant 0$, to dla każdego $n \in \mathbb{N}$:*

$$(1+a)^n \geqslant 1+n\cdot a+\frac{n(n-1)}{2}\cdot a^2. \tag{5.2}$$

Dowód. Dla $n = 1$ prawa strona nierówności (5.2) jest równa $1+1\cdot a =$ $= 1+a = (1+a)^1$, czyli nierówność (5.2) zachodzi dla $n = 1$. Natomiast dla $n \geqslant 2$ ze wzoru dwumianowego Newtona mamy, że $(1+a)^n =$ $= 1+n\cdot a+\frac{n(n-1)}{2}\cdot a^2+\binom{n}{3}\cdot a^3+\ldots+\binom{n}{n-1}a^{n-1}+a^n$. Ale $a \geqslant 0$, więc z własności 5.8 mamy, że $\binom{n}{3}\cdot a^3+\ldots+\binom{n}{n-1}a^{n-1}+a^n \geqslant 0$. Stąd $(1+a)^n \geqslant 1+n\cdot a+\frac{n(n-1)}{2}\cdot a^2$. □

Definicja 5.20. Wartością bezwzględną elementu $a \in K$ nazywamy element $|a| \in K$ określony wzorem:

$$|a| = \begin{cases} a & \text{dla} \quad a \geqslant 0, \\ -a & \text{dla} \quad a < 0. \end{cases} \tag{5.3}$$

Bezpośrednio z określenia wartości bezwzględnej wynika, że dla dowolnego $a \in K$ zachodzą następujące własności:

$$|a| = 0 \iff a = 0, \tag{5.4}$$

$$|a| \geqslant 0, \tag{5.5}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$$a \leqslant |a|, \tag{5.6}$$

$$|a|^2 = a^2, \tag{5.7}$$

$$|a| = |-a|, \tag{5.8}$$

$$\text{jeśli } c > 0, \text{ to } |a| = c \iff [a = c \text{ lub } a = -c]. \tag{5.9}$$

Własność 5.21. *Dla dowolnych $x, y \in K$:*
(i) $|xy| = |x| \cdot |y|$,
(ii) $|x + y| \leqslant |x| + |y|$ *(***nierówność trójkąta***)*,
(iii) $||x| - |y|| \leqslant |x - y|$.

Dowód. (i). Ze wzoru (5.7), $|xy|^2 = (xy)^2 = x^2y^2 = |x|^2 \cdot |y|^2 = (|x| \cdot |y|)^2$, czyli $|xy|^2 = (|x| \cdot |y|)^2$. Ponadto z (5.5) mamy, że $|xy|, |x| \cdot |y| \geqslant 0$, więc $|xy| = |x| \cdot |y|$ z własności 5.17.

(ii). Na mocy (5.6) jest $xy \leqslant |xy|$. Zatem z (i) $xy \leqslant |x| \cdot |y|$, skąd $2xy \leqslant 2|x| \cdot |y|$. W konsekwencji $x^2 + 2xy + y^2 \leqslant x^2 + 2|x| \cdot |y| + y^2$, ale na mocy (5.7) jest $x^2 = |x|^2$ i $y^2 = |y|^2$, czyli $x^2 + 2xy + y^2 \leqslant |x|^2 + 2|x| \cdot |y| + |y|^2$. Stąd mamy, że $(x + y)^2 \leqslant (|x| + |y|)^2$. Zatem na mocy (5.7), $|x + y|^2 \leqslant (|x| + |y|)^2$. Dalej, z (5.5) wynika, że $|x + y|, |x| + |y| \geqslant 0$, więc $|x + y| \leqslant |x| + |y|$ z własności 5.16.

(iii). Z (ii) mamy, że $|x-y|+|y| \geqslant |(x-y)+y| = |x|$, więc $|x|-|y| \leqslant |x-y|$, ale $y-x = -(x-y)$, więc z (5.8) dostajemy, że $|y-x| = |x-y|$. Ponadto z (ii), $|y - x| + |x| \geqslant |(y - x) + x| = |y|$, więc stąd $|y| - |x| \leqslant |x - y|$. Ponadto $||x| - |y|| = |x| - |y|$ lub $||x| - |y|| = -(|x| - |y|) = |y| - |x|$, więc $||x| - |y|| \leqslant |x - y|$. □

Własność 5.22. *Dla dowolnego $a > 0$ i dla każdego $x \in K$:*

$$|x| < a \iff -a < x < a. \tag{5.10}$$

Dowód. Możliwe są tylko dwa przypadki: (1) $x < 0$ i (2) $x \geqslant 0$. W przypadku (1): $|x| = -x$, więc $|x| < a \iff -x < a \iff 0 < a + x \iff -a < x$, czyli $-a < x < 0$. Natomiast w przypadku (2), $|x| = x$, więc $|x| < a \iff x < a$, czyli $0 \leqslant x < a$. Ostatecznie mamy zatem, że $|x| < a \iff -a < x < a$. □

Własność 5.23. *Dla dowolnej liczby naturalnej n i dla dowolnych $x_1, x_2, \ldots, x_n \in K$ zachodzi następująca nierówność:*

$$|x_1 + x_2 + \ldots + x_n| \leqslant |x_1| + |x_2| + \ldots + |x_n|. \tag{5.11}$$

Dowód. Zastosujemy indukcję względem naturalnego n. Dla $n = 1$ nierówność (5.11) jest oczywista. Załóżmy, że ta nierówność zachodzi dla pewnego naturalnego n przy dowolnych $x_1, \ldots, x_n \in K$. Weźmy dowolne $x_1, \ldots, x_n, x_{n+1} \in K$. Wtedy $x_1 + \ldots + x_n + x_{n+1} = (x_1 + \ldots + x_n) + x_{n+1}$, więc z nierówności trójkąta otrzymujemy, że $|x_1 + \ldots + x_n + x_{n+1}| \leqslant |x_1 + \ldots + x_n| + |x_{n+1}|$. Stąd i z założenia indukcyjnego, $|x_1 + \ldots + x_n + x_{n+1}| \leqslant |x_1| + \ldots + |x_n| + |x_{n+1}|$. Zatem nierówność (5.11) zachodzi wówczas dla liczby $n + 1$.

Wobec tego na mocy zasady indukcji matematycznej nierówność (5.11) zachodzi dla dowolnego $n \in \mathbb{N}$. □

Własność 5.24. *Dla dowolnych liczb całkowitych m i n mamy, że $n \cdot 1 < m \cdot 1 \iff n < m$.*

Dowód. Na mocy własności 5.10 jest $n \cdot 1 < m \cdot 1 \iff n \cdot 1 - m \cdot 1 < 0$, ale ze stwierdzenia 1.41 mamy, że $n \cdot 1 - m \cdot 1 = (n - m) \cdot 1$, więc $n \cdot 1 < m \cdot 1 \iff (n-m) \cdot 1 < 0$. Dalej, z własności 5.3 i 5.5 uzyskujemy, że $(n - m) \cdot 1 < 0 \iff n - m < 0$, więc $n \cdot 1 < m \cdot 1 \iff n < m$. □

Stwierdzenie 1.41 i własność 5.24 pokazują, że w ciele K dla $n \in \mathbb{Z}$ można dokonać utożsamienia elementu $n \cdot 1$ z liczbą całkowitą n:

$$n \cdot 1 \equiv n \text{ dla } n \in \mathbb{Z}. \tag{5.12}$$

Przy tym utożsamieniu $\mathbb{Z} \subseteq K$, przy czym relacja mniejszości w $\mathbb{Z}$ i relacja mniejszości $<$ w ciele K obcięta do zbioru $\mathbb{Z}$ są identyczne. Od tej pory będziemy używali nieustannie tego utożsamienia. Konsekwencją tego utożsamienia jest też następujące utożsamienie:

$$\frac{k \cdot 1}{n \cdot 1} \equiv \frac{k}{n} \text{ dla } k \in \mathbb{Z},\ n \in \mathbb{N}. \tag{5.13}$$

Wobec tego dalej będziemy traktowali ciało uporządkowane liczb wymiernych $\mathbb{Q}$ jako podzbiór zbioru K, przy czym uporządkowanie $<$ w K obcięte do $\mathbb{Q}$ pokrywa się z naturalną relacją mniejszości w $\mathbb{Q}$.

Definicja 5.25. Niech A i B będą niepustymi podzbiorami zbioru K. Wówczas określamy:
(i) $A + B = \{a + b : a \in A,\ b \in B\}$,
(ii) $A \cdot B = \{a \cdot b : a \in A,\ b \in B\}$,
(iii) $-A = \{-a : a \in A\}$.

Lemat 5.26. *Dla dowolnych $a, b \in K$:*

$$\{z \in K : z < a + b\} = \{x \in K : x < a\} + \{y \in K : y < b\}.$$

Dowód. Weźmy dowolne $z_0 \in K$. Załóżmy, że $z_0 < a+b$. Wtedy $z_0 - b < a$. Zatem z własności 5.7, istnieje $u \in K$ takie, że $z_0 - b < u < a$. Stąd $u \in \{x \in K : x < a\}$ i $z_0 - u < b$, a zatem $z_0 - u \in \{y \in K : y < b\}$. Ponadto $z_0 = u + (z_0 - u)$, więc $z_0 \in \{x \in K : x < a\} + \{y \in K : y < b\}$.

Na odwrót. Załóżmy, że $z_0 \in \{x \in K : x < a\} + \{y \in K : y < b\}$. Wtedy $z_0 = u + v$ dla pewnych $u \in \{x \in K : x < a\}$ i $v \in \{y \in K : y < b\}$, skąd $u < a$ i $v < b$, więc z własności 5.14, $u + v < a + b$, czyli $z_0 < a + b$, a zatem $z_0 \in \{z \in K : z < a + b\}$. □

Lemat 5.27. *Dla dowolnych $a, b \in K$ takich, że $a > 0$ i $b > 0$:*

$$\{z \in K : 0 < z < ab\} = \{x \in K : 0 < x < a\} \cdot \{y \in K : 0 < y < b\}.$$

Dowód. Weźmy dowolne $z_0 \in K$. Załóżmy, że $0 < z_0 < a \cdot b$. Ponieważ $b > 0$, więc wtedy $0 < \frac{z_0}{b} < a$. Zatem z własności 5.7, istnieje $u \in K$ takie, że $\frac{z_0}{b} < u < a$. Stąd $u \in \{x \in K : 0 < x < a\}$ i $0 < \frac{z_0}{u} < b$, a zatem $\frac{z_0}{u} \in \{y \in K : 0 < y < b\}$. Ale $z_0 = u \cdot \frac{z_0}{u}$, więc $z_0 \in \{x \in K : 0 < x < a\} \cdot \{y \in K : 0 < y < b\}$.

Na odwrót. Załóżmy, że $z_0 \in \{x \in K : 0 < x < a\} \cdot \{y \in K : 0 < y < b\}$. Wtedy $z_0 = u \cdot v$ dla pewnych $u \in \{x \in K : 0 < x < a\}$ i $v \in \{y \in K : 0 < y < b\}$, skąd $0 < u < a$ i $0 < v < b$, więc z własności 5.15, $0 < u \cdot v < a \cdot b$, czyli $0 < z_0 < a \cdot b$, a zatem $z_0 \in \{z \in K : 0 < z < ab\}$. □

5.2 Kres górny i kres dolny

Definicja 5.28. Niech X będzie niepustym podzbiorem zbioru K. Mówimy, że $a \in K$ **ogranicza z góry zbiór** X, jeżeli $x \leqslant a$ dla każ-

dego $x \in X$. Zbiór X nazywamy **ograniczonym z góry**, gdy istnieje element $a \in K$ ograniczający ten zbiór z góry.

Definicja 5.29. Niech X będzie niepustym podzbiorem zbioru K ograniczonym z góry. Mówimy, że $a_0 \in K$ jest **kresem górnym** zbioru X, jeżeli a_0 ogranicza z góry zbiór X i dla każdego $a \in K$ takiego, że $a < a_0$ istnieje $x \in X$ takie, że $x > a$. Kres górny zbioru X oznaczamy symbolem $\sup(X)$.

Własność 5.30. *Niech X będzie niepustym podzbiorem zbioru K ograniczonym z góry. Wówczas* $\sup(X)$ *jest najmniejszym elementem ciała K ograniczającym zbiór X z góry.*

Dowód. Oczywiście $x \leqslant \sup(X)$ dla każdego $x \in X$. Załóżmy, że $a \in K$ ogranicza z góry zbiór X. Jeśli nie jest prawdą, że $\sup(X) \leqslant a$, to $a < \sup(X)$, więc istnieje $x_0 \in X$ takie, że $x_0 > a$ i mamy sprzeczność z założeniem, że a ogranicza zbiór X z góry. Wobec tego musi być $\sup(X) \leqslant a$, czyli $\sup(X)$ jest najmniejszym elementem ograniczającym zbiór X z góry.

Na odwrót, załóżmy, że $c \in K$ jest najmniejszym elementem ograniczającym zbiór X z góry. Weźmy dowolne $a \in K$ takie, że $a < c$. Wtedy z minimalności c mamy, że a nie ogranicza zbioru X z góry, więc istnieje $x \in X$ takie, że $x > a$. Wobec tego $c = \sup(X)$. □

Definicja 5.31. Niech X będzie niepustym podzbiorem zbioru K. Mówimy, że $c \in K$ **ogranicza z dołu zbioru** X, jeżeli $c \leqslant x$ dla każdego $x \in X$. Zbiór X nazywamy **ograniczonym z dołu**, gdy istnieje element $c \in K$ ograniczający ten zbiór z dołu.

Definicja 5.32. Niech X będzie niepustym podzbiorem zbioru K ograniczonym z dołu. Mówimy, że $c_0 \in K$ jest **kresem dolnym** zbioru X, jeżeli c_0 ogranicza z dołu zbiór X i dla każdego $a \in K$ takiego, że $c_0 < a$ istnieje $x \in X$ takie, że $x < a$. Kres dolny zbioru X oznaczamy symbolem $\inf(X)$.

Własność 5.33. *Niech X będzie niepustym podzbiorem zbioru K ograniczonym z dołu. Wówczas* $\inf(X)$ *jest największym elementem ciała K ograniczającym zbiór X z dołu.*

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Oczywiście $\inf(X) \leqslant x$ dla każdego $x \in X$. Załóżmy, że $a \in K$ ogranicza z dołu zbiór X. Jeśli nie jest prawdą, że $a \leqslant \inf(X)$, to $a > \inf(X)$, więc istnieje $x_0 \in X$ takie, że $x_0 < a$ i mamy sprzeczność z założeniem, że a ogranicza zbiór X z dołu. Wobec tego musi być $a \leqslant \inf(X)$, czyli $\inf(X)$ jest największym elementem ograniczającym zbiór X z dołu.

Na odwrót, załóżmy, że $c \in K$ jest największym elementem ograniczającym zbiór X z dołu. Weźmy dowolne $a \in K$ takie, że $a > c$. Wtedy z maksymalności c mamy, że a nie ogranicza zbioru X z dołu, więc istnieje $x \in X$ takie, że $a > x$. Wobec tego $c = \inf(X)$. □

Przykład 5.34. Wyznaczymy kres górny i kres dolny podzbioru $A = \{\frac{m}{m+n} \ : \ m, n \in \mathbb{N}\}$ ciała uporządkowanego liczb wymiernych. Ponieważ dla $m, n \in \mathbb{N}$ jest $m < m + n$, więc $\frac{m}{n+m} < 1$. Wobec tego liczba 1 ogranicza z góry zbiór A. Ponadto $1 \notin A$, bo $m \neq m + n$ dla wszystkich $m, n \in \mathbb{N}$. Weźmy dowolną liczbę wymierną a, która ogranicza zbiór A z góry i załóżmy, że $a < 1$. Ponieważ $\frac{1}{2} \in A$, więc $\frac{1}{2} \leqslant a$, skąd $a > 0$. Wobec tego istnieją liczby naturalne p, q takie, że $a = \frac{p}{q}$. Ale $a < 1$, więc $p < q$. Stąd $q \geqslant p+1$, więc $q = p+n$ dla pewnego $n \in \mathbb{N}$. Stąd $\frac{p+1}{q+1} \in A$ oraz $\frac{p+1}{q+1} - a = \frac{p+1}{q+1} - \frac{p}{q} = \frac{(p+1)q-(q+1)p}{q(q+1)} = \frac{q-p}{q(q+1)} > 0$, czyli $\frac{p+1}{q+1} > a$ i mamy sprzeczność. Wobec tego $\sup(A) = 1$. Jest jasne, że 0 ogranicza zbiór A z dołu i $0 \notin A$. Pokażemy, że $0 = \inf(A)$. Gdyby tak nie było, to pewna dodatnia liczba wymierna b ograniczałaby zbiór A z dołu. Ale wtedy $b = \frac{t}{s}$ dla pewnych $t, s \in \mathbb{N}$, a ponieważ $\frac{1}{2} \in A$, więc $\frac{t}{s} \leqslant \frac{1}{2} < 1$, skąd $t < s$. Stąd $\frac{t}{s+1} \in A$ oraz $\frac{t}{s+1} < \frac{t}{s} = b$ i mamy sprzeczność. Wobec tego $\inf(A) = 0$.

Przykład 5.35. Wyznaczymy kres górny i kres dolny podzbioru $A = \{\frac{1}{n} - \frac{2}{m} \ : \ m, n \in \mathbb{N}\}$ ciała uporządkowanego liczb wymiernych. Dla dowolnych $m, n \in \mathbb{N}$ mamy, że $\frac{1}{n} - \frac{2}{m} \leqslant 1 - \frac{2}{m} < 1$, czyli liczba 1 ogranicza z góry zbiór A. Załóżmy, że istnieje liczba wymierna $a < 1$, która ogranicza z góry zbiór A. Wtedy $a \geqslant \frac{1}{1} - \frac{2}{4} = \frac{1}{2}$, czyli $\frac{1}{2} \leqslant a < 1$. Ale dla $m \in \mathbb{N}$ mamy, że $1 - \frac{2}{2m} \in A$, więc $1 - \frac{1}{m} \in A$. Stąd $1 - \frac{1}{m} \leqslant a$ dla każdego $m \in \mathbb{N}$. Zatem $\frac{1}{m} > 1 - a$ i $m < \frac{1}{1-a}$ dla każdego $m \in \in \mathbb{N}$, co przeczy stwierdzeniu 2.22. Uzyskana sprzeczność pokazuje, że

nie istnieje ograniczenie górne zbioru A mniejsze od 1. Wobec tego $\sup(A) = 1$.

Ponadto, dla $m, n \in \mathbb{N}$: $\frac{1}{n} - \frac{2}{m} > \frac{-2}{m} \geqslant -2$, więc liczba -2 ogranicza z dołu zbiór A. Ponadto, dla $n \in \mathbb{N}$ mamy, że $\frac{1}{n} - \frac{2}{1} \in A$, czyli $-2 + \frac{1}{n} \in A$. Weźmy dowolna liczbę wymierną $c > -2$. Wtedy $c + 2$ jest dodatnią liczbą wymierną, więc $c + 2 = \frac{p}{q}$ dla pewnych $p, q \in \mathbb{N}$, skąd $c + 2 \geqslant \frac{1}{q} > \frac{1}{q+1}$, a zatem $c > -2 + \frac{1}{q+1}$, co oznacza, że c nie ogranicza z dołu zbioru A. Wobec tego $\inf(A) = -2$.

Lemat 5.36. *Niech A i B będą niepustymi podzbiorami zbioru K. Jeżeli istnieją $\sup A \in K$ i $\sup B \in K$, to istnieje też $\sup(A + B)$ oraz $\sup(A + B) = \sup A + \sup B$.*

Dowód. Weźmy dowolne $x \in A + B$. Wtedy $x = a + b$ dla pewnych $a \in A$ i $b \in B$. Stąd $a \leqslant \sup A$ i $b \leqslant \sup B$, więc z własności 5.14, $a + b \leqslant \sup A + \sup B$, czyli $x \leqslant \sup A + \sup B$. Zatem $\sup A + \sup B$ ogranicza zbiór $A+B$ z góry. Jeśli $\sup A+\sup B$ nie jest kresem górnym zbioru $A+B$, to istnieje $\alpha \in K$ takie, że α ogranicza zbiór $A+B$ z góry i $\alpha < \sup A+\sup B$. Z lematu 5.26 istnieją $p, q \in K$ takie, że $\alpha = p+q$ oraz $p < \sup A$ i $q < \sup B$. Stąd z definicji kresu górnego istnieją $a \in A$ i $b \in B$ takie, że $p < a$ i $q < b$. Zatem z własności 5.14, $p + q < a + b$, czyli $\alpha < a + b$. Ale $a + b \in A + B$ i α ogranicza z góry zbiór $A + B$, więc mamy sprzeczność. Wobec tego $\sup A + \sup B = \sup(A + B)$. □

Lemat 5.37. *Niech A i B będą niepustymi podzbiorami zbioru K takimi, że $a > 0$ dla każdego $a \in A$ i $b > 0$ dla każdego $b \in B$. Jeżeli istnieją $\sup A \in K$ i $\sup B \in K$, to $\sup A > 0$, $\sup B > 0$ i istnieje też $\sup(A \cdot B)$ oraz $\sup(A \cdot B) = \sup A \cdot \sup B$.*

Dowód. Ponieważ $a > 0$ dla każdego $a \in A$ i $\sup A$ ogranicza zbiór A z góry, więc $\sup A > 0$. Analogicznie pokazujemy, że $\sup B > 0$. Weźmy dowolne $x \in A \cdot B$. Wtedy $x = a \cdot b$ dla pewnych $a \in A$ i $b \in B$. Stąd $0 < a \leqslant \sup A$ i $0 < b \leqslant \sup B$, więc z własności 5.15, $0 < a \cdot b \leqslant \sup A \cdot \sup B$, czyli $0 < x \leqslant \sup A \cdot \sup B$. Zatem $\sup A \cdot \sup B$ ogranicza zbiór $A \cdot B$ z góry. Jeśli $\sup A \cdot \sup B$ nie jest kresem górnym zbioru $A \cdot B$, to istnieje $\alpha \in K$ takie, że α ogranicza zbiór $A \cdot B$ z góry i $\alpha < \sup A \cdot \sup B$. Stąd $\alpha > 0$ i z lematu 5.27

istnieją $p, q \in K$ takie, że $\alpha = p \cdot q$ oraz $0 < p < \sup A$ i $0 < q < \sup B$. Stąd z definicji kresu górnego istnieją $a \in A$ i $b \in B$ takie, że $p < a$ i $q < b$. Zatem z własności 5.15, $p \cdot q < a \cdot b$, czyli $\alpha < a \cdot b$. Ponadto $a \cdot b \in A \cdot B$ i α ogranicza z góry zbiór $A \cdot B$, więc mamy sprzeczność. Wobec tego $\sup A \cdot \sup B = \sup(A \cdot B)$. □

Lemat 5.38. *Niech A będzie niepustym podzbiorem zbioru K. Wówczas:*

(i) jeżeli istnieje $\sup A$*, to istnieje* $\inf(-A)$ *i* $\inf(-A) = -\sup A$*,*

(ii) jeżeli istnieje $\inf A$*, to istnieje* $\sup(-A)$ *i* $\sup(-A) = -\inf A$*.*

Dowód. (i). Weźmy dowolne $x \in -A$. Wtedy $x = -a$ dla pewnego $a \in A$. Stąd $a \leqslant \sup A$, więc $-a \geqslant -\sup A$, czyli $x \geqslant -\sup A$. Zatem $-\sup A$ ogranicza z dołu zbiór $-A$. Załóżmy, że $-\sup A$ nie jest kresem dolnym zbioru $-A$. Wtedy istnieje $\alpha \in K$ ograniczająca z dołu zbiór $-A$ i taka, że $\alpha > -\sup A$. Stąd $-\alpha < \sup A$, więc z definicji kresu górnego istnieje $a \in A$ takie, że $-\alpha < a$, skąd $\alpha > -a$. Ale $-a \in -A$, więc mamy sprzeczność z tym, że α ogranicza z dołu zbiór $-A$. Wobec tego $-\sup A$ jest kresem dolnym zbioru $-A$, czyli $\inf(-A) = -\sup A$.

(ii). Weźmy dowolne $x \in -A$. Wtedy $x = -a$ dla pewnego $a \in A$. Stąd $a \geqslant \inf A$, więc $-a \leqslant -\inf A$, czyli $x \leqslant -\inf A$. Zatem $-\inf A$ ogranicza z góry zbiór $-A$. Załóżmy, że $-\inf A$ nie jest kresem górnym zbioru $-A$. Wtedy istnieje $\alpha \in K$ ograniczająca z góry zbiór $-A$ i taka, że $\alpha < -\inf A$. Stąd $-\alpha > \inf A$, więc z definicji kresu dolnego istnieje $a \in A$ takie, że $-\alpha > a$, skąd $\alpha < -a$. Ale $-a \in -A$, więc mamy sprzeczność z tym, że α ogranicza z góry zbiór $-A$. Wobec tego $-\inf A$ jest kresem górnym zbioru $-A$, czyli $\sup(-A) = -\inf A$. □

5.3 Aksjomat ciągłości

Definicja 5.39. Mówimy, że ciało uporządkowane K **spełnia aksjomat ciągłości**, jeżeli każdy niepusty podzbiór $X \subseteq K$ ograniczony z góry posiada kres górny.

Przykład 5.40. Pokażemy, że ciało uporządkowane liczb wymiernych nie spełnia aksjomatu ciągłości. Udowodnimy mianowicie, że podzbiór $A = \{a \in \mathbb{Q} : a \leqslant 0\} \cup \{a \in \mathbb{Q} : a > 0, a^2 < 2\}$ ciała $\mathbb{Q}$ jest

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

ograniczony z góry, ale nie posiada w $\mathbb{Q}$ kresu górnego. Jeżeli $a \in A$ i $a > 0$, to $a^2 < 2$, więc $a^2 < 4$, skąd $a < 2$. Wobec tego dla każdego $x \in A$ mamy, że $x \leqslant 2$ i zbiór A jest ograniczony z góry. Pokażemy, że w zbiorze A nie ma elementu największego. W tym celu wystarczy wykazać, że dla każdego $c > 0$ takiego, że $c^2 < 2$ istnieje $n \in \mathbb{N}$ takie, że $(c+\frac{1}{n})^2 < 2$. Ale $(c+\frac{1}{n})^2 = c^2+2\frac{c}{n}+\frac{1}{n^2} \leqslant c^2+2\frac{c}{n}+\frac{1}{n} = c^2+(2c+1)\cdot\frac{1}{n}$, więc wystarczy aby $c^2+(2c+1)\cdot\frac{1}{n} < 2$, czyli $n > \frac{2c+1}{2-c^2}$, a takie n można dobrać na mocy stwierdzenia 2.22.

Wobec tego, jeśli liczba wymierna c ogranicza z góry zbiór A, to $c > 0$ i $c^2 \geqslant 2$, gdyż $1 \in A$. Ponadto z przykładu 2.29 wynika, że $c^2 \neq 2$, więc $c^2 > 2$. Pokażemy, że dla pewnego $m \in \mathbb{N}$ liczba $c - \frac{1}{m}$ też ogranicza z góry zbiór A, co zakończy dowód. Ze stwierdzenia 2.22 wynika, że istnieje $m_0 \in \mathbb{N}$ takie, że $m_0 > \frac{1}{c}$, skąd dla wszystkich naturalnych $m \geqslant m_0$ jest $c - \frac{1}{m} > 0$. Szukamy takiego $m > m_0$, że $(c - \frac{1}{m})^2 > 2$. Wówczas dla każdego $x \in A$ będzie $x < c - \frac{1}{m}$, co zakończy dowód. Ale $(c - \frac{1}{m})^2 = c^2 - 2\frac{c}{m} + \frac{1}{m^2} > > c^2 - 2\frac{c}{m}$, więc wystarczy aby $c^2 - 2\frac{c}{m} > 2$, czyli aby $2\frac{c}{m} < c^2 - 2$, a więc aby $m > \frac{2c}{c^2-2}$. Wobec tego wystarczy aby $m \geqslant \max\{m_0, \frac{2c}{c^2-2}\}$, a to jest możliwe do zrealizowania na mocy stwierdzenia 2.22.

Stwierdzenie 5.41. *Niech K będzie ciałem uporządkowanym spełniającym aksjomat ciągłości. Wówczas każdy niepusty i ograniczony z dołu podzbiór X zbioru K posiada kres dolny.*

Dowód. Z założenia podzbiór A zbioru K złożony ze wszystkich ograniczeń dolnych zbioru X jest niepusty. Jest on także ograniczony z góry (na przykład przez dowolny element zbioru X). Wobec tego z aksjomatu ciągłości istnieje $\sup(A) = a \in K$. Załóżmy, że a nie ogranicza z dołu zbioru X. Wtedy $a > x$ dla pewnego $x \in X$. Ale $a = \sup(A)$, więc istnieje $b \in A$ takie, że $b > x$ i mamy sprzeczność z definicją zbioru A. Wobec tego a ogranicza z dołu zbiór X. W takim razie $a \in A$ oraz a jest największym ograniczeniem dolnym zbioru X. Zatem z własności 5.33 mamy, że $a = \inf(X)$. □

Stwierdzenie 5.42. (aksjomat Archimedesa). *Niech K będzie ciałem uporządkowanym spełniającym aksjomat ciągłości. Wówczas dla dowolnego $a \in K$ istnieje liczba naturalna n taka, że $n > a$.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje $a \in K$ taka, że $n \leqslant a$ dla każdego $n \in \mathbb{N}$. Zatem zbiór $\mathbb{N}$ jest niepusty i ograniczony z góry przez liczbę a. Wobec tego z aksjomatu ciągłości istnieje $c \in K$ takie, że $c = \sup(\mathbb{N})$. Stąd dla każdego $n \in \mathbb{N}$ jest $n + 1 \leqslant c$, skąd $n \leqslant c - 1$ dla każdego $n \in \mathbb{N}$, ale $c - 1 < c$, więc mamy sprzeczność z określeniem liczby c.

Uzyskana sprzeczność pokazuje, że dla dowolnego $a \in K$ istnieje liczba naturalna n taka, że $n > a$. □

Stwierdzenie 5.43. *Niech K będzie ciałem uporządkowanym spełniającym aksjomat ciągłości. Wówczas dla każdego $a \in K$ istnieje największa liczba całkowita k taka, że $k \leqslant a$.*

Dowód. Ze stwierdzenia 5.42 istnieje $n \in \mathbb{N}$ takie, że $n > -a$, skąd $-n < a$. Wobec tego zbiór A liczb całkowitych k takich, że $k \leqslant a$ jest niepusty. Ponadto ten zbiór jest ograniczony z góry przez a, więc z aksjomatu ciągłości istnieje $\sup(A) = c \in K$. Stąd $c \leqslant a$ na mocy własności 5.30, ale $c - 1 < c$, więc istnieje $m \in A$ takie, że $m > c - 1$. Ponadto $m \leqslant c$ i $c \leqslant a$, więc $m \leqslant a$. Jeśli $m + 1 \leqslant a$, to $m + 1 \in A$, a ponieważ $c = \sup(A)$, to $m+1 \leqslant c$. Jednak, jak pokazaliśmy, $m+1 > c$, więc mamy sprzeczność. Wobec tego $m + 1 > a$, skąd dla każdego całkowitego $k > m$ jest $k > a$. Wobec tego m jest największą liczbą w zbiorze A. □

Definicja 5.44. Niech K będzie ciałem uporządkowanym spełniającym aksjomat ciągłości. Wówczas dla każdego $a \in K$ największą liczbę całkowitą k taką, że $k \leqslant a$ nazywamy **częścią całkowitą elementu** a i oznaczamy symbolem $\lfloor a \rfloor$.

Wprost z definicji części całkowitej wynika, że dla każdego $x \in K$ zachodzą nierówności:

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1. \tag{5.14}$$

Stwierdzenie 5.45. *Niech K będzie ciałem uporządkowanym spełniającym aksjomat ciągłości. Jeżeli $a, b \in K$ i $b - a > 1$, to istnieje $k \in \mathbb{Z}$ takie, że $a < k < b$.*

Dowód. Niech $k = \lfloor a \rfloor + 1$. Ponieważ $\lfloor a \rfloor \in \mathbb{Z}$, więc $k \in \mathbb{Z}$. Ponadto z definicji części całkowitej $\lfloor a \rfloor \leqslant a < \lfloor a \rfloor + 1$, więc $a < k$. Ale $b - a > 1$, więc $a + 1 < b$ i $k - 1 \leqslant a$, czyli $k \leqslant a + 1$, skąd $k < b$. Wobec tego $a < k < b$. □

Stwierdzenie 5.46. *Niech K będzie ciałem uporządkowanym spełniającym aksjomat ciągłości. Dla dowolnych $a, b \in K$ takich, że $a < b$ istnieje liczba wymierna q taka, że $a < q < b$.*

Dowód. Z założenia $b - a > 0$, więc z własności 5.6, $\frac{1}{b-a} > 0$. Z Aksjomatu Archimedesa $n > \frac{1}{b-a}$ dla pewnego $n \in \mathbb{N}$. Stąd $n \cdot (b - a) > 1$ na mocy **P3** (b). Zatem $n \cdot b - n \cdot a > 1$ i na mocy stwierdzenia 5.45 istnieje $k \in \mathbb{Z}$ takie, że $n \cdot a < k < n \cdot b$. Stąd z **P3** (b), $a < \frac{k}{n} < b$ i wystarczy przyjąć $q = \frac{k}{n}$. □

Twierdzenie 5.47. *Niech K i L będą ciałami uporządkowanymi przez relacje $<_K$ i $<_L$ odpowiednio i spełniającymi aksjomat ciągłości. Wówczas istnieje bijekcja $F\colon K \to L$ taka, że $F(q) = q$ dla każdego $q \in \mathbb{Q}$ oraz dla dowolnych $a, b \in K$:*

(i) jeżeli $a <_K b$, to $F(a) <_L F(b)$,

(ii) $F(a + b) = F(a) + F(b)$ oraz $F(a \cdot b) = F(a) \cdot F(b)$.

Dowód. Dla niepustego podzbioru $X \subseteq \mathbb{Q}$ ograniczonego z góry przez pewną liczbę naturalną przez $\sup_K X$ oznaczmy kres góry zbioru X w ciele K, zaś przez $\sup_L X$ oznaczmy kres górny zbioru X w ciele L. Oba kresy są elementami odpowiednich ciał, gdyż te ciała spełniają aksjomat ciągłości. Analogicznie dla niepustego podzbioru $Y \subseteq \mathbb{Q}$ ograniczonego z dołu przez pewną liczbę całkowitą definiujemy $\inf_K Y$ i $\inf_L Y$.

Dla $a \in K$ oznaczmy $X(a) = \{q \in \mathbb{Q} : q <_K a\}$ i $Y(a) = \{q \in \mathbb{Q} : a \leqslant_K q\}$. Udowodnimy najpierw kilka użytecznych własności zbiorów $X(a)$ i $X(b)$.

$$\forall_{a \in K} \;\; X(a) \neq \emptyset,\; Y(a) \neq \emptyset,\; X(a) \cap Y(a) = \emptyset,\; X(a) \cup Y(a) = \mathbb{Q}. \tag{5.15}$$

Rzeczywiście, $a - 1 <_K a$, więc z własności 5.7 istnieje $q \in \mathbb{Q}$ takie, że $a - 1 <_K q <_K a$, skąd $q \in X(a)$ i $X(a) \neq \emptyset$. Ponadto, $a <_K a + 1$,

więc z własności 5.7, $a <_K u <_K a+1$ dla pewnego $u \in \mathbb{Q}$, czyli $Y(a) \neq \emptyset$. Jeśli $p \in X(a)$ i $s \in Y(q)$, to $p <_K a$ i $a \leqslant_K s$, skąd $p <_K s$. Stąd w szczególności $X(a) \cap Y(a) = \emptyset$. W końcu, z **P1** wynika, że $X(a) \cup Y(a) = \mathbb{Q}$.

Teraz wykażemy, że:

$$\text{Dla każdego } a \in K: \ \sup_L X(a) = \inf_L Y(a) \in L. \tag{5.16}$$

Z aksjomatu Archimedesa istnieje $n \in \mathbb{N}$ takie, że $a <_K n$, skąd dla każdego $u \in X(a)$ jest $u <_K n$, a stąd $u < n$. Zatem $u <_L n$, czyli n ogranicza z góry zbiór $X(a)$ w ciele L. Z aksjomatu ciągłości istnieje zatem $\sup_L X(a) \in L$. Ze stwierdzenia 5.43 istnieje $k \in \mathbb{Z}$ takie, że $k \leqslant_K a$, skąd dla $w \in Y(a)$ mamy: $k \leqslant_K w$, czyli $k < w$. Zatem $k <_L w$, czyli k ogranicza z dołu zbiór $Y(a)$ w ciele L i z aksjomatu ciągłości istnieje $\inf_L Y(a) \in L$. Weźmy dowolne $p \in X(a)$ i $q \in Y(a)$. Wtedy $p <_K a \leqslant_K q$, więc $p <_K q$, skąd $p < q$, a więc $p <_L q$. Wobec tego $p \leqslant_L \inf_L Y(a)$, skąd wobec dowolności p, $\sup_L X(a) \leqslant_L \inf_L Y(a)$. Załóżmy, że $\sup_L X(a) <_L \inf_L Y(a)$. Wtedy z własności 5.7 istnieje $s \in \mathbb{Q}$ takie, że $\sup_L X(a) <_L s <_L \inf_L Y(a)$. Stąd dla $w \in X(a)$ jest $w \leqslant_L \sup_L X(a) <_L s$, czyli $w <_L s$, więc $s \notin X(a)$ i z (5.15), $s \in Y(a)$ oraz $s <_L \inf_L Y(a)$, co prowadzi do sprzeczności. Wobec tego $\sup_L X(a) = \inf_L Y(a)$.

Teraz udowodnimy, że:

$$\text{Dla każdego } a \in \mathbb{Q}: \ \sup_L X(a) = \inf_L Y(a) = a. \tag{5.17}$$

Rzeczywiście, z (5.16) wynika, że $\sup_L X(a) = \inf_L Y(a)$. Ale $a \in Y(a)$, bo $a \in \mathbb{Q}$ i $a \leqslant a$, więc $a \leqslant_L a$. Zatem a jest najmniejszym elementem zbioru $Y(a)$, skąd $\inf_L Y(a) = a$.

Niech dla $a \in K$: $F(a) = \sup_L X(a) = \inf_L Y(a)$. Wtedy F jest funkcją ze zbioru K w zbiór L i na mocy (5.17), $F(w) = w$ dla każdego $w \in \mathbb{Q}$.

Weźmy teraz dowolne $a, b \in K$ takie, że $a <_K b$. Wtedy z własności 5.7 istnieją $u, v \in \mathbb{Q}$ takie, że $a <_K u <_K v <_K b$. Stąd dla każdego $x \in X(a)$: $x <_K u$, więc $x < u$, gdyż $x, u \in \mathbb{Q}$, skąd $x <_L u$. Zatem z dowolności x, $F(a) \leqslant u$. Ponadto dla każdego $y \in Y(b)$ jest $v <_K y$,

skąd $v < y$, bo $v, y \in \mathbb{Q}$, czyli $v <_L y$. Zatem z dowolności y, $v \leqslant_L F(b)$. Ponadto $u < v$, więc $u <_L$. Zatem $F(a) \leqslant_L u <_L v \leqslant_L F(b)$, skąd $F(a) <_L F(b)$, co dowodzi (i) oraz pokazuje, że funkcja F jest różnowartościowa.

Teraz udowodnimy, że funkcja F jest „na". W tym celu weźmy dowolne $y \in L$ i niech $X = \{q \in \mathbb{Q} : q <_L y\}$. Wtedy z przedstawionego wyżej rozumowania dla ciała K wynika, że zbiór X jest ograniczony z góry w ciele $\mathbb{Q}$, a stąd X jest ograniczony z góry w ciele K. Istnieje zatem $a = \sup_K X \in K$. Weźmy dowolne $w \in \mathbb{Q}$. Jeśli $w <_K a$, to istnieje $x \in X$ takie, że $w <_K x$. Stąd $w < x$, więc $w <_L x$ i $x <_L y$, skąd $w <_L y$, a zatem $w \in X$. Jeżeli zaś $w <_L y$, to z własności 5.7 istnieje $u \in \mathbb{Q}$ takie, że $w <_L u <_L y$. Zatem $u \in X$, skąd $u \leqslant_K a$. Wobec tego $w < u$, skąd $w <_K u \leqslant_K a$, skąd $w <_K a$. W ten sposób pokazaliśmy, że $X = \{w \in \mathbb{Q} : w <_K a\}$. Stąd $F(a) = \sup_L X$. Ale y ogranicza z góry w ciele L zbiór X i jeśli $t \in L$ jest takie, że $t <_L y$, to z wniosku 5.7 istnieje $w \in \mathbb{Q}$ takie, że $t <_L w <_L y$, więc $w \in X$ i y jest najmniejszym elementem w L ograniczającym zbiór X z góry, czyli $y = \sup_L X$. Wobec tego $y = F(a)$ i funkcja F jest „na". Kończy to dowód tego, że funkcja F jest bijekcją.

Teraz pokażemy, że $F(a+b) = F(a)+F(b)$ dla dowolnych $a, b \in K$. Z dowodu lematu 5.26 wynika, że $X(a+b) = X(a)+X(b)$, więc na mocy lematu 5.36, $\sup_L X(a+b) = \sup_L X(a) + \sup_L X(b)$, a to oznacza, że $F(a+b) = F(a)+F(b)$. Ale $F(q) = q$ dla $q \in \mathbb{Q}$, więc $F(0) = 0$. Zatem $0 = F(a + (-a)) = F(a) + F(-a)$, skąd otrzymujemy, że:

$$\text{Dla każdego } a \in K : \ F(-a) = -F(a). \tag{5.18}$$

Pozostaje do wykazania, że $F(a \cdot b) = F(a) \cdot F(b)$ dla dowolnych $a, b \in K$. Ponieważ $F(0) = 0$, więc wystarczy rozważać $a \neq 0$ i $b \neq 0$. Niech najpierw $a_K > 0$ i $b_K > 0$. Dla $x \in K$ takich, że $x > 0$ niech $A(x) = \{w \in \mathbb{Q} : 0 <_K x <_K a\}$. Wówczas $\sup_L A(x) = \sup_L X(x) = F(x)$. Stąd i z dowodu lematu 5.27, $F(a \cdot b) = \sup_L A(a \cdot b) = \sup_L A(a) \cdot A(b) = \sup_L A(a) \cdot \sup_L A(b) = F(a) \cdot F(b)$, czyli $F(a \cdot b) = F(a) \cdot F(b)$. Wobec tego:

$$F(a \cdot b) = F(a) \cdot F(b), \ \text{ jeżeli } 0 <_K a \ , 0 <_K b. \tag{5.19}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Jeśli $0 <_K a$ i $b <_K 0$, to $0 <_K -b$ i $b = -(-b)$ oraz $a \cdot b = -[a \cdot (-b)]$, więc ze wzorów (5.18) i (5.19) mamy, że $F(a \cdot b) = -F(a \cdot (-b)) = -[F(a) \cdot F(-b)] = -[F(a) \cdot (-F(b))] = F(a) \cdot F(b)$.

Jeżeli $a <_K 0$ i $0 <_K b$, to analogicznie pokazujemy, że $F(a \cdot b) = F(a) \cdot F(b)$.

W końcu, niech $a <_K 0$ o $b <_K 0$. Wtedy $a = -(-a)$, $b = -(-b)$, $0 <_K -a$ i $0 <_K -b$ oraz $a \cdot b = (-a) \cdot (-b)$, więc ze wzorów (5.18) i (5.19) mamy, że $F(a \cdot b) = F((-a) \cdot (-b)) = F(-a) \cdot F(-b) = [-F(a)] \cdot [-F(b)] = F(a) \cdot F(b)$. □

Udowodnione twierdzenie pokazuje, że z dokładnością do izomorfizmu ciał zachowującego porządek może istnieć co najwyżej jedno ciało uporządkowane spełniające aksjomat ciągłości. Ma więc sens następująca:

Definicja 5.48. Ciałem liczb rzeczywistych nazywamy takie ciało uporządkowane, które spełnia aksjomat ciągłości.

W następnym rozdziale zostanie przedstawiona konstrukcja Dedekinda ciała liczb rzeczywistych.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 6

Konstrukcja Dedekinda ciała liczb rzeczywistych

Pierwsza konstrukcja liczb rzeczywistych z wymiernych jest dziełem niemieckiego matematyka Richarda Dedekinda, który żył w latach 1831 - 1916. Badacz rozwinął tę ideę po raz pierwszy w 1858 roku, choć opublikował ją dopiero w 1872 roku. Tak napisał na początku artykułu [9] w którym ją przedstawiał:

> "Jako profesor Politechniki w Zurychu wykładając po raz pierwszy idee rachunku różniczkowego, bardziej niż kiedykolwiek odczuwałem brak prawdziwie naukowych podstaw arytmetyki. Omawiając pojęcie zbliżania się wielkości zmiennej do ustalonej wartości granicznej, a zwłaszcza dowodząc twierdzenia, że każda wielkość, która rośnie w sposób ciągły, ale nie przekraczając określonej wartości, musi z pewnością zbliżać się do wartości granicznej, odwołałem się do dowodów geometrycznych. (...) To uczucie niezadowolenia było tak obezwładniające, że postanowiłem kontynuować badania w tej kwestii, aż znajdę czysto arytmetyczną i doskonale rygorystyczną podstawę dla zasad analizy nieskończenie małych."

Dedekind zdefiniował liczbę rzeczywistą jako parę (L, R) zbiorów liczb wymiernych, które mają następujące właściwości: Każda liczba

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

wymierna należy do dokładnie jednego ze zbiorów L lub R. Każda liczba wymierna z L jest mniejsza od każdej liczby wymiernej z R.

Taka para nazywana jest przekrojem Dedekinda (po niemiecku Schnitt). Jest raczej długim (i żmudnym) zadaniem zdefiniowanie operacji arytmetycznych i relacji porządku na takich przekrojach oraz sprawdzenie, czy spełniają one aksjomaty ciała. Uwspółcześnione szczegóły tej konstrukcji zostaną przedstawione w niniejszym rozdziale.

Richard Dedekind był jednym z ostatnich studentów Gaussa. Jego „arytmetyzacja analizy" była jego najważniejszym wkładem w matematykę, ale nie została entuzjastycznie przyjęta przez czołowych matematyków jego czasów, zwłaszcza Kroneckera i Weierstrassa. Jego pomysły zostały jednak ciepło przyjęte przez Jordana, a zwłaszcza przez Cantora, z którym się przyjaźnił.

6.1 Przekroje Dedekinda

Definicja 6.1. Przekrojem Dedekinda nazywamy niepusty i właściwy podzbiór A zbioru liczb wymiernych $\mathbb{Q}$ nieposiadający elementu największego i taki, że wraz z każdą liczbą należącą do niego zawiera każdą liczbę wymierną od niej mniejszą.

Wobec tego $A \subseteq \mathbb{Q}$ jest przekrojem Dedekinda wtedy i tylko wtedy, gdy spełnione są następujące warunki:

D1. $A \neq \emptyset$ i $A \neq \mathbb{Q}$,

D2. dla każdego $a \in A$ istnieje $b \in A$ takie, że $a < b$,

D3. jeżeli $a \in A$ i $q \in \mathbb{Q}$ oraz $q < a$, to $q \in A$.

Przykład 6.2. Zauważmy, że dla dowolnej liczby wymiernej a zbiór

$$a^* = \{q \in \mathbb{Q} : q < a\} \tag{6.1}$$

jest przekrojem Dedekinda. Rzeczywiście, $a - 1 < a$, więc $a - 1 \in a^*$, skąd $a^* \neq \emptyset$ oraz $a < a + 1$, więc $a + 1 \notin a^*$, czyli $a^* \neq \mathbb{Q}$. Weźmy dowolne $x \in a^*$. Wtedy $x \in \mathbb{Q}$ i $x < a$, więc $\frac{x+a}{2} \in \mathbb{Q}$ oraz $x < \frac{x+a}{2} < a$, czyli $\frac{x+a}{2} \in a^*$ i warunek **D2** jest też spełniony. Ponadto dla wymiernych $y < x$ mamy, że $y < a$, więc $y \in a^*$, a to oznacza, że **D3** też zachodzi.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 6.3. *Niech A będzie dowolnym przekrojem Dedekinda. Wówczas:*

(i) zbiór A jest ograniczony z góry przez każdą liczbę wymierną nie należącą do A,

(ii) dla każdego $n \in \mathbb{N}$ istnieje dokładnie jedna liczba całkowita k taka, że $\frac{k}{n} \in A$ oraz $\frac{k+1}{n} \notin A$,

(iii) dla każdego $n \in \mathbb{N}$ istnieje $q \in \mathbb{Q}$ takie, że $(q - \frac{1}{n})^* \subset A \subset (q + \frac{1}{n})^*$.

Dowód. (i). Z **D1** wynika, że istnieją liczby wymierne, które nie należą do A i niech w będzie dowolną z tych liczb. Weźmy dowolne $a \in A$. Wtedy $a \neq w$, więc $a < w$ lub $w < a$. Ale w drugim przypadku na mocy **D3**, $w \in A$, wbrew założeniu, więc $a < w$. Zatem w ogranicza z góry zbiór A.

(ii). Weźmy dowolne $n \in \mathbb{N}$ i dowolne $w \in \mathbb{Q} \setminus A$. Wtedy na mocy (i), $a < w$ dla każdego $a \in A$. Z **D1** istnieje liczba wymierna $a_0 \in A$. Wtedy $[a_0] \in \mathbb{Z}$ i $[a_0] \leqslant a_0$, więc z **D3**, $[a_0] \in A$, skąd $\frac{n[a_0]}{n} \in A$. Wobec tego zbiór C wszystkich liczb całkowitych l takich, że $\frac{l}{n} \in A$ jest niepusty. Ponadto wtedy $\frac{l}{n} < w$, więc $l < nw$, co oznacza, że zbiór C jest ograniczony z góry. Z zasady maksimum wynika, że w zbiorze C istnieje liczba największa k. Wtedy $\frac{k}{n} \in A$ oraz $\frac{k+1}{n} \notin A$. Ponadto dla liczb całkowitych t: jeśli $t < k$, to $t + 1 \leqslant k$, skąd $\frac{t+1}{n} \leqslant \frac{k}{n}$ i na mocy **D3**, $\frac{t+1}{n} \in A$, zaś dla $t > k$ jest $t \geqslant k + 1$, więc $\frac{t}{n} \geqslant \frac{k+1}{n}$, a ponieważ $\frac{k+1}{n} \notin A$, to z **D3**, $\frac{t}{n} \notin A$. Wobec tego k jest jedyną liczbą całkowitą, dla której $\frac{k}{n} \in A$ oraz $\frac{k+1}{n} \notin A$.

(iii). Weźmy dowolne $n \in \mathbb{N}$. Na mocy (ii) istnieje $k \in \mathbb{Z}$ takie, że $q = \frac{k}{2n} \in A$ i $q + \frac{1}{2n} \notin A$. Zatem na mocy (i) dla każdego $a \in A$ mamy, że $a < q + \frac{1}{2n}$, a ponieważ $q + \frac{1}{2n} < q + \frac{1}{n}$, więc $A \subset (q + \frac{1}{n})^*$. Ponadto jeśli $w \in \mathbb{Q}$ i $w < q - \frac{1}{n}$, to $w < q - \frac{1}{2n}$, skąd $w \in A$. Zatem $(q - \frac{1}{n})^* \subseteq A$. Ale $q \in A$ i $q \notin (q - \frac{1}{n})^*$, więc $(q - \frac{1}{n})^*$. □

Stwierdzenie 6.4. *Dla dowolnych przekrojów Dedekinda A i B zachodzi jedna i tylko jedna z możliwości: $A \subset B$ albo $A = B$ albo $B \subset A$.*

Dowód. Wystarczy wykazać, że jeśli $A \neq B$, to $A \subset B$ lub $B \subset A$. Załóżmy, że A nie jest zawarte w B. Wtedy istnieje $a \in A$ takie, że

$a \notin B$. Ze stwierdzenia 6.3 (i) mamy, że wtedy $b < a$ dla wszystkich $b \in B$. Stąd i z **D3**, $b \in A$ dla każdego $b \in B$, czyli $B \subseteq A$. Ale $B \neq A$, więc $B \subset A$. □

Stwierdzenie 6.5. *Dla dowolnych przekrojów Dedekinda A i B zbiór*

$$A + B = \{a + b : a \in A, b \in B\}$$

też jest przekrojem Dedekinda.

Dowód. Ponieważ $a \neq \emptyset$ i $B \neq \emptyset$, więc też $A + B \neq \emptyset$. Ponadto istnieją liczby wymierne x i y takie, że $x \notin A$ i $y \notin B$. Stąd i ze stwierdzenia 6.3 (i), $a < x$ dla każdego $a \in A$ oraz $b < y$ dla każdego $b \in B$. Zatem $a + b < x + y$ dla dowolnych $a \in A$, $b \in B$. Wobec tego $c < x + y$ dla każdego $c \in A + B$, skąd $x + y \notin A + B$, czyli $A + B \neq \mathbb{Q}$.

Weźmy dowolne $c \in A + B$. Wtedy $c = a + b$ dla pewnych $a \in A$, $b \in B$. Zatem z **D2** istnieją $a' \in A$ oraz $b' \in B$ takie, że $a < a'$ i $b < b'$. Stąd $c = a + b < a' + b'$ oraz $a' + b' \in A + B$. Zatem $A + B$ spełnia warunek **D2**.

Weźmy dowolne $c \in A + B$ i dowolne wymierne $q < c$. Wtedy $c = a + b$ dla pewnych $a \in A$, $b \in B$. Stąd $q < a + b$. Z lematu 5.26 istnieją liczby wymierne u i v takie, że $q = u + v$, $u < a$ i $v < b$. Zatem z **D3**, $u \in A$ i $v \in B$, więc $q \in A + B$ i warunek **D3** też jest spełniony przez zbiór $A + B$. □

Definicja 6.6. Dla dowolnego przekroju Dedekinda A oznaczmy przez $-A$ zbiór złożony z tych liczb wymiernych y, dla których istnieje liczba wymierna $z < 0$ o tej własności, że $a + y < z$ dla wszystkich $a \in A$.

Stwierdzenie 6.7. *Dla dowolnego przekroju Dedekinda A zbiór $-A$ też jest przekrojem Dedekinda. Ponadto $A + (-A) = 0^*$.*

Dowód. Weźmy dowolne $n \in \mathbb{N}$. Wtedy ze stwierdzenia 6.3 (ii) istnieje $k \in \mathbb{Z}$ takie, że $\frac{k}{n} \in A$ i $\frac{k+1}{n} \notin A$. Stąd na mocy stwierdzenia 6.3 (i), $a < \frac{k+1}{n}$ dla każdego $a \in A$. Zatem $(-\frac{k+2}{n}) + a < -\frac{1}{n}$ dla każdego $a \in A$. Stąd $-\frac{k+2}{n} \in -A$, czyli $-A \neq \emptyset$. Zatem $\frac{k}{n} + (-\frac{k+2}{n}) \in A + (-A)$, skąd

$$-\frac{2}{n} \in A + (-A) \text{ dla każdego } n \in \mathbb{N}. \tag{6.2}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Jeśli $-\frac{k}{n} \in -A$, to istnieje wymierne $z < 0$ takie, że $a + (-\frac{k}{n}) < z$, skąd $a + (-\frac{k}{n}) < 0$ dla każdego $a \in A$. Ale $a = \frac{k}{n} \in A$, więc stąd $0 < 0$ i mamy sprzeczność. W takim razie $-\frac{k}{n} \notin -A$, więc $-A \neq \mathbb{Q}$.

Weźmy dowolne $y \in -A$. Wtedy istnieje wymierne $w < 0$ takie, że $a + y < w$ dla każdego $a \in A$. Stąd $a + (y - \frac{w}{2}) < \frac{w}{2}$ dla każdego $a \in A$ i $\frac{w}{2}$ jest ujemną liczbą wymierną, więc $y - \frac{w}{2} > y$ oraz $y - \frac{w}{2} \in -A$. Wobec tego $-A$ spełnia warunek **D2**.

Weźmy dowolne $y \in -A$ i dowolne wymierne $q < y$. Wtedy istnieje wymierne $w < 0$ takie, że $a+y < w$ dla każdego $a \in A$. Ale $a+q < a+y$, więc $a + q < w$ dla każdego $a \in A$. Zatem $q \in -A$ i warunek **D3** też jest spełniony. Wobec tego $-A$ jest przekrojem Dedekinda.

Weźmy dowolne $x \in A+(-A)$. Wtedy $x = a+y$ dla pewnych $a \in A$ i $y \in -A$. Zatem istnieje liczba wymierna $z < 0$ taka, że $a + y < z$, skąd $a + y < 0$, czyli $x < 0$. Zatem $A + (-A) \subseteq 0^*$. Weźmy dowolne $x \in 0^*$. Wtedy $x \in \mathbb{Q}$ i $x < 0$. Ponieważ ciało $\mathbb{Q}$ spełnia aksjomat Archimedesa, więc istnieje liczba naturalna n taka, że $n > \frac{2}{-x}$, skąd $x < -\frac{2}{n}$. Ponadto z (6.2) mamy, że $-\frac{2}{n} \in A + (-A)$, więc z **D3**, $x \in A + (-A)$, skąd $0^* \subseteq A + (-A)$. Mamy też, że $A + (-A) \subseteq 0^*$, więc $A + (-A) = 0^*$. □

Stwierdzenie 6.8. *Dla dowolnych przekrojów Dedekinda A, B i C spełnione są następujące zależności:*

(i) $A + B = B + A$,

(ii) $(A + B) + C = A + (B + C)$,

(iii) $A + 0^* = A$,

(iv) $-A$ *jest jedynym przekrojem Dedekinda C spełniającym równanie* $A + C = 0^*$,

(v) jeżeli $A \subset B$, *to* $A + C \subset B + C$,

(vi) $-(-A) = A$.

Dowód. (i). Z przemienności dodawania liczb wymiernych, $B + A = \{b + a : b \in B, a \in A\} = \{a + b : a \in A, b \in B\} = A + B$.

(ii). Z łączności dodawania liczb wymiernych, $(A+B)+C = \{a+b : a \in A, b \in B\} + C = \{(a+b)+c : a \in A, b \in B, c \in C\} = \{a+(b+c) : a \in A, b \in B, c \in C\} = A + (B + C)$.

(iii). Weźmy dowolne $x \in A + 0^*$. Wtedy $x = a + y$ dla pewnych $a \in A$ oraz $y \in 0^*$. Zatem $y < 0$, skąd $a + y < a$, czyli $x < a$ i z **D3**, $x \in A$. Zatem $A + 0^* \subseteq A$.

Weźmy dowolne $a \in A$. Wtedy z **D2** istnieje $b \in A$ takie, że $a < b$. Stąd $a - b < 0$, więc $a - b \in 0^*$. Zatem $a = b + (a - b) \in A + 0^*$, skąd $A \subseteq A + 0^*$. Mamy też, że $A + 0^* \subseteq A$, więc ostatecznie $A + 0^* = A$.

(iv). Ze stwierdzenia 6.7, $A + (-A) = 0^*$. Załóżmy, że dla pewnego przekroju Dedekinda C jest $A + C = 0^*$. Wtedy stąd i z (i), $C + A = 0^*$, więc $(C + A) + (-A) = 0^* + (-A) = (-A) + 0^* = -A$ na mocy stwierdzenia 6.7. Ponadto z (ii) i ze stwierdzenia 6.7 oraz z (iii), $(C + A) + (-A) = C + (A + (-A)) = C + 0^* = C$, więc $C = -A$.

(v). Weźmy dowolne $x \in A + C$. Wtedy $x = a + c$ dla pewnych $a \in A$ i $c \in C$, ale $A \subset B$, więc $a \in B$, skąd $a + c \in B + C$, czyli $x \in B + C$. Wobec tego $A + C \subseteq B + C$. Jeśli $A + C = B + C$, to $(A + C) + (-C) = (B + C) + (-C)$ i na mocy (ii), $A + (C + (-C)) = B + (C + (-C))$, czyli na mocy stwierdzenia 6.7, $A + 0^* = B + 0^*$, skąd na mocy (iii), $A = B$ i mamy sprzeczność. Wobec tego $A + C \subseteq B + C$ i $A + C \neq B + C$, skąd $A + C \subset B + C$.

(vi). Na mocy (iv) jest $A + (-A) = 0^*$, więc z (i) uzyskujemy, że $(-A) + A = 0^*$ i znowu na mocy (iv) dostajemy $A = -(-A)$. □

Stwierdzenie 6.9. *Niech $\mathcal{X}$ będzie niepustą rodziną przekrojów Dedekinda zawartych w pewnym przekroju Dedekinda A. Wówczas mnogościowa suma B wszystkich zbiorów z rodziny $\mathcal{X}$ jest przekrojem Dedekinda i zawiera wszystkie przekroje Dedekinda z rodziny $\mathcal{X}$. Ponadto jeśli przekrój Dedekinda C zawiera każdy ze zbiorów rodziny $\mathcal{X}$, to $B \subseteq C$.*

Dowód. Wprost z definicji B mamy, że $X \subseteq B$ dla każdego $X \in \mathcal{X}$, skąd wynika, że $B \neq \emptyset$. Jeżeli $x \in B$, to $x \in X$ dla pewnego $X \in \mathcal{X}$, ale $X \subseteq A$, więc $x \in A$, skąd $B \subseteq A$. Ponadto, $A \neq \mathbb{Q}$, więc $B \neq \mathbb{Q}$.

Weźmy dowolne $a \in B$. Wtedy $a \in X$ dla pewnego $X \in \mathcal{X}$. Stąd i z **D2** istnieje $b \in X$ takie, że $a < b$. Ale wtedy $b \in B$, więc B spełnia warunek **D2**.

Niech $a \in B$ i niech liczba wymierna $x < a$. Wtedy $a \in X$ dla pewnego $X \in \mathcal{X}$. Stąd i z **D3**, $x \in X$, więc $x \in B$, czyli B spełnia **D3**.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

W ten sposób wykazaliśmy, że B jest przekrojem Dedekinda i z teorii zbiorów wynika, że B jest najmniejszym podzbiorem zbioru $\mathbb{Q}$ zawierającym wszystkie zbiory rodziny $X \in \mathcal{X}$. □

Stwierdzenie 6.10. *Dla dowolnych liczb wymiernych a i b:*
(i) $a^* = b^* \iff a = b$,
(ii) $a^* \subset b^* \iff a < b$,
(iii) $a^* + b^* = (a + b)^*$,
(iv) $-a^* = (-a)^*$.

Dowód. Załóżmy, że $a < b$ i weźmy dowolne $w \in a^*$. Wtedy $w < a$ i $a < b$, więc $w < b$, czyli $w \in b^*$. Wobec tego $a^* \subseteq b^*$, ale $a \in b^*$ i $a \notin a^*$, więc $a^* \subset b^*$. Na odwrót, załóżmy, że $a^* \subset b^*$. Wtedy $a \neq b$. Jeśli $b < a$, to z pierwszej części rozumowania, $b^* \subset a^*$, co przeczy temu, że $a^* \subset b^*$. Wobec tego musi być $a < b$. W ten sposób mamy wykazany podpunkt (ii), a z niego od razu wynika (i).

(iii). Weźmy dowolne $w \in a^* + b^*$. Wtedy $w = x + y$ dla pewnych $x \in A^*$ i $y \in b^*$. Stąd $x < a$ i $y < b$, więc $x + y < a + b$, a zatem $w < a + b$, czyli $w \in (a + b)^*$. Na odwrót, niech $w \in (a + b)^*$. Wtedy $w < a + b$ i z lematu 2.26, $w = x + y$ dla pewnych liczb wymiernych x i y takich, że $x < a$ i $y < b$. Zatem $x \in a^*$ i $y \in b^*$, a zatem $w \in a^* + b^*$. Wobec tego $a^* + b^* = (a + b)^*$.

(iv). Na mocy (iii) mamy, że $a^* + (-a)^* = (a + (-a))^* = 0^*$, więc ze stwierdzenia 6.8 (iv), $(-a)^* = -a^*$. □

Przekroje Dedekinda A takie, że $0^* \subset A$ będziemy nazywali **dodatnimi**. Jeśli przekrój Dedekinda A jest dodatni, to $0^* \subset A$, więc istnieje $w \in A$ takie, że $w \notin 0^*$, czyli $w \geqslant 0$ i z **D2** istnieje $a \in A$ takie, że $a > w$, skąd $a > 0$. Wobec tego dodatni przekrój Dedekinda zawsze zawiera pewną wymierną liczbę dodatnią. Na odwrót, jeśli do przekroju Dedekinda D należy pewna liczba dodatnia w, to wszystkie liczby wymierne mniejsze od w też należą do A na mocy **D3**, skąd $0^* \subseteq A$, a ponieważ dodatkowo $w \in A$ i $w \notin 0^*$, więc $0^* \subset A$. W ten sposób pokazaliśmy, że przekrój Dedekinda jest dodatni wtedy i tylko wtedy, gdy zawiera pewną dodatnią liczbę wymierną. Mnożenie przekrojów Dedekinda określamy najpierw w zbiorze dodatnich przekrojów Dedekinda.

Definicja 6.11. Iloczynem dodatnich przekrojów Dedekinda A i B nazywamy zbiór

$$A \circ B = \{w \in \mathbb{Q} : w \leqslant 0\} \cup \{a \cdot b : a, b > 0, a \in A, b \in B\}. \qquad (6.3)$$

Lemat 6.12. *Iloczyn dowolnych dwóch dodatnich przekrojów Dedekinda A i B jest dodatnim przekrojem Dedekinda i $A \circ B = \{w \in \mathbb{Q} : w < ab$ dla pewnych dodatnich $a \in A, b \in B\}$.*

Dowód. Ponieważ przekroje Dedekinda A i B są dodatnie, więc istnieją dodatnie liczby wymierne $a \in A$ i $b \in B$. Stąd $ab > 0$ i $ab \in A \circ B$. Ponadto istnieją dodatnie liczby wymierne r i s takie, że $x < r$ i $y < s$ dla dowolnych $x \in A$ i $y \in B$. Zatem dla dowolnych dodatnich $x \in A$ oraz $y \in B$ mamy, że $x \cdot y < r \cdot s$, skąd na mocy definicji $A \circ B$ mamy, że $t < r \cdot s$ dla wszystkich $t \in A \circ B$. Zatem $rs \notin A \circ B$ i $A \circ B \neq \mathbb{Q}$.

Weźmy dowolne $x \in A \circ B$. Pokażemy, że istnieje $y \in A \circ B$ takie, że $x < y$. Jeśli $x \leqslant 0$, to wystarczy przyjąć $y = ab$. Niech dalej $x > 0$. Wtedy $x = uv$ dla pewnych dodatnich $u \in A$ i $v \in B$. Zatem istnieje $u' \in A$ takie, że $u < u'$, skąd $u' > 0$ i wobec tego $x = uv < u'v$ oraz $u'v \in A \circ B$, więc wystarczy wziąć $y = u'v$.

Pokażemy, że jeżeli $x \in A \circ B$ i $w \in \mathbb{Q}$ oraz $w < x$, to $w \in A \circ B$. Jest to oczywiste dla $w \leqslant 0$. Niech dalej $w > 0$. Wtedy $x > 0$, bo $x > w$. Zatem istnieją dodatnie $p \in A$ oraz $q \in B$ takie, że $x = pq$, skąd $0 < w < pq$. Z lematu 5.27 istnieją liczby wymierne dodatnie f i g takie, że $x = fg$ oraz $f < p$ i $g < q$. Stąd $f \in A$ i $g \in B$ oraz $x \in A \circ B$.

W ten sposób wykazaliśmy, że $A \circ B$ jest dodatnim przekrojem Dedekinda. Z definicji $A \circ B$ mamy od razu, że $A \circ B \subseteq C$, gdzie $C = \{w \in \mathbb{Q} : w < ab$ dla pewnych dodatnich $a \in A, b \in B\}$. Na odwrót, weźmy dowolne $c \in C$. Jeśli $c \leqslant 0$, to $c \in A \circ B$. Niech dalej $c > 0$. Wtedy $0 < c < ab$ dla pewnych dodatnich $a \in A$ i $b \in B$. Z lematu 5.27 istnieją dodatnie liczby wymierne p i q takie, że $p < a$ i $q < b$ oraz $c = pq$. Stąd $p \in A$ i $q \in B$, więc $c \in A \circ B$. Wobec tego $A \circ B = C$, co kończy dowód. □

Lemat 6.13. *Dla dowolnych dodatnich przekrojów Dedekinda A, B i C:*

(i) $A \circ B = B \circ A$,
(ii) $A \circ (B \circ C) = (A \circ B) \circ C$,
(iii) $A \circ 1^* = A$,
(iv) $0^* \subset B + C$ *i* $A \circ (B + C) = A \circ B + A \circ C$.

Dowód. Ze wzoru (6.3) i z przemienności mnożenia liczb wymiernych mamy od razu, że $A \circ B = B \circ A$.

(ii). Wystarczy udowodnić, że dodatnia liczba wymierna w należy do zbioru $A \circ (B \circ C)$ wtedy i tylko wtedy, gdy $w \in (A \circ B) \circ C$. Niech zatem $w \in A \circ (B \circ C)$. Wtedy istnieją dodatnie $a \in A$ i $x \in B \circ C$ takie, że $w = a \cdot x$. Stąd zaś $x = bc$ dla pewnych dodatnich $b \in B$ i $c \in C$. Zatem $x = a \cdot (b \cdot c) = (a \cdot b) \cdot c \in (A \circ B) \circ C$, bo $ab \in A \circ B$ i $ab > 0$. Podobnie pokazujemy, że jeśli $w \in (A\circ)\circ C$, to $w \in A\circ(B\circ C)$.

(iii). Weźmy dowolne $a \in A$. Istnieje dodatnie $\alpha \in A$. Jeśli $a \leqslant 0$, to $\frac{a}{\alpha} \in 1^*$ i $\alpha \in A$, więc $a = \alpha \cdot \frac{a}{\alpha} \in A \circ 1^*$. Jeśli $a > 0$, to istnieje $b \in A$ takie, że $a < b$, skąd $0 < \frac{a}{b} < 1$, skąd $\frac{a}{b} \in 1^*$ oraz $a = b \cdot \frac{a}{b}$, więc $a \in A \circ 1^*$. Wobec tego $A \subseteq A \circ 1^*$. Weźmy dowolne $w \in A \circ 1^*$. Jeśli $x \leqslant 0$, to $x \in A$. Jeśli zaś $x > 0$, to istnieją dodatnie $u \in A$ i $v \in 1^*$ takie, że $w = uv$. Ale $0 < u$ i $0 < v < 1$, więc $w < u$, skąd $w \in A$. Zatem $A \circ 1^* \subseteq A$ i ostatecznie $A = A \circ 1^*$.

(iv). Ponieważ przekroje Dedekinda B i C są dodatnie, więc istnieją dodatnie liczby wymierne $b \in B$ i $c \in C$, skąd $b + c > 0$ oraz $b + c \in$ $\in B + C$, a to oznacza, że $0^* \subset B + C$.

Weźmy dowolne $w \in A \circ (B + C)$. Jeśli $w \leqslant 0$, to $\frac{w}{2} \leqslant 0$, więc $\frac{w}{2} \in A \circ B$ i $\frac{w}{2} \in A \circ C$ oraz $w = \frac{w}{2} + \frac{w}{2}$, więc $w \in A \circ B + A \circ C$. Niech dalej $w > 0$. Wtedy $w = a \cdot x$ dla pewnych dodatnich $a \in A$ i $x \in B + C$. Stąd $x = b + c$ dla pewnych $b \in B$ i $c \in C$, a ponieważ $0^* \subset B$ i $0^* \subset C$, więc $b < b'$ i $c < c'$ dla pewnych dodatnich $b' \in B$ i $c' \in C$. Stąd $w < a \cdot (b' + c') = ab' + ac'$ i z lematu 5.26 istnieją $p \in A \circ B$ oraz $q \in A \circ C$ takie, że $w = p + q$ oraz $p < ab'$ i $q < ac'$. Zatem $p \in A \circ B$ i $q \in A \circ C$, skąd $w \in A \circ B + A \circ C$. Wobec tego $A \circ (B + C) \subseteq A \circ B + A \circ C$.

Weźmy dowolne $w \in A\circ B+A\circ C$. Jeżeli $w \leqslant 0$, to $w \in A\circ(B+C)$. Niech dalej $w > 0$. Wtedy $w = x+y$ dla pewnych $x \in A\circ B$ i $y \in A\circ C$. Ale z lematu 5.12, $0^* \subset A \circ B$ i $0^* \subset A \circ C$, więc istnieją dodatnie $p \in$ $\in A \circ B$ i $q \in A \circ C$ takie, że $x < p$ i $y < q$, skąd $w < p + q$. Zatem

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$p = ab$ dla pewnych dodatnich $a \in A$ i $b \in B$ oraz $q = a'c$ dla pewnych dodatnich $a' \in A$ i $c \in C$. Niech $\alpha = \max\{a, a'\}$. Wtedy $ab \leqslant \alpha b \in$ $\in A \circ B$ i $a'c \leqslant \alpha c \in A \circ C$, skąd $w < \alpha b + \alpha c = \alpha(b+c) \in A \circ (B+C)$, więc $w \in A \circ (B + C)$. Wobec tego $A \circ B + A \circ C \subseteq A \circ (B + C)$ i ostatecznie $A \circ (B + C) = A \circ B + A \circ C$. □

Dla dodatniego przekroju Dedekinda A oznaczmy przez A^{-1} zbiór złożony ze wszystkich liczb wymiernych $w \leqslant 0$ oraz ze wszystkich dodatnich liczb wymiernych y, dla których istnieje dodatnia liczba wymierna $z < 1$ taka, że $a \cdot y < z$ dla wszystkich $a \in A$.

Lemat 6.14. *Dla każdego dodatniego przekroju Dedekinda A zbiór A^{-1} jest dodatnim przekrojem Dedekinda i $A \circ A^{-1} = 1^*$. Ponadto, jeśli C jest dodatnim przekrojem Dedekinda takim, że $A \circ C = 1^*$, to $C = A^{-1}$.*

Dowód. Ponieważ $0^* \subset A$, więc istnieje dodatnia liczba wymierna α taka, że $a < \alpha$ dla każdego $a \in A$. Stąd $a \cdot \frac{1}{2\alpha} < \frac{1}{2}$ dla każdego $a \in A$, więc $\frac{1}{2\alpha} \in A^{-1}$. Ale $\frac{1}{2\alpha} > 0$, więc zbiór A^{-1} zawiera liczbę dodatnią i wszystkie liczby wymierne $w \leqslant 0$. Dalej, istnieje dodatnie $a \in A$, skąd $\frac{1}{a} > 0$. Ale $a \cdot \frac{1}{a} = 1$, więc z definicji A^{-1} mamy, że $\frac{1}{a} \notin A^{-1}$, skąd $A^{-1} \neq \mathbb{Q}$.

Udowodnimy, że dla każdego $y \in A^{-1}$ istnieje $y' \in A^{-1}$ takie, że $y < y'$. Jeśli $y \leqslant 0$, to wystarczy przyjąć $y' = \frac{1}{2\alpha}$. Niech dalej $y > 0$. Wtedy istnieje dodatnia liczba wymierna $z < 1$ taka, że $a \cdot y < z$ dla wszystkich $a \in A$. Istnieje liczba wymierna w taka, że $z < w < 1$, skąd $\frac{w}{z} > 1$, więc $y \cdot \frac{w}{z} > y$ oraz dla każdego $a \in A$ mamy, że $a \cdot (y \cdot \frac{w}{z}) <$ $< z \cdot \frac{w}{z} = w < 1$. Zatem wystarczy przyjąć $y' = y \cdot \frac{w}{z}$.

Weźmy dowolne $y \in A^{-1}$ i dowolne wymierne $q < y$. Jeśli $q \leqslant 0$, to $q \in A^{-1}$. Niech dalej $q > 0$. Wtedy $y > 0$. Zatem istnieje dodatnia liczba wymierna $z < 1$ taka, że dla każdego $a \in A$: $a \cdot y < z$. Stąd dla dodatnich $a \in A$: $a \cdot q < a \cdot y < z$, czyli $a \cdot q < z$. Ponadto dla $a \leqslant 0$ mamy, że $a \cdot q \leqslant 0$, więc też $a \cdot q < z$. Wobec tego $q \in A^{-1}$ i w ten sposób zakończyliśmy dowód tego, że zbiór A^{-1} jest dodatnim przekrojem Dedekinda.

Teraz wykażemy, że $A \circ A^{-1} = 1^*$. W tym celu weźmy dowolne $x \in A \circ A^{-1}$. Jeśli $x \leqslant 0$, to $x \in 1^*$. Jeśli zaś $x > 0$, to $x = a \cdot y$

dla pewnych dodatnich $a \in A$ i $y \in A^{-1}$. Ale wtedy istnieje dodatnia liczba wymierna $z < 1$ taka, że $uy < z$ dla wszystkich $u \in A$, skąd $a \cdot y < z$, czyli $a \cdot y < 1$, więc $x < 1$. Zatem $x \in 1^*$ i $A \circ A^{-1} \subseteq 1^*$.

Weźmy dowolne $x \in 1^*$. Wtedy $x < 1$. Jeśli $x \leqslant 0$, to $x \in A \circ A^{-1}$. Niech dalej $x > 0$. Z aksjomatu Archimedesa w ciele $\mathbb{Q}$ wynika, że istnieje liczba naturalna $m > \frac{2x}{1-x}$. Weźmy dowolne dodatnie $a \in A$. Wtedy z aksjomatu Archimedesa istnieje liczba naturalna $s > m$ i taka, że $s > \frac{1}{a}$, skąd $\frac{1}{s} < a$, a zatem $\frac{1}{s} \in A$ i $s > \frac{2x}{1-x}$. Ze stwierdzenia 6.3 (ii) istnieje liczba całkowita k taka, że $\frac{k}{s^2} \in A$ oraz $\frac{k+1}{s^2} \notin A$. Ponieważ $\frac{s}{s^2} = \frac{1}{s} \in A$, więc $k \geqslant s$, skąd $k > 0$ oraz $k > \frac{2x}{1-x}$, a zatem $x < \frac{k}{k+2}$. Ale ze stwierdzenia 6.3 (i) mamy, że $a < \frac{k+1}{s^2}$ dla każdego $a \in A$, więc $a \cdot \frac{s^2}{k+2} < \frac{k+1}{k+2}$ dla każdego $a \in A$. Stąd $\frac{s^2}{k+2} \in A^{-1}$ i $\frac{k}{s^2} \cdot \frac{s^2}{k+2} \in A \circ A^{-1}$, czyli $\frac{k}{k+2} \in A \circ A^{-1}$. Ale $x < \frac{k}{k+2}$ i $A \circ A^{-1}$ jest przekrojem Dedekinda, więc $x \in A \circ A^{-1}$. Wobec tego $1^* \subseteq A \circ A^{-1}$, a ponieważ mamy też, że $A \circ A^{-1} \subseteq 1^*$, więc $A \circ A^{-1} = 1^*$.

Niech C będzie dodatnim przekrojem Dedekinda takim, że $A \circ C = 1^*$. Wtedy ze stwierdzenia 6.13, $C \circ A = 1^*$ oraz $(C \circ A) \circ A^{-1} = 1^* \circ A^{-1} = A^{-1}$ oraz $(C \circ A) \circ A^{-1} = C \circ (A \circ A^{-1}) = C \circ 1^* = C$. Wobec tego $C = A^{-1}$. □

Lemat 6.15. *Niech A, B i C będą dodatnimi przekrojami Dedekinda. Jeżeli $A \subset B$, to $A \circ C \subset B \circ C$.*

Dowód. Weźmy dowolne $x \in A \circ C$. Wtedy z lematu 6.12 istnieją dodatnie $a \in A$ i $c \in C$ takie, że $x < a \cdot c$. Ale $A \subset B$, więc $a \in B$ i z lematu 6.12, $x \in B \circ C$. Zatem $A \circ C \subseteq B \circ C$. Jeśli $A \circ C = B \circ C$, to $(A \circ C) \circ C^{-1} = (B \circ C) \circ C^{-1}$, skąd na mocy lematu 6.13, $A \circ (C \circ C^{-1}) = B \circ (C \circ C^{-1})$. Z lematu 6.14 mamy, że $A \circ 1^* = B \circ 1^*$ i z lematu 6.13, $A = B$, wbrew temu, że $A \subset B$. Wobec tego $A \circ C \neq B \circ C$ i $A \circ C \subset B \circ C$. □

Zauważmy, że jeśli C jest przekrojem Dedekinda takim, że $C \subset 0^*$, to na mocy lematu 6.8 (iv), $C + (-C) \subset 0^* + (-C)$, czyli $0^* \subset -C$, a zatem $-C$ jest wtedy dodatnim przekrojem Dedekinda.

Teraz zdefiniujemy iloczyn $A \circ B$ dowolnych przekrojów Dedekinda A i B przyjmując, że $A \circ B = 0^*$, jeśli $A = 0^*$ lub $B = 0^*$ oraz

jeśli $A \subset 0^*$ i $0^* \subset B$, to $A \circ B = -[(-A) \circ B]$ oraz jeśli $0^* \subset A$ i $B \subset 0^*$, to $A \circ B = -[A \circ (-B)]$ oraz jeśli $A \subset 0^*$ i $B \subset 0^*$, to $A \circ B = (-A) \circ (-B)$. Z tych określeń i z lematu 6.12 wynika, że tak określony iloczyn przekrojów Dedekinda jest przekrojem Dedekinda.

Lemat 6.16. *Dla dowolnych przekrojów Dedekinda A i B:*
(i) $(-A) \circ B = A \circ (-B) = -(A \circ B)$,
(ii) $(-A) \circ (-B) = A \circ B$.

Dowód. (i). Jeśli $A = 0^*$, to $-A = 0^*$, więc $(-A) \circ B = A \circ (-B) = -(A \circ B) = 0^*$. Podobnie, dla $b = 0^*$ też $(-A) \circ B = A \circ (-B) = -(A \circ B) = 0^*$. Niech dalej $A \neq 0^*$ i $B \neq 0^*$. Wtedy na mocy stwierdzenia 6.4 możliwe są tylko następujące przypadki:

(1). $0^* \subset A$ i $0^* \subset B$. Wtedy $-A \subset 0^*$ i $-B \subset 0^*$, więc z definicji mnożenia przekrojów Dedekinda i ze stwierdzenia 6.8 (vi): $(-A) \circ B = -[[-(-A)] \circ B] = -(A \circ B)$ i $A \circ (-B) = -[A \circ (-(-B))] = -(A \circ B)$.

(2). $0^* \subset A$ i $B \subset 0^*$. Wtedy $-A \subset 0^*$ i $0^* \subset -B$, więc z definicji mnożenia przekrojów Dedekinda i ze stwierdzenia 6.8 (vi): $(-A) \circ B = (-(-A)) \circ (-B) = A \circ (-B) = -(A \circ B)$, bo $A \circ B = -[A \circ (-B)]$.

(3). $A \subset 0^*$ i $0^* \subset B$. Wtedy $0^* \subset -A$ i $-B \subset 0^*$, więc z definicji mnożenia przekrojów Dedekinda i ze stwierdzenia 6.8 (vi): $(-A) \circ B = -(A \circ B)$ i $A \circ (-B) = (-A) \circ (-(-B)) = (-A) \circ B$.

(4). $A \subset 0^*$ i $B \subset 0^*$. Wtedy $0^* \subset A$ i $0^* \subset B$, więc z definicji mnożenia przekrojów Dedekinda i ze stwierdzenia 6.8 (vi): $(-A) \circ B = -[(-A) \circ (-B)] = -(A \circ B)$ i $A \circ (-B) = -[(-A) \circ (-B)] = -(A \circ B)$.

(ii). Na mocy (i) mamy, że $(-A) \circ (-B) = -[A \circ (-B)] = -[-(A \circ B)] = A \circ B$. □

Lemat 6.17. *Dla dowolnych dodatnich przekrojów Dedekinda A, B i C:*

$$A \circ (B + (-C)) = A \circ B + A \circ (-C).$$

Dowód. Możliwe są tylko następujące przypadki:

(1). $B + (-C) = 0^*$. Wtedy $B = C$ i $A \circ (B + (-C)) = 0^*$ i $A \circ B + A \circ (-C) = A \circ B + [-(A \circ B)]] = 0^*$, więc $A \circ (B + (-C)) = A \circ B + A \circ (-C)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

(2). $0^* \subset B+(-C)$. Wtedy z lematu 6.13, $A\circ(B+(-C))+A\circ C = A\circ[(B+(-C)]+C] = A\circ[B+((-C)+C)] = A\circ[B+0^*] = A\circ B$ oraz $[A\circ B + A\circ(-C)] + A\circ C = [A\circ B + [-(A\circ C)]] + A\circ C = A\circ B + [-(A\circ C) + A\circ C] = A\circ B + 0^* = A\circ B$, więc $A\circ(B+(-C)) + A\circ C = [A\circ B + A\circ(-C)] + A\circ C$, skąd po skróceniu $A\circ C$ mamy tezę.

(3). $B + (-C) \subset 0^*$. Wtedy $0^* \subset -(B+(-C)) = (-B) + C$ i z lematów 6.13 i 6.16 oraz z (2), $A\circ(B+(-C)) = -[A\circ((-B)+C)] = -[A\circ(C+(-B))] = -[A\circ C + A\circ(-B)] = -(A\circ C)+(-(A\circ(-B)) = A\circ(-C) + A\circ B = A\circ B + A\circ(-C)$. □

Stwierdzenie 6.18. *Dla dowolnych przekrojów Dedekinda A, B i C zachodzą następujące zależności:*

(i) $A\circ B = B\circ A$,

(ii) $A\circ(B\circ C) = (A\circ B)\circ C$,

(iii) $A\circ 1^* = A$,

(iv) jeśli $A \neq 0^*$, *to* $A\circ U = 1^*$ *dla pewnego przekroju Dedekinda* U,

(v) $A\circ(B+C) = A\circ B + A\circ C$,

(vi) jeśli $A \subset B$ *i* $0^* \subset C$, *to* $A\circ C \subset B\circ C$.

Dowód. (i). Jeśli $A = 0^*$ lub $B = 0^*$, to $A\circ B = B\circ A = 0^*$. Niech dalej $A \neq 0^*$ i $B \neq 0^*$. Wtedy na mocy stwierdzenia 6.4 możliwe są tylko następujące przypadki:

(1). $0^* \subset A$ i $0^* \subset B$. Wtedy $A\circ B = B\circ A$ na mocy lematu 6.13 (i).

(2). $0^* \subset A$ i $B \subset 0^*$. Wtedy z definicji mnożenia przekrojów Dedekinda i z lematów 6.16 i 6.13 (i), $B\circ A = -((-B)\circ A) = -(A\circ(-B)) = A\circ B$.

(3). $A \subset 0^*$ i $0^* \subset B$. Wtedy z definicji mnożenia przekrojów Dedekinda i z lematów 6.16 i 6.13 (i) mamy, że $B\circ A = -(B\circ(-A)) = -((-A)\circ B) = A\circ B$.

(4). $A \subset 0^*$ i $B \subset 0^*$. Wtedy z definicji mnożenia przekrojów Dedekinda i z lematów 6.16 i 6.13 (i), $B\circ A = (-B)\circ(-A) = (-A)\circ(-B) = A\circ B$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

(ii). Jeżeli $A = 0^*$ lub $B = 0^*$ lub $C =^*$, to $A \circ (B \circ C) = 0^*$ i $(A \circ B) \circ C = 0^*$, więc $A \circ (B \circ C) = (A \circ B) \circ C$. Niech dalej $A \neq 0^*$ i $B \neq 0^*$ i $C \neq 0^*$. Wtedy na mocy stwierdzenia 6.4 możliwe są tylko następujące przypadki:

(1). $0^* \subset A$ i $0^* \subset B$ i $0^* \subset C$. Wtedy na mocy lematu 6.13 (ii), $A \circ (B \circ C) = (A \circ B) \circ C$.

(2). $0^* \subset A$ i $0^* \subset B$ i $C \subset 0^*$. Wtedy $0^* \subset -C$ i z lematów 6.16 i 6.13, $A \circ (B \circ C) = A \circ [-(B \circ (-C)] = -[A \circ [B \circ (-C)]] = = -[(A \circ B) \circ (-C)] = (A \circ B) \circ C$, bo $-(-C) = C$.

(3). $0^* \subset A$ i $B \subset 0^*$ i $C \subset 0^*$. Wtedy $0^* \subset -B$ i $0^* \subset -C$ i z lematów 6.16 i 6.13 mamy, że $A \circ (B \circ C) = A \circ [(-B) \circ (-C)] = = (A \circ (-B)] \circ (-C) = [-(A \circ B)] \circ (-C) = (A \circ B) \circ C$.

(4). $0^* \subset A$ i $B \subset 0^*$ i $0^* \subset C$. Wtedy $0^* \subset -B$ i z lematów 6.16 i 6.13, $A \circ (B \circ C) = A \circ [-((-B) \circ C)] = -[A \circ ((-B) \circ C)] = = -[(A \circ (-B)) \circ C] = [-(A \circ (-B))] \circ C = (A \circ B) \circ C$.

(5). $A \subset 0^*$ i $0^* \subset B$ i $0^* \subset C$. Wtedy $0^* \subset -A$ i z lematów 6.16 i 6.13, $A \circ (B \circ C) = -[(-A) \circ (B \circ C)] = -[[(-A) \circ B] \circ C] = = [-((-A) \circ B)] \circ C = (A \circ B) \circ C$.

(6). $A \subset 0^*$ i $0^* \subset B$ i $C \subset 0^*$. Wtedy $0^* \subset -A$ i $0^* \subset -C$ i z lematów 6.16 i 6.13 mamy, że $A \circ (B \circ C) = A \circ [-(B \circ (-C))] = = (-A) \circ [B \circ (-C)] = [(-A) \circ B] \circ (-C) = [-(A \circ B)] \circ (-C) = = (A \circ B) \circ C$.

(7). $A \subset 0^*$, $B \subset 0^*$ i $C \subset 0^*$. Wtedy $0^* \subset -A$ i $0^* \subset -B$ i $0^* \subset -C$ i z lematów 6.16 i 6.13, $A \circ (B \circ C) = A \circ [(-B) \circ (-C)] = = -[(-A) \circ [(-B) \circ (-C)]] = -[[(-A) \circ (-B)] \circ (-C)] = (A \circ B) \circ C$.

(8). $A \subset 0^*$ i $B \subset 0^*$ i $0^* \subset C$. Wtedy $0^* \subset -A$ i $0^* \subset -B$ i z lematów 6.16 i 6.13 mamy, że $A \circ (B \circ C) = A \circ [-((-B) \circ C)] = = (-A) \circ [(-B) \circ C] = [(-A) \circ (-B)] \circ C = (A \circ B) \circ C$.

(iii). Dla $A = 0^*$ mamy $A \cdot 1^* = 0^* = A^*$. Niech dalej $A \neq 0^*$. Wtedy ze stwierdzenia 6.4, $0^* \subset A$ i na mocy lematu 6.13 jest $A \circ 1^* = A$ lub $A \subset 0^*$ i wtedy $A \circ 1^* = -((-A) \circ 1^*) = -(-A) = A$.

(iv). Jeśli $0^* \subset A$, to na mocy lematu 6.14 wystarczy przyjąć $U = = A^{-1}$. Jeżeli zaś $A \subset 0^*$, to $0^* \subset -A$ i dla $U = -(-A)^{-1}$ na mocy lematu 6.16, mamy, że $A \circ U = (-A) \circ (-A)^{-1} = 1^*$.

(v). Jeśli $A = 0^*$, to $A \circ (B + C) = 0^*$ i $A \circ B + A \circ C = 0^* + 0^* = 0^*$,

więc $A\circ(B+C)=A\circ B+A\circ C$. Jeśli $B=0^*$, to $A\circ(B+C)=A\circ C$ i $A\circ B+A\circ C=0^*+A\circ C=A\circ C$, więc $A\circ(B+C)=A\circ B+A\circ C$. Jeśli $C=0^*$, to $A\circ(B+C)=A\circ B$ i $A\circ B+A\circ C=A\circ B+0^*=A\circ B$, więc $A\circ(B+C)=A\circ B+A\circ C$. Niech dalej $A\neq 0^*$ i $B\neq 0^*$ i $C\neq 0^*$.

Jeśli przekroje A, B i C są dodatnie, to na mocy lematu 6.13, $A\circ(B+C)=A\circ B+A\circ C$. Z lematu 6.17 wynika, że jeśli $0^*\subset A$, $0^*\subset B$ i $C\subset 0^*$, to $A\circ(B+C)=A\circ B+A\circ C$. Podobnie, jeśli $0^*\subset A$, $B\subset 0^*$ i $0^*\subset C$, to $A\circ(B+C)=A\circ B+A\circ C$. Jeżeli zaś $0^*\subset A$, $B\subset 0^*$ i $C\subset 0^*$, to $B+C\subset 0^*$ i $A\circ(B+C)=-[A\circ[(-B)+(-C)]]=$ $=-[A\circ(-B)+A\circ(-C)]=-(A\circ(-B))+[-(A\circ(-C))]=A\circ B+A\circ C$.

W ten sposób mamy wykazaną tezę dla każdego dodatniego przekroju Dedekinda A i dla dowolnych przekrojów Dedekinda B i C. Pozostaje do rozpatrzenia przypadek, gdy $A\subset 0^*$. Wtedy jednak z pierwszej części dowodu i z definicji mnożenia przekrojów Dedekinda, $A\circ(B+C)=-[(-A)\circ(B+C)]=-[(-A)\circ B+(-A)\circ C]=$ $=-[(-A)\circ B]+(-[(-A)\circ C])=A\circ B+A\circ C$.

(vi). Skoro $A\subset B$, więc $0^*\subset B+(-A)$, skąd $0*\subset(B+(-A))\circ C$. Ale z (i) i (v), $(B+(-A))\circ C=B\circ C+(-A)\circ C=B\circ C+(-(A\circ C))$, więc $0^*\subset B\circ C+(-(A\circ C))$. Stąd z lematu 6.8, $A\circ C\subset B\circ C$. □

Stwierdzenie 6.19. *Dla dowolnych liczb wymiernych a i b mamy, że $a^*\circ b^*=(a\cdot b)^*$.*

Dowód. Jeśli $a=0$ lub $b=0$, to $a\cdot b=0$ i $a^*\circ b^*=0^*$, więc wtedy $a^*\circ b^*=(a\cdot b)^*$. Niech dalej $a\neq 0$ i $b\neq 0$.

Rozważmy najpierw przypadek, gdy $a>0$ i $b>0$. Wtedy ze stwierdzenia 6.10, $0^*\subset a^*$ i $0^*\subset b^*$. Weźmy dowolne $x\in a^*\circ b^*$. Jeśli $x\leqslant 0$, to $x\in(a\cdot b)^*$. Niech zatem $x>0$. Wtedy $x=u\cdot v$ dla pewnych dodatnich $u\in a^*$ i $v\in b^*$. Stąd $x<a\cdot b$, czyli $x\in(a\cdot b)^*$. Wobec tego $a^*\cdot b^*\subset(a\cdot b)^*$. Na odwrót, niech $x\in(a\cdot b)^*$. Jeśli $x\leqslant 0$, to $x\in a^*\circ b^*$. Niech zatem $x>0$. Wtedy $0<x<a\cdot b$ i na mocy lematu 5.27 istnieją dodatnie $p\in a^*$ oraz $q\in b^*$ takie, że $x=p\cdot q$. Ponadto $0<p<a$ i $0<q<b$, więc $x<a\cdot b$, skąd $x\in(a\cdot b)^*$. Zatem $a^*\circ b^*\subseteq(a\cdot b)^*$ i ostatecznie $a^*\circ b^*=(a\cdot b)^*$.

Niech teraz $a>0$ i $b<0$. Wtedy z udowodnionych wcześniej

własności, $a^* \circ b^* = -[a^* \circ (-b)^*] = -(a \cdot (-b))^* = -(-a \cdot b)^* = = (-(-a \cdot b))^* = (a \cdot b)^*$. Analogicznie będzie w przypadku, gdy $a < 0$ i $b > 0$. Natomiast, gdy $a < 0$ i $b < 0$, to $a \cdot b = (-a) \cdot (-b)$, więc $(a \cdot b)^* = [(-a) \cdot (-b)]^* = (-a)^* \circ (-b)^* = a^* \circ b^*$. □

Ze stwierdzeń 6.8, 6.10 i 6.18 wynika, że zbiór $\mathcal{R}$ wszystkich przekrojów Dedekinda z wyżej zdefiniowanymi dodawaniem i mnożeniem przekrojów oraz z elementami: zerowym 0^* i jedynkowym 1^* tworzy ciało. Ponadto, relacja inkluzji $\subset$ spełnia warunki **P1** i **P3** ciała uporządkowanego na mocy stwierdzeń 6.4, 6.8 (v) i 6.18 (vi) oraz warunek **P2** jest spełniony na mocy tego, że relacja inkluzji jest zawsze przechodnia. Wobec tego $\mathcal{R}$ z relacją $\subset$ jest ciałem uporządkowanym. Ze stwierdzenia 6.9 wynika, że ciało to spełnia aksjomat ciągłości. Stąd i z twierdzenia 5.47 wynika następujące

Twierdzenie 6.20. *Z dokładnością do izomorfizmu ciał zachowującego porządek istnieje dokładnie jedno ciało uporządkowane spełniające aksjomat ciągłości i jest nim ciało $\mathcal{R}$ wszystkich przekrojów Dedekinda z relacją inkluzji i dodawaniem oraz mnożeniem przekrojów zdefiniowanymi wyżej.*

Stwierdzenia 6.10 i 6.19 pokazują, że przekształcenie $a \mapsto a^*$ dla $a \in \in \mathbb{Q}$ jest bijekcją zachowującą dodawanie i mnożenie oraz zachowującą porządek. Wobec tego dla $a \in \mathbb{Q}$ można dokonać utożsamienia: $a \equiv a^*$. Przy tym utożsamieniu $\mathbb{Q} \subset \mathcal{R}$.

Od tej pory tak skonstruowane ciało liczb rzeczywistych będziemy oznaczali symbolem $\mathbb{R}$.

Definicja 6.21. Przekrojem Dedekinda ciała $\mathbb{R}$ nazywamy niepusty i właściwy podzbiór A zbioru liczb rzeczywistych nieposiadający elementu największego i taki, że wraz z każdą liczbą należącą do niego zawiera każdą liczbę rzeczywistą od niej mniejszą.

Twierdzenie 6.22. (zasada ciągłości Dedekinda). *Jeżeli A jest dowolnym przekrojem Dedekinda ciała $\mathbb{R}$, to w zbiorze $\mathbb{R} \setminus A$ istnieje element najmniejszy.*

Dowód. Ponieważ $A \neq \mathbb{R}$, więc istnieje $r \in \mathbb{R} \setminus A$. Jeżeli $r \leqslant a$ dla pewnego $a \in A$, to $r \in A$, co prowadzi do sprzeczności. Zatem $a < r$ dla każdego $a \in A$, ale zbiór A jest niepusty, więc z aksjomatu ciągłości istnieje $g = \sup A \in \mathbb{R}$. Wtedy $a \leqslant g$ dla każdego $a \in A$, a ponieważ w A nie ma elementu największego, więc $a < g$ dla każdego $a \in A$, skąd $g \in \mathbb{R} \setminus A$. Załóżmy, że g nie jest najmniejszym elementem w zbiorze $\mathbb{R} \setminus A$. Wtedy istnieje $x \in \mathbb{R} \setminus A$ takie, że $x < g$. Z definicji kresu górnego wynika, że x nie ogranicza z góry zbioru A, więc istnieje $\alpha \in A$ takie, że $\alpha > x$. Ale A jest przekrojem Dedekinda, więc stąd $x \in A$ i mamy sprzeczność. Wobec tego g jest najmniejszym elementem w zbiorze $\mathbb{R} \setminus A$. □

Na zakończenie kilka słów komentarza. „Liczby rzeczywiste" skonstruowane metodą Dedekinda są w istocie rzeczy pewnymi podzbiorami zbioru liczb wymiernych, co może wydać się nieco szokujące lub nawet ekstrawaganckie. Nawet „liczby wymierne" a^* dla $a \in \mathbb{Q}$, są takiej postaci. Chciałbym jednak zapewnić Czytelnika, że mamy tu do czynienia z dość często stosowaną w matematyce procedurą. Matematycy bowiem mniej zważają na naturę definiowanych obiektów, a bardziej na ich abstrakcyjne własności. Chwila zastanowienia pozwala docenić doniosłość i prostotę leżącej u podstaw całej konstrukcji idei. Chodzi bowiem o pytanie, skąd wziąć „materiał" do załatania luk w zbiorze liczb wymiernych. Odpowiedź Dedekinda brzmi: Nie szukajmy go wcale. Dziury w serze szwajcarskim wyznacza sam ser. Nie mówmy więc o lukach, ale o tym, co jest. Mówmy o zbiorach, które nazwaliśmy przekrojami. Przekroje wymierne pozostają we wzajemnie jednoznacznej odpowiedniości z liczbami wymiernymi, a niewymierne z „lukami". Mniejsza o to, że przekroje są skomplikowanymi obiektami. Chodzi o ich własności. Ostatecznie wszystkie możliwe konstrukcje i tak prowadzą do obiektów izomorficznych. Rzeczywiście, oprócz konstrukcji Dedekinda istnieje druga konstrukcja liczb rzeczywistych, w której w miejsce przekrojów rozważa się klasy abstrakcji równoważnych ciągów Cauchy'ego liczb wymiernych (patrz na przykład [33]). Samo sformułowanie wskazuje, że nie jest to droga dużo prostsza. Przeciwnie, sądzę, że początkujący student analizy lepiej poradzi sobie z wyłożoną wyżej teorią.

6.2 Pierwiastki arytmetyczne

Definicja 6.23. Niech $a \in \mathbb{R}$, $a \geqslant 0$ i niech $n = 2, 3, \ldots$. **Pierwiastkiem arytmetycznym** n-tego stopnia z liczby a nazywamy liczbę rzeczywistą $b \geqslant 0$ taką, że $b^n = a$. Piszemy wtedy: $b = \sqrt[n]{a}$.

Przykład 6.24. Ponieważ $0^n = 0$ i dla $b > 0$ jest $b^n > 0$, więc jedynym pierwiastkiem n-tego stopnia z liczby 0 jest liczba 0: $\sqrt[n]{0} = 0$.

Podobnie, $1^n = 1$ i jeżeli $b \geqslant 0$ jest takie, że $b^n = 1$, to $b^n = 1^n$, więc $b = 1$. Zatem jedynym pierwiastkiem n-tego stopnia z liczby 1 jest liczba 1: $\sqrt[n]{1} = 1$.

Zauważmy, że chociaż $(-2)^2 = 4$, to $-2 \neq \sqrt{4}$, gdyż $-2 < 0$. Dla dowolnego $x \in \mathbb{R}$ mamy, że $|x| \geqslant 0$ i $|x|^2 = x^2$. Wobec tego mamy wzór:

$$\sqrt{x^2} = |x|. \tag{6.4}$$

Twierdzenie 6.25. *Dla dowolnego rzeczywistego $a \geqslant 0$ i dla dowolnej liczby naturalnej $n \geqslant 2$ istnieje dokładnie jeden pierwiastek arytmetyczny n-tego stopnia z liczby a.*

Dowód. Na mocy przykładu 6.24 wystarczy rozpatrywać jedynie $a > 0$ takie, że $a \neq 1$. Jeżeli $b, c \geqslant 0$ i $b^n = a$ oraz $c^n = a$, to $b^n = c^n$ i na mocy własności 5.17, $b = c$. Wobec tego wystarczy dalej pokazać jedynie istnienie pierwiastka n-tego stopnia z liczby a.

Rozważmy najpierw przypadek, gdy $a > 1$. Niech $A = \{x \in \mathbb{R} : x \geqslant 1 \text{ i } x^n \leqslant a\}$. Ponieważ $1 \geqslant 1$ i $1^n = 1 < a$, więc $1 \in A$. Dla $x \in A$ mamy, że $x \geqslant 1$, więc z własności 5.16, $x^{n-1} \geqslant 1$, skąd z **P3** (b), $x^n \geqslant x$. Ale $x^n \leqslant a$, więc $x \leqslant a$. Zatem liczba a ogranicza zbiór A z góry. Z aksjomatu ciągłości istnieje zatem $\sup(A) = b \in \mathbb{R}$. Ponieważ $1 \in A$, więc $1 \leqslant b$. Ponadto z **P1** wynika, że $b^n < a$ lub $b^n > a$ lub $b^n = a$. Wykażemy, ze każda z dwóch pierwszych możliwości prowadzi do sprzeczności.

Załóżmy najpierw, że $b^n < a$. Weźmy dowolne $s > 0$ takie, że $s \leqslant 1$. Wtedy z własności 5.16, $0 < s^k \leqslant s$ dla każdego $k = 1, 2, \ldots, n$. Stąd i z dwumianu Newtona otrzymujemy, że $(b + s)^n \leqslant b^n + Ks$, gdzie $K = \binom{n}{1}a^{n-1} + \binom{n}{2}a^{n-2} + \ldots + \binom{n}{n-1}a + \binom{n}{n}$, czyli $K \geqslant 1$. Ponadto,

$b^n + Ks < a \iff Ks < a - b^n \iff s < \frac{a-b^n}{K}$, więc jeśli tylko $0 < s \leqslant 1$ i $s < \frac{a-b^n}{K}$, to $(b+s)^n < a$ i wtedy $b + s \in A$, przy czym $b + s > b = \sup(A)$, co prowadzi do sprzeczności.

Niech teraz $b^n > a$. Weźmy dowolne $s < b$ takie, że $s > 0$. Wtedy z własności 4.30 mamy, że $b^n - (b-s)^n = s \cdot [b^{n-1} + b^{n-2}(b-s) + \ldots + +b(b-s)^{n-2} + b^{n-1}]$ oraz $b^{n-1-j} \cdot (b-s)^j \leqslant b^{n-1}$ dla każdego $j = = 1, \ldots, n-1$, więc $b^n - (b-s)^n \leqslant s \cdot nb^{n-1} < b^n - a$, o ile tylko $s < \frac{b^n-a}{nb^{n-1}}$. Zatem jeśli $s > 0$ i $s < b$ i $s < \frac{b^n-a}{nb^{n-1}}$, to $b^n - (b-s)^n < b^n - a$, skąd dla takich s, $(b-s)^n > a$. Ale dla $x \in A$ mamy $x \geqslant 1$ i $x^n \leqslant a$, więc $(b-s)^n > x^n$ i z własności 5.16, $b - s > x$. Wobec tego $b - s < b$ i $b - s$ ogranicza z góry zbiór A, co prowadzi do sprzeczności.

Kończy to dowód istnienia pierwiastka arytmetycznego stopnia n z liczby $a > 1$.

Niech teraz $0 < a < 1$. Wówczas $\frac{1}{a} > 1$ z własności 5.6, więc z pierwszej części dowodu $\frac{1}{a} = c^n$ dla pewnego $c > 0$. Stąd $a = (\frac{1}{c})^n$ i $\frac{1}{c} > 0$. □

Następne stwierdzenie pokazuje, że dla każdego $n = 2, 3, \ldots$ funkcja $x \mapsto \sqrt[n]{x}$ jest rosnąca w całym przedziale $[0, \infty)$.

Stwierdzenie 6.26. *Jeżeli $a, b \in \mathbb{R}$ i $a, b \geqslant 0$, to dla dowolnego $n = 2, 3, \ldots$ zachodzi wzór:*

$$\sqrt[n]{a} < \sqrt[n]{b} \iff a < b. \tag{6.5}$$

Dowód. Ponieważ $\sqrt[n]{a}, \sqrt[n]{b} \geqslant 0$, więc na mocy własności 5.16 mamy, że $\sqrt[n]{a} < \sqrt[n]{b} \iff (\sqrt[n]{a})^n < (\sqrt[n]{b})^n$. Ale $(\sqrt[n]{a})^n = a$ i $(\sqrt[n]{b})^n = b$, więc $\sqrt[n]{a} < \sqrt[n]{b} \iff a < b$. □

Stwierdzenie 6.27. *Dla dowolnego $n = 2, 3, \ldots$ i dla dowolnych $a, b \in \mathbb{R}$ takich, że $a, b \geqslant 0$ zachodzą wzory:*

(i) $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$,

(ii) $\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$, *dla* $b \neq 0$,

(iii) $\sqrt[n]{a^k} = (\sqrt[n]{a})^k$, *jeśli* $a = 0$ *i* $k \in \mathbb{N}$ *lub* $a > 0$ *i* $k \in \mathbb{Z}$,

(iv) $\sqrt[n]{a^{nm}} = a^m$ *dla każdego* $m \in \mathbb{N}$.

Dowód. (i). Ponieważ $\sqrt[n]{a}, \sqrt[n]{b} \geqslant 0$, więc $\sqrt[n]{a} \cdot \sqrt[n]{b} \geqslant 0$. Ponadto, $(\sqrt[n]{a} \cdot \sqrt[n]{b})^n = (\sqrt[n]{a})^n \cdot (\sqrt[n]{b})^n = a \cdot b$, czyli z definicji pierwiastka arytmetycznego $\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{a \cdot b}$.

(ii). Skoro $b > 0$, więc $\sqrt[n]{b} > 0$ i na mocy (i), $\sqrt[n]{b} \cdot \sqrt[n]{\frac{a}{b}} = \sqrt[n]{b \cdot \frac{a}{b}} = \sqrt[n]{a}$, skąd po podzieleniu przez $\sqrt[n]{b} \neq 0$ mamy $\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$.

(iii). Dla $a = 0$ mamy, że $k \in \mathbb{N}$ i wtedy $a^k = 0$, $\sqrt[n]{a} = 0$, więc $\sqrt[n]{a^k} = \sqrt[n]{0} = 0 = (\sqrt[n]{a})^k$. Niech teraz $a > 0$. Wtedy $\sqrt[n]{a} > 0$, więc $(\sqrt[n]{a})^k > 0$ oraz na mocy własności 4.28 mamy, że $[(\sqrt[n]{a})^k]^n = (\sqrt[n]{a})^{kn} = [(\sqrt[n]{a})^n]^k = a^k$, więc $(\sqrt[n]{a})^k = \sqrt[n]{a^k}$ z definicji pierwiastka arytmetycznego.

(iv). Ponieważ $a \geqslant 0$, więc też $a^m \geqslant 0$ oraz $(a^m)^n = a^{nm}$ z własności 4.28, więc $a^m = \sqrt[n]{a^{nm}}$ z definicji pierwiastka arytmetycznego. □

Ćwiczenie 6.28. Udowodnić, że dla dowolnej liczby naturalnej n liczba $(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$ jest całkowita i parzysta. Pokazać, że $(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n} = b\sqrt{2}$ dla pewnej liczby całkowitej b.

Ćwiczenie 6.29. Udowodnić, że dla dowolnej liczby rzeczywistej a takiej, że $a^2 - a + 1 \geqslant 0$, $a^2 - a + 1 \geqslant 0$ mamy

$$-1 < \sqrt{a^2 + a + 1} - \sqrt{a^2 - a + 1} < 1.$$

Ćwiczenie 6.30. Znajdź liczby rzeczywiste a, b, c takie, że

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c}.$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 7

Ciało liczb zespolonych

Liczby zespolone zostały wprowadzone około 1545 roku przez słynnego włoskiego hazardzistę i matematyka Girolamo Cardana, który żył w latach 1501-1576. Cardano znalazł jawny wzór na wszystkie trzy pierwiastki równania stopnia trzeciego. Wielu matematyków przyczyniło się do pełnego rozwoju liczb zespolonych. Zasady dodawania, odejmowania, mnożenia i dzielenia liczb zespolonych opracował włoski matematyk Rafael Bombelli. Podstawowe oznaczenia, w tym i, zostały wprowadzone przez Leonarda Eulera, który zwizualizował liczby zespolone jako punkty na płaszczyźnie. Termin **liczba zespolona** wprowadził Carl Friedrich Gauss. Cauchy, francuski matematyk współczesny Gaussowi, rozszerzył pojęcie liczb zespolonych na pojęcie funkcji zespolonych. Czytelnikom zainteresowanym historią odkrywania liczb zespolonych można polecić na przykład pozycję [26].

Liczby zespolone można utożsamiać z trzema zbiorami: punktami na płaszczyźnie, zbiorem wszystkich (swobodnych) wektorów na płaszczyźnie oraz zbiorem wszystkich uporządkowanych par liczb rzeczywistych. Geometryczny obraz liczb zespolonych jako punktów na płaszczyźnie po raz pierwszy został opisany przez norwesko-duńskiego geodetę i matematyka Caspara Wessela, który żył w latach 1745–1818.

Przez długi czas uważano, że liczby zespolone to "zabawki" wymyślone i używane tylko przez matematyków. W końcu żadna pojedyncza wielkość w rzeczywistym świecie nie może być zmierzona liczbą

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

urojoną, liczbą, która żyje tylko w wyobraźni matematyków. Jednak w 1926 roku, austriacki fizyk teoretyk Erwin Schrödinger odkrył, że w języku świata cząstek subatomowych nieodzownym alfabetem są liczby zespolone. Chociaż żadna pojedyncza mierzalna wielkość fizyczna nie odpowiada liczbie zespolonej, parę wielkości fizycznych można bardzo naturalnie przedstawić za pomocą liczby zespolonej. Na przykład fala, która ma daną amplitudę i fazę, może być reprezentowana przy użyciu liczby zespolonej.

7.1 Konstrukcja ciała liczb zespolonych

W zbiorze $\mathbb{R} \times \mathbb{R}$ wprowadzamy działania $+$ i $\cdot$ za pomocą wzorów:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \tag{7.1}$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + a_2 \cdot b_1), \tag{7.2}$$

dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{R}$.

Twierdzenie 7.1. *Zbiór $\mathbb{R}\times\mathbb{R}$ z działaniami danymi wzorami* (7.1) *i* (7.2) *z wyróżnionymi elementami* $(0,0)$ *i* $(1,0)$ *tworzy ciało.*

Dowód. Sprawdzamy kolejno prawdziwość wszystkich aksjomatów ciała. Niech $a, b, a_1, a_2, a_3, b_1, b_2, b_3$ będą dowolnymi liczbami rzeczywistymi.

A1. Na mocy wzoru (7.1) i przemienności dodawania liczb rzeczywistych
$(a_2, b_2)+(a_1, b_1) = (a_2+a_1, b_2+b_1) = (a_1+a_2, b_1+b_2) = (a_1, b_1)+(a_2, b_2)$.

A2. Na mocy wzoru (7.1) i łączności dodawania liczb rzeczywistych
$[(a_1, b_1) + (a_2, b_2)] + (a_3, b_3) = (a_1 + a_2, b_1 + b_2) + (a_3, b_3) =$
$= ([a_1 + a_2] + a_3, [b_1 + b_2] + b_3) = (a_1 + [a_2 + a_3], b_1 + [b_2 + b_3]) =$
$= (a_1, b_1) + (a_2 + a_3, b_2 + b_3) = (a_1, b_1) + [(a_2, b_2) + (a_3, b_3)]$.

A3. Na mocy wzoru (7.1) i tego, że 0 jest elementem neutralnym dodawania liczb rzeczywistych $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$.

A4. Na mocy wzoru (7.1) mamy, że $(a, b) + (-a, -b) =$
$= (a + (-a), b + (-b)) = (0, 0)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

A5. Na mocy wzoru (7.2) i przemienności mnożenia liczb rzeczywistych mamy, że $(a_2, b_2) \cdot (a_1, b_1) = (a_2 \cdot a_1 - b_2 \cdot b_1, a_2 \cdot b_1 + a_1 \cdot b_2) =$
$= (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + a_2 \cdot b_1) = (a_1, b_1) \cdot (a_2, b_2)$.

A6. Na mocy wzoru (7.2), łączności i przemienności mnożenia liczb rzeczywistych, a także rozdzielności mnożenia liczb rzeczywistych względem dodawania (odejmowania) liczb rzeczywistych mamy:
$[(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \cdot (a_3, b_3) =$
$= ([a_1a_2 - b_1b_2] \cdot a_3 - [a_1b_2 + a_2b_1] \cdot b_3, [a_1a_2 - b_1b_2] \cdot b_3 + a_3 \cdot [a_1b_2 + a_2b_1]) =$
$= (a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - a_2b_1b_3, a_1a_2b_3 - b_1b_2b_3 + a_3a_1b_2 + a_3a_2b_1)$
oraz $(a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] = (a_1, b_1) \cdot (a_2a_3 - b_2b_3, a_2b_3 + a_3b_2) =$
$= (a_1 \cdot [a_2a_3 - b_2b_3] - b_1 \cdot [a_2b_3 + a_3b_2], a_1 \cdot [a_2b_3 + a_3b_2] + [a_2a_3 - b_2b_3] \cdot b_1) =$
$= (a_1a_2a_3 - a_1b_2b_3 - b_1a_2b_3 - b_1a_3b_2, a_1a_2b_3 + a_1a_3b_2 + a_2a_3b_1 - b_2b_3b_1)$.
Zatem $(a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] = [(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3)$.

A7. Na mocy wzoru (7.2) i różnych praw działań na liczbach rzeczywistych (jakich?): $(a_1, b_1) \cdot (a, 0) = (a_1 \cdot a - b_1 \cdot 0, a_1 \cdot 0 + a \cdot b_1) =$
$= (a \cdot a_1, a \cdot b_1)$, więc w szczególności dla $a = 1$: $(a_1, b_1) \cdot (1, 0) = (a_1, b_1)$, gdyż 1 jest elementem neutralnym mnożenia liczb rzeczywistych.

A8. Na mocy wzorów (7.1) i (7.2) oraz różnych praw działań arytmetycznych na liczbach rzeczywistych (jakich?) dostajemy, że
$(a_1, b_1) \cdot [(a_2, b_2) + (a_3, b_3)] = (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) =$
$= (a_1 \cdot [a_2 + a_3] - b_1 \cdot [b_2 + b_3], a_1 \cdot [b_2 + b_3] + [a_2 + a_3] \cdot b_1) =$
$= (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3, a_1b_2 + a_1b_3 + a_2b_1 + a_3b_1) =$
$= (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) + (a_1a_3 - b_1b_3, a_1b_3 + a_3b_1) = (a_1, b_1) \cdot (a_2, b_2) +$
$+ (a_1, b_1) \cdot (a_3, b_3)$.

A9. Niech $(a, b) \neq (0, 0)$. Wtedy $a \neq 0$ lub $b \neq 0$, skąd $a^2 + b^2 > 0$. Zatem liczby $\frac{a}{a^2+b^2}$ i $\frac{-b}{a^2+b^2}$ są dobrze określone oraz ze wzoru (7.2)
$(a, b) \cdot (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = (a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{(-b)}{a^2+b^2}, a\frac{(-b)}{a^2+b^2} + \frac{a}{a^2+b^2} \cdot b) = (\frac{a^2+b^2}{a^2+b^2}, 0) =$
$= (1, 0)$. □

Otrzymane w ten sposób ciało oznaczamy przez $\mathbb{C}$ i nazywamy **ciałem liczb zespolonych**. Elementy ciała $\mathbb{C}$ nazywamy **liczbami zespolonymi** i oznaczamy literami: z, w, z_1, z_2, i tak dalej. Geometrycznie liczby zespolone można więc traktować jako punkty na płaszczyźnie. Ze wzoru (7.1) wynika, że liczby zespolone dodajemy analogicznie jak wektory na płaszczyźnie zaczepione w początku układu

współrzędnych. Z tego powodu liczbę zespoloną (a, b) możemy utożsamić z wektorem o początku w punkcie $(0, 0)$ i końcu w punkcie (a, b). Interpretacja geometryczna mnożenia liczb zespolonych jest bardziej złożona.

Z określeń (7.1) i (7.2) i z dowodu twierdzenia 7.1 wynika od razu, że dla dowolnych liczb rzeczywistych a, b

$$\begin{gathered}(a,0)=(b,0)\Leftrightarrow a=b,\\(a,0)+(b,0)=(a+b,0),\\(a,0)\cdot(b,0)=(a\cdot b,0),\\-(a,0)=(-a,0),\\(a,0)^{-1}=(\tfrac{1}{a},0)\text{ dla }a\neq 0.\end{gathered}$$

Z tego powodu dla liczb rzeczywistych a można dokonać utożsamienia:

$$(a,0)\equiv a. \tag{7.3}$$

Przy takim utożsamieniu $\mathbb{R}\subseteq\mathbb{C}$.

Liczbę zespoloną

$$i=(0,1) \tag{7.4}$$

nazywamy **jednostką urojoną**. Zachodzi dla niej bardzo ważny wzór:

$$i^2=-1. \tag{7.5}$$

Rzeczywiście, na mocy wzoru (7.2):
$i^2=(0,1)\cdot(0,1)=(0\cdot 0-1\cdot 1,0\cdot 1+0\cdot 1)=(-1,0)\equiv -1$.

Z dowodu twierdzenia 7.1 dla dowolnych liczb rzeczywistych a, b mamy, że $(a,b)=(a,0)+(0,b)=(a,0)+(b,0)\cdot(0,1)\equiv a+bi$. Zatem dla $a,b\in\mathbb{R}$ można dokonać utożsamienia:

$$(a,b)\equiv a+bi. \tag{7.6}$$

Otrzymujemy w ten sposób **postać algebraiczną** $a+bi$ liczby zespolonej (a,b).

Dodawanie, odejmowanie i mnożenie liczb zespolonych zapisanych w postaci algebraicznej wykonuje się zatem tak samo jak dodawanie,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

odejmowanie i mnożenie wielomianów zmiennej i, przy czym należy pamiętać o tym, że w miejsce i^2 należy zawsze podstawić (-1). Na przykład $(1+2i)\cdot(3-i) = 3-i+6i-2i^2 = 3+5i+2 = 5+5i$, $(1+2i)+(3-i) = 4+i$, $(1+2i)-(3-i) = -2+3i$.

Natomiast przy dzieleniu liczb zespolonych wygodnie jest wykorzystywać tak zwane liczby sprzężone. Jeżeli a i b są liczbami rzeczywistymi, to **liczbą sprzężoną** do liczby $z = a+bi$ nazywamy liczbę $\overline{z} = a-bi$. Wówczas $z\cdot\overline{z} = (a+bi)\cdot(a-bi) = a^2-b^2i^2 = a^2-b^2\cdot(-1) = a^2+b^2 \in \mathbb{R}$. Zatem **aby podzielić liczbę zespoloną w przez liczbę zespoloną $z \neq 0$ należy licznik i mianownik ułamka $\frac{w}{z}$ pomnożyć przez liczbę sprzężoną z mianownikiem tego ułamka**, czyli $\frac{w}{z} = \frac{w\cdot\overline{z}}{z\cdot\overline{z}} = \frac{w\cdot\overline{z}}{a^2+b^2}$. Na przykład

$$\frac{2+3i}{1+i} = \frac{(2+3i)\cdot(1-i)}{(1+i)\cdot(1-i)} = \frac{2-2i+3i-3i^2}{1^2+1^2} = \frac{2+i+3}{2} = \frac{5}{2}+\frac{1}{2}i.$$

Jeżeli a, b są liczbami rzeczywistymi oraz $z = a+bi$, to **częścią rzeczywistą** liczby zespolonej z nazywamy liczbę $re(z) = a$, zaś **częścią urojoną** liczby z nazywamy liczbę (rzeczywistą!) $im(z) = b$. Na przykład $re(i) = 0$ oraz $im(i) = 1$. Łatwo zauważyć, że $re(z+w) = re(z)+re(w)$ dla dowolnych liczb zespolonych z, w. Ponadto, z tych oznaczeń wynika natychmiast, że **dwie liczby zespolone zapisane w postaci algebraicznej są równe wtedy i tylko wtedy, gdy ich części rzeczywiste są równe i ich części urojone są równe**:

$$z = w \iff [re(z) = re(w) \text{ oraz } im(z) = im(w)]. \tag{7.7}$$

Modułem liczby zespolonej $z = a+bi$, gdzie $a, b \in \mathbb{R}$ nazywamy liczbę rzeczywistą nieujemną

$$|z| = \sqrt{a^2+b^2}. \tag{7.8}$$

Z tych określeń mamy od razu, że

$$re(z) \leqslant |z| \text{ oraz } im(z) \leqslant |z|, \tag{7.9}$$

$$z\cdot\overline{z} = |z|^2. \tag{7.10}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

7.2 Własności sprzęgania

Własność 7.2. *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnych liczb zespolonych $z_1, z_2, \ldots, z_n$:*

$$\overline{z_1 + z_2 + \ldots + z_n} = \overline{z_1} + \overline{z_2} + \ldots + \overline{z_n}.$$

Dowód. Istnieją liczby rzeczywiste $a_1, \ldots, a_n, b_1, \ldots, b_n$ takie, że $z_k = a_k + b_k i$ dla $k = 1, \ldots, n$. Zatem $z_1 + \ldots + z_n = (a_1 + b_1 i) + \ldots + (a_n + b_n i) = (a_1 + \ldots + a_n) + (b_1 + \ldots + b_n)i$, skąd $\overline{z_1 + \ldots + z_n} = (a_1 + \ldots + a_n) - (b_1 + \ldots + b_n)i$ oraz $\overline{z_1} + \ldots + \overline{z_n} = (a_1 - b_1 i) + \ldots + (a_n - b_n i) = (a_1 + \ldots + a_n) - (b_1 + \ldots + b_n)i$, skąd mamy tezę. □

Własność 7.3. *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnych liczb zespolonych $z_1, z_2, \ldots, z_n$:*

$$\overline{z_1 \cdot z_2 \cdot \ldots \cdot z_n} = \overline{z_1} \cdot \overline{z_2} \cdot \ldots \cdot \overline{z_n}.$$

Dowód. Dla $n = 2$ istnieją liczby rzeczywiste a_1, a_2, b_1, b_2 takie, że $z_1 = a_1 + b_1 i$ oraz $z_2 = a_2 + b_2 i$. Stąd $z_1 \cdot z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$, czyli $\overline{z_1 \cdot z_2} = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + a_2 b_1)i$ oraz $\overline{z_1} \cdot \overline{z_2} = (a_1 - b_1 i) \cdot (a_2 - b_2 i) = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + a_2 b_1)i$, czyli teza zachodzi dla $n = 2$. Załóżmy teraz, że teza zachodzi dla pewnego naturalnego n. Wówczas dla liczb zespolonych $z_1, \ldots, z_n, z_{n+1}$ na mocy pierwszej części dowodu mamy, że $\overline{z_1 \cdot \ldots \cdot z_n \cdot z_{n+1}} = \overline{(z_1 \cdot \ldots \cdot z_n) \cdot z_{n+1}} = \overline{z_1 \cdot \ldots \cdot z_n} \cdot \overline{z_{n+1}}$, więc na mocy założenia indukcyjnego $\overline{z_1 \cdot \ldots \cdot z_n \cdot z_{n+1}} = \overline{z_1} \cdot \ldots \cdot \overline{z_n} \cdot \overline{z_{n+1}}$. Stąd na mocy zasady indukcji mamy tezę. □

Własność 7.4. *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnego $z \in \mathbb{C}$:*

$$\overline{z^n} = (\overline{z})^n.$$

Dowód. Wystarczy we własności 7.3 podstawić $z = z_1 = \ldots = z_n$. □

Własność 7.5. *Dla dowolnych $z, w \in \mathbb{C}$ takich, że $w \neq 0$ mamy, że $\overline{w} \neq 0$ oraz zachodzi wzór:*

$$\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}.$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Ponieważ $w \neq 0$ i $w = a + bi$ dla pewnych $a, b \in \mathbb{R}$, więc $a \neq 0$ lub $b \neq 0$, skąd $\overline{w} = a - bi \neq 0$. Ale $z = w \cdot \frac{z}{w}$, więc z własności 7.3, $\overline{z} = \overline{w} \cdot \overline{\left(\frac{z}{w}\right)}$, skąd po podzieleniu obu stron przez $\overline{w} \neq 0$ uzyskamy tezę. □

7.3 Własności modułu

Własność 7.6. *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnych liczb zespolonych $z_1, z_2, \ldots, z_n$:*

$$|z_1 \cdot z_2 \cdot \ldots \cdot z_n| = |z_1| \cdot |z_2| \cdot \ldots \cdot |z_n|.$$

Dowód. Na mocy wzoru (7.10) i własności 7.3 otrzymujemy, że $|z_1 \cdot \ldots \cdot z_n|^2 = (z_1 \cdot \ldots \cdot z_n) \cdot \overline{(z_1 \cdot \ldots \cdot z_n)} = z_1 \cdot \ldots \cdot z_n \cdot \overline{z_1} \cdot \ldots \cdot \overline{z_n} = (z_1 \cdot \overline{z_1}) \cdot \ldots \cdot (z_n \cdot \overline{z_n}) = |z_1|^2 \cdot \ldots \cdot |z_n|^2$, skąd po spierwiastkowaniu obu stron uzyskamy tezę. □

Własność 7.7. *Dla dowolnych $z, w \in \mathbb{C}$ takich, że $w \neq 0$ mamy, że $|w| \neq 0$ oraz zachodzi wzór:*

$$\left|\frac{z}{w}\right| = \frac{|z|}{|w|}.$$

Dowód. Ponieważ $w \neq 0$ i $w = a + bi$ dla pewnych $a, b \in \mathbb{R}$, więc $a \neq 0$ lub $b \neq 0$, skąd $a^2 + b^2 > 0$, a zatem $|w| = \sqrt{a^2 + b^2} \neq 0$. Ale $z = w \cdot \frac{z}{w}$, więc na mocy własności 7.6 otrzymujemy, że $|z| = |w| \cdot \left|\frac{z}{w}\right|$ i po podzieleniu obu stron przez $|w|$ uzyskamy tezę. □

Własność 7.8. *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnego $z \in \mathbb{C}$:*

$$|z^n| = |z|^n.$$

Dowód. Wystarczy podstawić $z = z_1 = \ldots = z_n$ we własności 7.6. □

Własność 7.9. (Nierówność trójkąta). *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnych liczb zespolonych $z_1, z_2, \ldots, z_n$:*

$$|z_1 + z_2 + \ldots + z_n| \leqslant |z_1| + |z_2| + \ldots + |z_n|.$$

Dowód. Zastosujemy indukcję ze względu na n. Niech $n = 2$. Jeśli $z_1 + z_2 = 0$, to nasz wzór zachodzi. Załóżmy dalej, że $z_1 + z_2 \neq 0$. Wtedy $|z_1 + z_2| > 0$. Ponadto $1 = re\left(\frac{z_1}{z_1+z_2} + + \frac{z_2}{z_1+z_2}\right) = re\left(\frac{z_1}{z_1+z_2}\right) + +re\left(\frac{z_2}{z_1+z_2}\right) \leqslant \left|\frac{z_1}{z_1+z_2}\right| + \left|\frac{z_2}{z_1+z_2}\right| = \frac{|z_1|}{|z_1+z_2|} + \frac{|z_2|}{|z_1+z_2|}$, skąd po pomnożeniu obu stron przez $|z_1 + z_2|$ uzyskamy tezę dla $n = 2$.
Załóżmy teraz, że nasza nierówność zachodzi dla pewnej liczby naturalnej n i niech $z_1, \ldots, z_{n+1}$ będą dowolnymi liczbami zespolonymi. Wówczas z pierwszej części dowodu i z założenia indukcyjnego mamy, że $|z_1 + \ldots + z_{n+1}| = |(z_1 + \ldots + z_n) + z_{n+1}| \leqslant |z_1 + \ldots + z_n| + |z_{n+1}| \leqslant$ $\leqslant |z_1| + \ldots + |z_n| + |z_{n+1}|$, czyli nasza nierówność zachodzi dla liczby $n + 1$.
Stąd na mocy zasady indukcji mamy tezę. □

Ćwiczenie 7.10. Udowodnić, że dla dowolnej liczby naturalnej n mamy $(1 + i)^{8n} = 2^{4n}$ oraz $(1 + i)^{4n} = (-1)^n 2^{2n}$.

Ćwiczenie 7.11. Udowodnić, że dla dowolnych liczb zespolonych z_1, z_2 mamy

$$|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2(|z_1|^2 + |z_2|^2),$$

$$|1 + z_1\overline{z_2}|^2 + |z_1 - z_2|^2 = (1 + |z_1|^2)(1 + |z_2|^2).$$

Ćwiczenie 7.12. Załóżmy, że dla liczb zespolonych z_1, z_2 oraz z_3 mamy $|z_1| = |z_2| = |z_3| \overset{\text{ozn}}{=} r$. Udowodnić, że

$$|z_1z_2 + z_2z_3 + z_3z_1| = r|z_1 + z_2 + z_3|.$$

Ćwiczenie 7.13. Korzystając z własności modułu liczby zespolonej wykazać, że iloczyn dwóch liczb całkowitych z których każda jest sumą kwadratów pewnych dwóch liczb całkowitych jest też sumą kwadratów pewnych dwóch liczb całkowitych.

Czytelnika pragnącego pogłębić swoją wiedzę na temat liczb zespolonych odsyłamy do monografii [5].

Rozdział 8

Podzielność liczb całkowitych

8.1 Określenie i własności podzielności liczb całkowitych

Podzielności liczb całkowitych nie definiujemy za pomocą dzielenia, lecz za pomocą mnożenia liczb całkowitych. Mianowicie:

Definicja 8.1. Powiemy, że liczba całkowita a **dzieli liczbę całkowitą** b (a jest dzielnikiem b, b jest podzielne przez a, b jest wielokrotnością a), jeżeli istnieje taka liczba całkowita t, że $b = a \cdot t$. Piszemy wtedy $a \mid b$. Jeżeli a nie dzieli b, to piszemy $a \nmid b$.

Przykład 8.2. Dla dowolnej liczby całkowitej a mamy, że

(1) $a \mid a$ (gdyż $a = a \cdot 1$), to znaczy każda liczba całkowita dzieli siebie,

(2) $a \mid 0$ (gdyż $0 = a \cdot 0$), to znaczy 0 jest podzielne przez każdą liczbę całkowitą,

(3) $1 \mid a$ (gdyż $a = 1 \cdot a$), to znaczy każda liczba całkowita jest podzielna przez 1,

(4) $0 \mid a \Leftrightarrow a = 0$ (bo $0 = 0 \cdot 0$ i jeżeli $0 \mid a$, to istnieje całkowite t takie, że $a = 0 \cdot t$, skąd $a = 0$), to znaczy 0 jest jedyną liczbą całkowitą podzielną przez 0.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 8.3. *Liczba całkowita a jest podzielna przez liczbę naturalną m wtedy i tylko wtedy, gdy a daje resztę 0 z dzielenia przez m.*

Dowód. Jeżeli $[a]_m = 0$, to z twierdzenia o dzieleniu z resztą $a = qm$ dla pewnego $q \in \mathbb{Z}$, czyli $m \mid a$. Na odwrót, jeśli $m \mid a$, to $a = tm$ dla pewnego $t \in \mathbb{Z}$, więc $a = tm + 0$ i z twierdzenia o dzieleniu z resztą wynika, że $[a]_m = 0$. □

Przykład 8.4. Na mocy uwagi 2.26, $[101]_7 = 3$, więc ze stwierdzenia 8.3 mamy, że $7 \nmid 101$.

Przykład 8.5. Z przykładu 2.35 i ze stwierdzenia 8.3 mamy, że $31 \nmid 10^n + a$ dla dowolnej liczby naturalnej n i dla każdego $a \in \in \{1, 2, 4, 5, 7, 8, 9\}$.

Twierdzenie 8.6. *Wśród dowolnych kolejnych m liczb całkowitych istnieje dokładnie jedna liczba podzielna przez liczbę naturalną m.*

Dowód. Teza jest oczywista dla $m = 1$. Niech dalej $m > 1$. Ogólna postać m kolejnych liczb całkowitych: $n, n+1, \ldots, n+(m-1)$, gdzie $n \in \mathbb{Z}$. Z twierdzenia o dzieleniu z resztą $n = qm + r$ dla pewnych $q, r \in \mathbb{Z}$ takich, że $0 \leqslant r < m$. Jeśli $r = 0$, to $m \mid n$. Jeśli zaś $r \neq 0$, to $1 \leqslant r \leqslant m-1$, więc $0 < m - r < m$ i wtedy liczba $n + (m - r)$ występuje w ciągu $n, n+1, \ldots, n+(m-1)$ oraz $n+(m-r) = (q+1)m$, więc ta liczba jest podzielna przez m.

Przypuśćmy, że wśród liczb $n, n+1, \ldots, n+(m-1)$ co najmniej dwie są podzielne przez m. Wtedy istnieją liczby całkowite i, j takie, że $0 \leqslant i < j < m$ oraz $m \mid n+i$ i $m \mid n+j$. Zatem $m+i = km$ i $m+j = lm$ dla pewnych $k, l \in \mathbb{Z}$. Stąd $j - i = (l-k)m$, ale $0 < j - i \leqslant j < m$, więc $0 < (l-k)m < m$, skąd $0 < l - k < 1$, co przeczy temu, że $l - k$ jest liczbą całkowitą.

Wobec tego wśród dowolnych kolejnych m liczb całkowitych istnieje dokładnie jedna liczba podzielna przez m. □

Przykład 8.7. Pokażemy, że dla każdej liczby całkowitej k liczba $k^3 + 3k^2 + 2k$ jest podzielna przez 3. Zauważmy, że $k^3 + 3k^2 + 2k =$

$= k(k^2 + 3k + 2) = k(k + 1)(k + 2)$, czyli liczba $k^3 + 3k^2 + 2k$ jest iloczynem trzech kolejnych liczb całkowitych k, $k + 1$ i $k + 2$, a zatem na mocy twierdzenia 8.6 ta liczba jest podzielna przez 3.

Stwierdzenie 8.8. *Niech a, b, c będą dowolnymi liczbami całkowitymi. Wówczas:*
(1) *jeżeli $a \mid b$ i $b \mid c$, to $a \mid c$,*
(2) *jeżeli $a \mid b$ i $a \mid c$, to $a \mid (b \cdot x + c \cdot y)$ dla dowolnych liczb całkowitych x, y (w szczególności $a \mid (b + c)$ oraz $a \mid (b - c)$),*
(3) *jeżeli $a \mid b$ i $a \mid (b + c)$, to $a \mid c$,*
(4) *warunki: $a \mid b$, $a \mid (-b)$, $(-a) \mid b$ i $(-a) \mid (-b)$ są równoważne,*
(5) *dla $c \neq 0$: $a \mid b \iff (a \cdot c) \mid (b \cdot c)$.*
(6) *jeżeli $c \mid (a - b)$, to $c \mid a \iff c \mid b$.*

Dowód. (1). Z założenia istnieją liczby całkowite t, s takie, że $b = a \cdot t$ i $c = b \cdot s$, skąd $c = a \cdot (t \cdot s)$, ale $t \cdot s$ jest liczbą całkowitą, więc $a \mid c$.

(2). Z założenia istnieją liczby całkowite t, s takie, że $b = a \cdot t$ i $c = a \cdot s$. Zatem dla $x, y \in \mathbb{Z}$ mamy, że $b \cdot x + c \cdot y = a \cdot t \cdot x + a \cdot s \cdot y = a \cdot (t \cdot x + s \cdot y)$. Ponadto $t \cdot x + s \cdot y$ jest liczbą całkowitą, więc $a \mid (b \cdot x + c \cdot y)$. Podstawiając $x = y = 1$ uzyskamy, że $a \mid (a + b)$. Podstawiając $x = 1, y = -1$ uzyskamy, że $a \mid (b - c)$.

(3). Na mocy (2) mamy, że $a \mid [(b + c) - b]$, czyli $a \mid c$.

(4). Jeżeli $a \mid b$, to istnieje całkowite t takie, że $b = a \cdot t$, skąd $-b = a \cdot (-t)$ i $(-t)$ jest całkowite, więc $a \mid (-b)$. Jeżeli $a \mid (-b)$, to istnieje całkowite t takie, że $-b = a \cdot t$, skąd $b = (-a) \cdot t$, więc $(-a) \mid b$. Jeżeli $(-a) \mid b$, to istnieje całkowite t takie, że $b = (-a) \cdot t$, skąd $-b = (-a) \cdot (-t)$, więc $(-a) \mid (-b)$. Jeżeli $(-a) \mid (-b)$, to istnieje całkowite t takie, że $-b = (-a) \cdot t$, skąd $b = a \cdot t$, więc $a \mid b$.

(5). Jeżeli $a \mid b$, to istnieje całkowite t takie, że $b = a \cdot t$, skąd $b \cdot c = a \cdot c \cdot t$, czyli $(a \cdot c) \mid (b \cdot c)$. Jeżeli zaś $(a \cdot c) \mid (b \cdot c)$, to istnieje całkowite t takie, że $b \cdot c = a \cdot c \cdot t$ i $c \neq 0$, więc $b = a \cdot t$, skąd $a \mid b$.

(6). Niech $c \mid (a - b)$. Jeśli $c \mid b$, to na mocy (2), $c \mid ((a - b) + b)$, czyli $c \mid a$. Jeżeli zaś $c \mid a$, to na mocy (2), $c \mid (a - (a - b))$, czyli $c \mid b$. □

Przykład 8.9. Stwierdzenie 8.8 (6) stosuje się do wykazywania znanych ze szkoły cech podzielności przez liczby: 2, 3, 4, 5 i 9. Mianowicie zauważamy, że $10 - 1 = 9$, $100 - 1 = 99 = 9 \cdot 11$, $1000 - 1 =$

$= 999 = 9 \cdot 111$, itd. i ogólnie dla naturalnych n:

$$1\underbrace{00\ldots0}_{n\ zer} - 1 = \underbrace{99\ldots9}_{n\ cyfr\ 9} = 9 \cdot \underbrace{11\ldots1}_{n\ jedynek}, \tag{8.1}$$

skąd wynika, że $9 \mid (10^k - 1)$ i $3 \mid (10^k - 1)$ dla każdego $k \in \mathbb{N}$. Niech $n \in \mathbb{N}$ i niech a będzie liczbą naturalną $(n+1)$-cyfrową. Oznaczmy kolejne cyfry tej liczby od prawej strony przez $c_0, c_1, \ldots, c_n$. Wtedy $a = c_0 + 10c_1 + 10^2c_2 + \ldots + 10^nc_n$ i często będziemy pisali, że

$$a = \overline{c_n \ldots c_1 c_0} \tag{8.2}$$

(aby odróżnić liczbę a od iloczynu $c_n \ldots c_1 c_0$). Na przykład ogólna postać liczby dwucyfrowej to $\overline{xy}$, gdzie $x, y \in \{0, 1, \ldots, 9\}$ i $x \neq 0$.

Sumą cyfr liczby a postaci (8.2) jest liczba $s = c_0 + c_1 + \ldots + c_n$, zaś różnica liczby a i sumy jej cyfr wynosi $a - s = 9c_1 + 99c_2 + \ldots + \underbrace{99\ldots9}_{n\ cyfr\ 9}c_n$. Po wyciągnięciu przed nawias liczby 9 widzimy zatem, że $9 \mid (a - s)$ i $3 \mid (a - s)$. Zatem na mocy stwierdzenie 8.8 (6) mamy następujące cechy podzielności przez 3 i 9:

Liczba naturalna jest podzielna przez 3 wtedy i tylko wtedy, gdy suma jej cyfr jest podzielna przez 3.

Liczba naturalna jest podzielna przez 9 wtedy i tylko wtedy, gdy suma jej cyfr jest podzielna przez 9.

Zauważmy, że dla liczby a postaci (8.2), $2 \mid (a - c_0)$ i $5 \mid (a - c_0)$, więc na mocy stwierdzenie 8.8 (6) mamy następujące cechy podzielności przez 2 i 5:

Liczba naturalna jest podzielna przez 2 wtedy i tylko wtedy, gdy jej cyfra jedności jest podzielna przez 2.

Liczba naturalna jest podzielna przez 5 wtedy i tylko wtedy, gdy jej cyfra jedności jest podzielna przez 5.

Oczywiście, cyframi podzielnymi przez 2 są jedynie: 0, 2, 4, 6 i 8, zaś cyframi podzielnymi przez 5 są jedynie 0 i 5.

Liczbą utworzoną z dwóch ostatnich cyfr liczby a postaci (8.2) nazywamy liczbę $\overline{c_1 c_0} = 10c_1 + c_0$. Zauważmy, że $100 \mid (a - \overline{c_1 c_0})$ i $4 \mid 100$, więc na mocy stwierdzenia 8.8 (6) otrzymujemy stąd cechę podzielności przez 4:

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Liczba naturalna jest podzielna przez 4 wtedy i tylko wtedy, gdy liczba utworzona z jej dwóch ostatnich cyfr jest podzielna przez 4.

8.2 Podzielność przez liczby naturalne

Przykład 8.2 i stwierdzenie 8.8 (4) redukują badanie podzielności liczb całkowitych do badania podzielności przez liczby naturalne.

Przykład 8.10. Zbadamy dla jakich $n \in \mathbb{N}$ liczba n^2+1 jest podzielna przez liczbę $n+1$. Dla $n=1$: $n^2+1 = n+1 = 2$ i $2 \mid 2$. Natomiast dla $n>1$ mamy, że $2 < n+1$ i $n^2+1 = (n-1)\cdot(n+1)+2$, więc $[n^2+1]_{n+1} = 2 \neq 0$, a zatem wtedy $n+1 \nmid n^2+1$. Wobec tego: $n+1 \mid n^2+1 \iff n=1$.

Ćwiczenie 8.11. Udowodnij, że jeżeli $n \in \mathbb{N}$, to liczba n^2+2 jest podzielna przez $n+2$ wtedy i tylko wtedy, gdy $n \in \{1,4\}$.

Stwierdzenie 8.12. *Niech m,n będą liczbami naturalnymi. Wówczas:*

(i) $m \mid n \iff$ [istnieje $t \in \mathbb{N}$ takie, że $n = t \cdot m$],

(ii) jeżeli $m \mid n$, *to* $m \leqslant n$,

(iii) jeżeli $m \mid n$ *i* $n \mid m$, *to* $m = n$.

Dowód. (i). Jeżeli $m \mid n$, to $n = t \cdot m$ dla pewnego $t \in \mathbb{Z}$, ale $m, n > 0$, więc $t \cdot m > 0$ i $m > 0$, skąd $t > 0$, czyli $t \in \mathbb{N}$. Jeżeli zaś $n = t \cdot m$ dla pewnego $t \in \mathbb{N}$, to $t \in \mathbb{Z}$, więc $m \mid n$.

(ii). Załóżmy, że $m \mid n$. Wtedy na mocy (i), $n = t \cdot m$ dla pewnego $t \in \mathbb{N}$. Stąd $t \geqslant 1$, więc $t \cdot m \geqslant 1 \cdot m$, a zatem $n \geqslant m$.

(iii). Załóżmy, że $m \mid n$ i $n \mid m$. Wtedy z (ii), $m \leqslant n$ i $n \leqslant m$, skąd $m = n$. □

Stwierdzenie 8.13. *Niech m będzie liczbą naturalną. Wówczas różnica liczb całkowitych a, b jest podzielna przez m wtedy i tylko wtedy, gdy te liczby dają takie same reszty z dzielenia przez m.*

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Załóżmy, że $m \mid (a-b)$. Zatem $a-b = t \cdot m$ dla pewnego $t \in \mathbb{Z}$, skąd $a = b + tm$. Z twierdzenia 2.25 (o dzieleniu z resztą), istnieją $u, v \in \mathbb{Z}$ takie, że $a = um + [a]_m$ i $b = vm + [b]_m$. Stąd $a = vm+[b]_m+tm = (t+v)m+[b]_m$. Ponadto $t+v \in \mathbb{Z}$ oraz $a = um+[a]_m$ i $a = (t+v)m + [b]_m$, więc z twierdzenia 2.25, $u = t+v$ i $[a]_m = [b]_m$, czyli liczby a i b dają takie same reszty z dzielenia przez m.

Na odwrót, załóżmy, że $[a]_m = [b]_m$. Z twierdzenia 2.25, $a = qm + [a]_m$ i $b = tm + [b]_m$ dla pewnych $q, t \in \mathbb{Z}$, skąd $a - b = (q-t)m$, a ponieważ $q - t \in \mathbb{Z}$, więc $m \mid (a-b)$. □

Przykład 8.14. Ze stwierdzenia 8.13 i z przykładu 8.9 wynikają od razu następujące, znane ze szkoły, fakty:

Reszta z dzielenia liczby naturalnej przez 3 jest równa reszcie z dzielenia przez 3 sumy cyfr tej liczby.

Reszta z dzielenia liczby naturalnej przez 9 jest równa reszcie z dzielenia przez 9 sumy cyfr tej liczby.

Reszta z dzielenia liczby naturalnej przez 2 jest równa reszcie z dzielenia przez 2 jej cyfry jedności.

Reszta z dzielenia liczby naturalnej przez 5 jest równa reszcie z dzielenia przez 5 jej cyfry jedności.

Reszta z dzielenia liczby naturalnej przez 4 jest równa reszcie z dzielenia przez 4 liczby utworzonej z dwóch ostatnich cyfr tej liczby.

Ćwiczenie 8.15. Wyznacz wszystkie cyfry x takie, że liczba $2343x$ jest podzielna przez 4 i jest podzielna przez 9.

Niech d będzie liczbą naturalną dzielącą liczbę naturalną m. Wówczas będziemy mówili, że d jest naturalnym dzielnikiem liczby m. Wtedy ze stwierdzenia 8.12 istnieje liczba naturalna d' taka, że $m = d \cdot d'$, skąd mamy, że $d' \mid m$. W tej sytuacji liczbę d' będziemy nazywali **dzielnikiem dopełniającym** dla d liczby m. Oczywiście $d' = \frac{m}{d}$. Zauważmy, że wówczas d jest dzielnikiem dopełniającym dla d' liczby m, czyli $(d')' = d$. **Zbiór wszystkich naturalnych dzielników liczby** m będziemy oznaczali przez D_m. Na przykład $D_1 = \{1\}$ i $D_2 = \{1, 2\}$ na mocy stwierdzenia 8.12.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Twierdzenie 8.16. *Niech* $1 = d_1 < d_2 < \ldots < d_k$ *będą wszystkimi naturalnymi dzielnikami liczby naturalnej* m*, których kwadraty są* $\leqslant m$*. Wówczas liczby*

$$1 = d_1 < d_2 < \ldots < d_k \leqslant d'_k < d'_{k-1} < \ldots < d'_2 < d'_1 = m \qquad (8.3)$$

są wszystkimi dzielnikami naturalnymi liczby m*.*

Dowód. Mamy, że $d_k \cdot d'_k = m$ i $d_k^2 \leqslant m$, więc $d_k^2 \leqslant d_k \cdot d'_k$, skąd $d_k \leqslant d'_k$. Niech $i, j = 1, ..., k$ oraz $i < j$. Wtedy $d_i < d_j$, skąd $d'_i = \frac{m}{d_i} > \frac{m}{d_j} = d'_j$. Zatem $d_1 < ... < d_k \leqslant d'_k < d'_{k-1} < ... < d'_1$ oraz wypisane liczby są dzielnikami m. Przypuśćmy, że nie są to wszystkie dzielniki naturalne liczby m. Wówczas istnieje dzielnik naturalny d liczby m różny od wszystkich liczb postaci (8.3). Wtedy $d^2 > m$ na mocy założenia o liczbach $d_1, ..., d_k$ oraz $d \cdot d' = m$. Gdyby $(d')^2 > m$, to $d^2 \cdot (d')^2 > m^2$, skąd $m = d \cdot d' > m$ i mamy sprzeczność. Zatem $(d')^2 \leqslant m$, skąd istnieje $i \leqslant k$ takie, że $d' = d_i$. Wtedy $d = (d')' = d'_i$ i mamy sprzeczność. Zatem liczby (8.3) są wszystkimi dzielnikami naturalnymi liczby m. □

Przykład 8.17. Wyznaczymy wszystkie dzielniki naturalne liczby 56. Mamy, że $7^2 \leqslant 56 < 8^2$. Wypisujemy zatem liczby 1, 2, 3, 4, 5, 6, 7 i sprawdzamy kolejno, która z nich dzieli liczbę 56. $1 \mid 56$, więc $d_1 = 1$ oraz $d'_1 = 56$, $2 \mid 56$, więc $d_2 = 2$ oraz $d'_2 = 28$, $3 \nmid 56$, bo $3 \nmid (5 + 6)$, gdyż $3 \nmid (1 + 1)$, a ponieważ $3 \mid 6$, więc też $6 \nmid 56$. Dalej, $4 \cdot 14 = 56$, więc $d_3 = 4$ oraz $d'_3 = 14$, $5 \nmid 56$, bo $6 \neq 0, 5$. $56 = 7 \cdot 8$, więc $d_4 = 7$ oraz $d'_4 = 8$. Zatem z twierdzenia 8.16, $D_{56} = \{1, 56; 2, 28; 4, 14; 7, 8\}$.

Ćwiczenie 8.18. Stosując twierdzenie 8.16 wyznacz wszystkie dzielniki naturalne liczby 96.

Wniosek 8.19. *Liczba naturalna* m *posiada nieparzystą liczbę wszystkich dzielników naturalnych wtedy i tylko wtedy, gdy* m *jest kwadratem liczby naturalnej.*

Dowód. Zastosujmy do liczby m oznaczenia twierdzenia 8.16. Jeżeli $d_k < d'_k$, to liczba wszystkich dzielników naturalnych liczby m jest

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

równa $2k$, czyli jest liczbą parzystą. Jeżeli zaś $d_k = d'_k$, to liczba wszystkich dzielników naturalnych liczby m jest równa $k + (k-1) = 2k - 1$, a więc jest liczbą nieparzystą i wówczas $m = d_k \cdot d'_k = d_k^2$, czyli m jest kwadratem liczby naturalnej. Wobec tego, jeśli liczba m posiada nieparzystą liczbę wszystkich dzielników naturalnych, to m jest kwadratem liczby naturalnej.

Na odwrót, niech $m = n^2$ dla pewnego $n \in \mathbb{N}$. Wtedy $d_k = d'_k = n$, więc liczba m posiada nieparzystą liczbę wszystkich dzielników naturalnych. □

8.3 Największy wspólny dzielnik

Mówimy, że liczba naturalna d jest **wspólnym dzielnikiem** liczb całkowitych $a_1, ..., a_k$, jeżeli $d \mid a_i$ dla każdego $i = 1, 2, ..., k$. **Zbiór wszystkich wspólnych dzielników liczb** $a_1, a_2, ..., a_k$ oznaczamy symbolem $D(a_1, a_2, \ldots, a_k)$. Wobec tego mamy wzór:

$$D(a_1, a_2, \ldots, a_k) = D_{a_1} \cap D_{a_2} \cap \ldots \cap D_{a_k}. \tag{8.4}$$

Największym wspólnym dzielnikiem liczb $a_1, a_2, \ldots, a_k$ nazywamy największą liczbę w zbiorze $D(a_1, a_2, \ldots, a_k)$ i oznaczamy ją symbolem $\mathrm{NWD}(a_1, a_2, \ldots, a_k)$. Największy wspólny dzielnik liczb całkowitych $a_1, a_2, \ldots, a_k$ bywa też oznaczany symbolem $(a_1, a_2, \ldots, a_k)$.

Przykład 8.20. Z przykładu 8.17, $D_{56} = \{1, 56; 2, 28; 4, 14; 7, 8\}$. Analogicznie można obliczyć, że $D_{48} = \{1, 48; 2, 24; 3, 16; 2, 12; 6, 8\}$. Wobec tego $D(48, 56) = \{1, 2, 4, 8\}$, czyli wspólnymi dzielnikami liczb 48 i 56 są jedynie liczby: 1, 2, 4 i 8. Stąd $\mathrm{NWD}(48, 56) = 8$. Zauważmy jeszcze, że $D_0 = \mathbb{N}$, więc **nie istnieje** $\mathrm{NWD}(0, 0, \ldots, 0)$.

Ćwiczenie 8.21. Wprost z definicji wyznacz największy wspólny dzielnik liczb 56 i 96.

Stwierdzenie 8.22. *Jeżeli wśród liczb całkowitych* $a_1, a_2, \ldots, a_k$ *jest liczba różna od* 0*, to istnieje* $\mathrm{NWD}(a_1, a_2, \ldots, a_k)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Z założenia $a_i \neq 0$ dla pewnego $i = 1, 2, \ldots, k$. Z przykładu 8.2 mamy, że $1 \in D(a_1, ..., a_k)$. Jeżeli $d \in D(a_1, ..., a_k)$, to d jest liczbą naturalną oraz $d \mid a_i$. Zatem ze stwierdzenia 8.8, $d \mid (-a_i)$. Ponadto $a_i \neq 0$, więc $|a_i|$ jest liczbą naturalną i ze stwierdzenia 8.12, $d \leqslant |a_i|$. Zatem na mocy zasady maksimum w zbiorze $D(a_1, ..., a_k)$ istnieje liczba największa, czyli istnieje $\mathrm{NWD}(a_1, a_2, \ldots, a_k)$. □

Następne stwierdzenie grupuje podstawowe własności największego wspólnego dzielnika.

Stwierdzenie 8.23. *Niech $a_1, a_2, \ldots, a_k$ będą liczbami całkowitymi, z których co najmniej jedna jest różna od 0 i niech $a \in \mathbb{Z}$. Wówczas:*

(i) $\mathrm{NWD}(a_1, ..., a_k) = \mathrm{NWD}(|a_1|, ..., |a_k|)$,

(ii) $\mathrm{NWD}(a_1, ..., a_k, 0) = \mathrm{NWD}(a_1, ..., a_k)$,

(iii) jeżeli d jest wspólnym naturalnym dzielnikiem liczb $a_1, ..., a_k$, to $\mathrm{NWD}(d, a_1, ..., a_k) = d$,

(iv) $\mathrm{NWD}(d, 0, 0, \ldots, 0) = d$ *dla każdego naturalnego d,*

(v) $\mathrm{NWD}(a, a_1, ..., a_k) = \mathrm{NWD}(a, a_1 - q_1 a, ..., a_k - q_k a)$ *dla dowolnych $q_1, q_2, ..., q_k \in \mathbb{Z}$.*

Dowód. (i). Ze stwierdzenia 8.8 zbiory $D(a_1, ..., a_k)$ i $D(|a_1|, ..., |a_k|)$ są równe, więc ich największe elementy też są równe, czyli $\mathrm{NWD}(a_1, ..., a_k)$ jest równe $\mathrm{NWD}(|a_1|, ..., |a_k|)$.

(ii). Ze stwierdzenia 8.8, zbiory $D(a_1, ..., a_k, 0)$ i $D(a_1, ..., a_k)$ są równe, więc ich największe elementy też są równe. Wobec tego $\mathrm{NWD}(a_1, ..., a_k, 0) = \mathrm{NWD}(a_1, ..., a_k)$.

(iii). Jeżeli $n \in D(d, a_1, ..., a_k)$, to $n \in \mathbb{N}$ i $n \mid d$, skąd na mocy stwierdzenia 8.12, $n \leqslant d$. Ponadto $d \in D(d, a_1, ..., a_k)$, bo $d \mid d$, $d \in \mathbb{N}$ i z założenia $d \mid a_i$ dla każdego $i = 1, 2, \ldots, k$. Zatem d jest największym elementem zbioru $D(d, a_1, ..., a_k)$, czyli $\mathrm{NWD}(d, a_1, ..., a_k) = d$.

(iv). Ponieważ $d \mid 0$, więc teza wynika od razu z (iii).

(v). Ze stwierdzenia 8.8 łatwo wyprowadzamy, że $D(a, a_1, ..., a_k) = D(a, a_1 - q_1 a, ..., a_k - q_k a)$. Zatem największe elementy tych zbiorów też są równe: $\mathrm{NWD}(a, a_1, ..., a_k) = \mathrm{NWD}(a, a_1 - q_1 \cdot a, ..., a_k - q_k \cdot a)$. □

Na uzyskanych w ten sposób własnościach opiera się następujący

algorytm wyznaczania największego wspólnego dzielnika liczb naturalnych:

ALGORYTM EUKLIDESA. Niech dany będzie niepusty, skończony zbiór A_1 liczb naturalnych. Wyznaczamy najpierw najmniejszą liczbę a_1 tego zbioru. Jeżeli a_1 dzieli wszystkie liczby naszego zbioru, to ich największy wspólny dzielnik jest równy a_1 i algorytm jest zakończony. W przeciwnym przypadku wyznaczamy reszty z dzielenia pozostałych liczb zbioru A_1 przez a_1. Następnie wykreślamy wszystkie zerowe reszty i tworzymy nowy zbiór A_2 złożony z a_1 i z wszystkich nie wykreślonych reszt. Wówczas największy wspólny dzielnik liczb ze zbioru A_1 jest równy największemu wspólnemu dzielnikowi liczb ze zbioru A_2. Następnie stosujemy nasz algorytm do zbioru A_2. Jeżeli a_2 jest najmniejszą liczbą ze zbioru A_2, to oczywiście $a_1 > a_2$. Wynika stąd, że po skończonej liczbie kroków nasz algorytm musi się zakończyć i doprowadzi nas do obliczenia największego wspólnego dzielnika liczb ze zbioru A_1.

Przykład 8.24. $\mathrm{NWD}(-42,-58,72) = \mathrm{NWD}(42,58,72) = \mathrm{NWD}(42,58-42,72-42) = \mathrm{NWD}(42,16,30) = \mathrm{NWD}(16,30,42) = \mathrm{NWD}(16,30-16,42-2\cdot 16) = \mathrm{NWD}(16,14,10) = \mathrm{NWD}(10,14,16)$. $\mathrm{NWD}(10,14,16) = \mathrm{NWD}(10,14-10,16-10) = \mathrm{NWD}(10,4,6) = \mathrm{NWD}(4,6,10) = \mathrm{NWD}(4,6-4,10-2\cdot 4) = \mathrm{NWD}(4,2,2) = \mathrm{NWD}(2,2,4) = 2$, bo 2 jest wspólnym dzielnikiem liczb 2 i 4. Zatem ostatecznie $\mathrm{NWD}(-42,-58,72) = 2$.

Przykład 8.25. Obliczymy przy pomocy algorytmu Euklidesa $\mathrm{NWD}(952,276)$. Mamy, że $\mathrm{NWD}(952,276) = \mathrm{NWD}(276,952) = \mathrm{NWD}(276,124) = \mathrm{NWD}(124,276) = \mathrm{NWD}(124,28)$. Zatem mamy stąd, że $\mathrm{NWD}(952,276) = \mathrm{NWD}(28,124) = \mathrm{NWD}(28,12)$, czyli $\mathrm{NWD}(952,276) = \mathrm{NWD}(12,4) = \mathrm{NWD}(4,12) = 4$, bo $4 \mid 12$.

Ćwiczenie 8.26. Stosując algorytm Euklidesa wyznacz liczby: $\mathrm{NWD}(377,987)$ oraz $\mathrm{NWD}(60,75,135)$.

Uwaga 8.27. Zauważmy, że stosując algorytm Euklidesa do liczb naturalnych a i b takich, że $b \nmid a$ uzyskamy dla pewnego $s \in \mathbb{N}$ malejący

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

ciąg liczb naturalnych $b > r_1 > \ldots > r_s$ oraz ciąg pewnych liczb całkowitych $q_0, q_1, \ldots, q_s$ taki, że zachodzą następujące równości:

$$\begin{cases} a & = & q_0 b & + & r_1 \\ b & = & q_1 r_1 & + & r_2 \\ r_1 & = & q_2 r_2 & + & r_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{s-2} & = & q_{s-1} r_{s-1} & + & r_s \\ r_{s-1} & = & q_s r_s & & \end{cases},$$

przy czym $r_s = \mathrm{NWD}(a, b)$. Pierwszy z tych wzorów daje $r_1 = a \cdot 1 + b \cdot (-q_0)$, wobec czego drugi daje $r_2 = b - (a - bq_0)q_1 = a(-q_1) + b(1 + q_0 q_1)$. W podobny sposób z trzeciego wzoru dostaniemy, że $r_3 = ax_3 + by_3$ dla pewnych $x_3, y_3 \in \mathbb{Z}$, itd., aż wreszcie $\mathrm{NWD}(a, b) = r_s = ax_s + by_s$ dla pewnych $x_s, y_s \in \mathbb{Z}$. Wynika stąd, że dzięki algorytmowi Euklidesa potrafimy efektywnie znajdować liczby całkowite x i y takie, że $ax + by = \mathrm{NWD}(a, b)$. Więcej na ten temat piszemy w podrozdziale 2 rozdziału 16. Natomiast zastosowanie algorytmu Euklidesa do przedstawiania liczb wymiernych w postaci ułamka łańcuchowego omawiamy w podrozdziale 2 rozdziału 18.

Twierdzenie 8.28. *Niech $n \in \mathbb{N}$ i $n \geqslant 2$ oraz niech $a_1, a_2, \ldots, a_n$ będą liczbami całkowitymi i co najmniej jedna z nich jest różna od zera. Wtedy istnieją liczby całkowite $x_1, x_2, \ldots, x_n$ takie, że*

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = \mathrm{NWD}(a_1, a_2, \ldots, a_n).$$

Dowód. Oznaczmy przez A zbiór wszystkich liczb postaci $a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$ dla $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. Zauważmy, że podstawiając $x_i = \pm 1$ oraz $x_j = 0$ dla $j \neq i$ uzyskujemy, że $\pm a_i \in A$ dla każdego $i = 1, 2, \ldots, n$. Ponadto pewna z liczb $a_1, a_2, \ldots, a_n$ jest różna od zera, więc $A \cap \mathbb{N} \neq \emptyset$. Z zasady minimum wynika zatem, że w zbiorze $A \cap \mathbb{N}$ istnieje liczba najmniejsza d, przy czym $d = a_1 u_1 + a_2 u_2 + \ldots + a_n u_n$ dla pewnych $u_1, u_2, \ldots, u_n \in \mathbb{Z}$. Weźmy dowolne $a \in A$. Wtedy $a = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$ dla pewnych $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ oraz z twierdzenia o dzieleniu z resztą $a = qd + r$ dla pewnych $q, r \in \mathbb{Z}$ takich, że $0 \leqslant r < d$. Stąd $r = a_1(x_1 - qu_1) + a_2(x_2 - qu_2) + \ldots + a_n(x_n - qu_n) \in A$. Zatem z

minimalności d, $r \notin \mathbb{N}$, czyli $r = 0$. Wobec tego $d \mid a$ dla każdego $a \in A$. W szczególności d jest wspólnym dzielnikiem liczb $a_1, a_2, \ldots, a_n$, więc $d \leqslant \mathrm{NWD}(a_1, a_2, \ldots, a_n) = D$. Ponadto dla każdego $i = 1, 2, \ldots, n$, $a_i = Db_i$ dla pewnego $b_i \in \mathbb{Z}$, więc $d = D(u_1b_1 + u_2b_2 + \ldots + u_nb_n)$, skąd $D \mid d$. Ponieważ $d, D \in \mathbb{N}$, więc na mocy stwierdzenia 8.12, $D \leqslant d$. Dodatkowo jest też $d \leqslant D$, więc $d = D$, czyli $a_1u_1 + a_2u_2 + \ldots + a_nu_n = \mathrm{NWD}(a_1, a_2, \ldots, a_n)$. □

Definicja 8.29. Powiemy, że liczby całkowite $a_1, a_2, ..., a_k$ są **względnie pierwsze**, jeżeli $\mathrm{NWD}(a_1, a_2, ..., a_k) = 1$.

Twierdzenie 8.30. (zasadnicze twierdzenie arytmetyki). *Niech a i b będą liczbami całkowitymi względnie pierwszymi. Wówczas dla dowolnej liczby całkowitej c z tego, że $a \mid b \cdot c$ wynika $a \mid c$.*

Dowód. Z twierdzenia 8.28 istnieją liczby całkowite x i y takie, że $a \cdot x + b \cdot y = 1$. Zatem $c = acx + bcy$, ale $a \mid b \cdot c$, więc z przykładu 8.2 i ze stwierdzenia 8.8 mamy, że $a \mid (acx + bcy)$, czyli $a \mid c$. □

Uwaga 8.31. Odnotujmy, że czasem w literaturze (na przykład w [22]) zasadniczym twierdzeniem arytmetyki nazywane jest twierdzenie 9.18 o jednoznaczności rozkładu.

Twierdzenie 8.32. *Jeżeli liczby całkowite $a_1, a_2, ..., a_k$ podzielimy przez ich największy wspólny dzielnik d, to otrzymamy liczby względnie pierwsze.*

Dowód. Istnieją liczby całkowite $b_1, ..., b_k$ takie, że $a_i = d \cdot b_i$ dla $i = 1, ..., k$. Niech $t = \mathrm{NWD}(b_1, ..., b_k)$. Wtedy istnieją liczby całkowite $c_1, ..., c_k$ takie, że $b_i = t \cdot c_i$ dla $i = 1, ..., k$. Zatem $a = (dt)c_i$ dla $i = 1, ..., k$. Stąd $d \cdot t \in D(a_1, ..., a_k)$, więc $d \cdot t \leqslant d$, czyli $t = 1$. Zatem liczby $b_1, ..., b_k$ są względnie pierwsze. □

Stwierdzenie 8.33. *Każdą liczbę wymierną można jednoznacznie zapisać w postaci $\frac{a}{b}$, gdzie $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ są takie, że* $\mathrm{NWD}(a, b) = 1$.

Dowód. Weźmy dowolną liczbę wymierną q. Z wniosku 3.19, $q = \frac{x}{y}$ dla pewnych $x \in \mathbb{Z}$ i $y \in \mathbb{N}$. Niech $d = \mathrm{NWD}(x, y)$. Wówczas na mocy

twierdzenia 8.32, $x = ad$ i $y = bd$ dla pewnych $a \in \mathbb{Z}$, $b \in \mathbb{N}$ takich, że $\mathrm{NWD}(a, b) = 1$. Stąd $q = \frac{ad}{bd} = \frac{a}{b}$. Niech teraz $r \in \mathbb{Z}$ i $s \in \mathbb{N}$ będą takie, że $q = \frac{r}{s}$ oraz $\mathrm{NWD}(r, s) = 1$. Wtedy $\frac{a}{b} = \frac{r}{s}$, skąd $as = br$. Zatem $b \mid as$ i $\mathrm{NWD}(b, a) = 1$, więc z zasadniczego twierdzenia arytmetyki $b \mid s$. Analogicznie pokazujemy, że $s \mid b$, ale $b, s \in \mathbb{N}$, więc $b \leqslant s$ i $s \leqslant b$, skąd $b = s$. Wobec tego $as = sr$ i po skróceniu przez s, $a = r$. □

8.4 Najmniejsza wspólna wielokrotność

Niech $a_1, a_2, ..., a_k$ będą niezerowymi liczbami całkowitymi. Wówczas liczbę całkowitą podzielną przez wszystkie te liczby nazywamy ich **wspólną wielokrotnością**. Zbiór wszystkich naturalnych wspólnych wielokrotności takich liczb będziemy oznaczali przez $W(a_1, ..., a_k)$. Ponieważ liczby $a_1 \cdot ... \cdot a_k$ oraz $-a_1 \cdot ... \cdot a_k$ są wspólnymi niezerowymi wielokrotnościami liczb $a_1, ..., a_k$, więc zbiór $W(a_1, ..., a_k)$ jest niepusty. Zatem z zasady minimum istnieje w nim liczba najmniejsza. Nazywamy ją **najmniejszą wspólną wielokrotnością** liczb $a_1, ..., a_k$ i oznaczamy przez $\mathrm{NWW}(a_1, \ldots, a_k)$.

Przykład 8.34. Zauważmy, że naturalnymi wielokrotnościami liczby 4 są 4, 8, 12, 16, 20, 24, ..., zaś naturalnymi wielokrotnościami liczby 6 są 6, 12, 18, 24, ... Stąd $W(4, 6) = \{12, 24, \ldots\}$, więc $\mathrm{NWW}(4, 6) = 12$.

Ćwiczenie 8.35. Wprost z definicji najmniejszej wspólnej wielokrotności wyznacz $\mathrm{NWW}(6, 10, 15)$.

Twierdzenie 8.36. *Każda wspólna wielokrotność niezerowych liczb całkowitych $a_1, ..., a_k$ jest podzielna przez ich najmniejszą wspólną wielokrotność. W szczególności liczba całkowita a jest podzielna przez każdą z liczb $a_1, \ldots, a_k$ wtedy i tylko wtedy, gdy a jest podzielna przez* $\mathrm{NWW}(a_1, \ldots, a_k)$.

Dowód. Niech $m = \mathrm{NWW}(a_1, ..., a_k)$ i niech M będzie wspólną wielokrotnością liczb $a_1, ..., a_k$. Wtedy $a_i \mid M$ oraz $a_i \mid m$ dla $i = 1, ..., k$. Ponadto z twierdzenia o dzieleniu z resztą istnieją liczby całkowite q, r

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

takie, że $M = q \cdot m + r$ oraz $0 \leqslant r < m$. Wtedy ze stwierdzenia 8.8 mamy, że $a_i \mid r$ dla $i = 1, ..., k$. Zatem r nie może być liczbą naturalną, bo inaczej $r \in W(a_1, ..., a_k)$ oraz r jest mniejsze od najmniejszej liczby tego zbioru, którą jest m. Stąd $r = 0$ i $m \mid M$.

Załóżmy, że $\mathrm{NWW}(a_1, \ldots, a_k)$ dzieli liczbę całkowitą a. Wprost z definicji mamy, że $a_i \mid \mathrm{NWW}(a_1, \ldots, a_k)$, więc ze stwierdzenia 8.8, $a_i \mid a$ dla każdego $i = 1, \ldots, k$. □

Twierdzenie 8.37. *Dla dowolnych niezerowych liczb całkowitych* $a_1, \ldots, a_n, a_{n+1}$ *zachodzi wzór:*

$$\mathrm{NWW}(a_1, \ldots, a_n, a_{n+1}) = \mathrm{NWW}(\mathrm{NWW}(a_1, \ldots, a_n), a_{n+1}). \quad (8.5)$$

Dowód. Niech $\mathrm{NWW}(a_1, \ldots, a_n, a_{n+1}) = M$ i $\mathrm{NWW}(a_1, \ldots, a_n) = m$. Wtedy $a_i | M$ dla $i = 1, \ldots, n$, więc z twierdzenia 8.36, $m | M$. Mamy też $a_{n+1} | M$, więc z twierdzenia 8.36, $\mathrm{NWW}(m, a_{n+1}) | M$. Ponadto $m | \mathrm{NWW}(m, a_{n+1})$ i $a_{n+1} | \mathrm{NWW}(m, a_{n+1})$ oraz $a_i | m$ dla $i = 1, \ldots, n$, więc ze stwierdzenia 8.8, $a_i | \mathrm{NWW}(m, a_{n+1})$ dla $i = 1, \ldots, n, n+1$. Stąd na mocy twierdzenia 8.36, $M | \mathrm{NWW}(m, a_{n+1})$, ale $M, \mathrm{NWW}(m, a_{n+1})$ są liczbami naturalnymi oraz $\mathrm{NWW}(m, a_{n+1}) | M$ i $M | \mathrm{NWW}(m, a_{n+1})$, więc ze stwierdzenia 8.8, $M = \mathrm{NWW}(m, a_{n+1})$. □

Ćwiczenie 8.38. Niech dla liczb naturalnych $m, n > 1$ dane będą niezerowe liczby całkowite $a_1, \ldots, a_n, b_1, \ldots, b_m$. Stosując ideę dowodu twierdzenia 8.37 udowodnij, że wówczas zachodzi wzór:

$$\mathrm{NWW}(a_1, \ldots, a_n, b_1, \ldots, b_m) = \mathrm{NWW}(a, b),$$

gdzie $a = \mathrm{NWW}(a_1, \ldots, a_n)$ i $b = \mathrm{NWW}(b_1, \ldots, b_m)$.

Twierdzenie 8.39. *Największy wspólny dzielnik liczb całkowitych* $a_1, ..., a_k$, *z których co najmniej jedna jest różna od zera, jest podzielny przez każdy ich wspólny dzielnik.*

Dowód. Niech $D = \mathrm{NWD}(a_1, ..., a_k)$ i niech d będzie wspólnym dzielnikiem tych liczb. Z przykładu 8.2 i ze stwierdzenia 8.8 wynika, że bez zmniejszania ogólności możemy zakładać, że d jest liczbą naturalną. Wtedy $D \mid a_i$ oraz $d \mid a_i$, więc a_i jest wspólną wielokrotnością liczb D i d dla $i = 1, ..., k$. Zatem z twierdzenia 8.36 mamy, że

$\mathrm{NWW}(D,d) \mid a_i$ dla $i = 1, ..., k$, skąd $\mathrm{NWW}(D,d) \in D(a_1, ..., a_k)$. Zatem $\mathrm{NWW}(D,d) \leqslant D$. Ponadto $D \mid \mathrm{NWW}(D,d)$, więc ze stwierdzenia 8.12, $D \leqslant \mathrm{NWW}(D,d)$. Stąd $D = \mathrm{NWW}(D,d)$, ale $d \mid \mathrm{NWW}(D,d)$, więc $d \mid D$. □

Ćwiczenie 8.40. Niech dla liczb naturalnych $m, n > 1$ dane będą liczby całkowite $a_1, \ldots, a_n$ nie wszystkie równe 0 i liczby całkowite $b_1 \ldots, b_m$ też nie wszystkie równe 0. Stosując twierdzenie 8.39 udowodnij, że wówczas zachodzi wzór:

$$\mathrm{NWD}(a_1, \ldots, a_n, b_1, \ldots, b_m) = \mathrm{NWD}(a, b),$$

gdzie $a = \mathrm{NWD}(a_1, \ldots, a_n)$ i $b = \mathrm{NWD}(b_1, \ldots, b_m)$.

Twierdzenie 8.41. *Niech $a_1, a_2, \ldots, a_n$ będą liczbami całkowitymi, z których co najmniej jedna jest różna od zera. Wówczas zbiór wszystkich wspólnych dzielników tych liczb jest równy zbiorowi wszystkich naturalnych dzielników ich największego wspólnego dzielnika, czyli zachodzi wzór:*

$$D(a_1, a_2, \ldots, a_n) = D_{NWD(a_1,a_2,\ldots,a_n)}. \tag{8.6}$$

Dowód. Weźmy dowolne $d \in D(a_1, \ldots, a_n)$. Wtedy d jest liczbą naturalną oraz d jest wspólnym dzielnikiem liczb $a_1, \ldots, a_n$. Zatem z twierdzenia 8.39, $d \mid \mathrm{NWD}(a_1, \ldots, a_n)$, czyli $d \in D_{NWD(a_1,\ldots,a_n)}$.

Na odwrót, weźmy dowolne $d \in D_{NWD(a_1,\ldots,a_n)}$. Wtedy d jest liczbą naturalną oraz $d \mid \mathrm{NWD}(a_1, \ldots, a_n)$, więc ze stwierdzenia 8.8, d jest wspólnym dzielnikiem liczb $a_1, \ldots, a_n$, czyli $d \in D(a_1, \ldots, a_n)$. Zatem ostatecznie $D(a_1, \ldots, a_n) = D_{NWD(a_1,\ldots,a_n)}$. □

Przykład 8.42. Wyznaczymy wszystkie wspólne dzielniki liczb 96 i 60. Stosując algorytm Euklidesa otrzymujemy, że $\mathrm{NWD}(60, 96) = \mathrm{NWD}(60, 36) = \mathrm{NWD}(36, 24) = \mathrm{NWD}(24, 12) = 12$. Ponadto $D_{12} = \{1, 2, 3, 4, 6, 12\}$, więc na mocy twierdzenia 8.41 wszystkimi wspólnymi dzielnikami liczb 96 i 60 są liczby: 1, 2, 3, 4, 6, 12.

Ćwiczenie 8.43. Stosując twierdzenie 8.41 wyznacz wszystkie wspólne naturalne dzielniki liczb 120 i 216.

Twierdzenie 8.44. *Dla dowolnych liczb naturalnych a i b zachodzi wzór:*

$$a \cdot b = \mathrm{NWD}(a,b) \cdot \mathrm{NWW}(a,b). \tag{8.7}$$

Dowód. Oznaczmy $d = \mathrm{NWD}(a,b)$ oraz $m = \mathrm{NWW}(a,b)$. Wówczas istnieją liczby naturalne k, l, x, y takie, że $a = dk$, $b = dl$, $m = ax$, $m = by$. Ponadto $kld = al = kb$, więc z twierdzenia 8.36 istnieje naturalne n takie, że $kld = mn$. Stąd $al = nax$ oraz $kb = nby$, więc $l = nx$ i $k = ny$ oraz $a = (dn)y$ i $b = (dn)x$. Zatem $dn \in D(a,b)$, skąd $dn \leqslant d$. Zatem $n = 1$ i $kld = \mathrm{NWW}(a,b)$ oraz otrzymujemy, że $\mathrm{NWD}(a,b) \cdot \mathrm{NWW}(a,b) = d \cdot kld = (kd) \cdot (ld) = ab$. □

Twierdzenie 8.45. *Niech $a_1, a_2, \ldots, a_n$ będą niezerowymi liczbami całkowitymi. Wówczas dla dowolnej liczby naturalnej d zachodzi wzór:*

$$\mathrm{NWW}(d \cdot a_1, d \cdot a_2, \ldots, d \cdot a_n) = d \cdot \mathrm{NWW}(a_1, a_2, \ldots, a_n). \tag{8.8}$$

Dowód. Niech $\mathrm{NWW}(d \cdot a_1, \ldots, d \cdot a_n) = M$ i $\mathrm{NWW}(a_1, \ldots, a_n) = m$. Wtedy $a_i \mid m$ oraz $(d \cdot a_i) \mid M$, skąd istnieje liczba całkowita c_i taka, że $M = d \cdot a_i \cdot c_i$ oraz ze stwierdzenia 8.8 (5), $(d \cdot a_i) \mid (d \cdot m)$ dla $i = 1, \ldots, n$. Zatem z twierdzenia 8.36 mamy, że $M \mid (d \cdot m)$, więc istnieje liczba naturalna t taka, że $d \cdot m = M \cdot t$. Stąd $d \cdot m = d \cdot a_i \cdot c_i \cdot t$, czyli $m = t \cdot a_i \cdot c_i$ dla $i = 1, \ldots, n$. Zatem istnieje liczba naturalna s taka, że $m = t \cdot s$ oraz $s = a_i \cdot c_i$ dla $i = 1, \ldots, n$. Zatem z twierdzenia 8.36, $m \mid s$, ale $s \mid m$, więc ze stwierdzenia 8.12, $m = s$, czyli $t = 1$. Stąd $d \cdot m = M$. □

Twierdzenie 8.46. *Niech $a_1, a_2, \ldots, a_n$ będą liczbami całkowitymi, z których co najmniej jedna jest różna od zera. Wtedy dla dowolnej liczby naturalnej d zachodzi wzór:*

$$\mathrm{NWD}(d \cdot a_1, d \cdot a_2, \ldots, d \cdot a_n) = d \cdot \mathrm{NWD}(a_1, a_2, \ldots, a_n). \tag{8.9}$$

Dowód. Oznaczmy $\mathrm{NWD}(d \cdot a_1, \ldots, d \cdot a_n) = K$, $\mathrm{NWD}(a_1, \ldots, a_n) = k$. Wtedy $k \mid a_i$ oraz $K \mid (d \cdot a_i)$, skąd ze stwierdzenia 8.8, $(d \cdot k) \mid (d \cdot a_i)$ oraz $d \cdot a_i = K \cdot c_i$ dla pewnego całkowitego c_i przy każdym $i = 1, \ldots, n$. Stąd z twierdzenia 8.39, $(d \cdot k) \mid K$, więc istnieje liczba naturalna t taka, że $K = d \cdot k \cdot t$. Zatem $d \cdot a_i = d \cdot k \cdot t \cdot c_i$, skąd $a_i = k \cdot t \cdot c_i$, czyli $(k \cdot t) \mid a_i$ dla $i = 1, \ldots, n$. Zatem $k \cdot t \leqslant k$, skąd $t = 1$ i $K = d \cdot k$. □

Przykład 8.47. Wzory (8.5) i (8.7) oraz algorytm Euklidesa pozwalają znajdowanie najmniejszej wspólnej wielokrotności dowolnej skończonej liczby niezerowych liczb całkowitych. Obliczymy tą metodą NWW$(6, 8, 15)$.

Ze wzoru (8.5),

$$\mathrm{NWW}(6, 8, 15) = \mathrm{NWW}(\mathrm{NWW}(6, 8), 15).$$

Z (8.7), $\mathrm{NWW}(6, 8) = \frac{6 \cdot 8}{NWD(6,8)}$. Ponadto mamy, że $\mathrm{NWD}(6, 8) = \mathrm{NWD}(6, 8-6) = \mathrm{NWD}(2, 6) = 2$, więc $\mathrm{NWW}(6, 8) = \frac{6 \cdot 8}{2} = 3 \cdot 8 = 24$. Wobec tego $\mathrm{NWW}(6, 8, 15) = \mathrm{NWW}(24, 15) = 3 \cdot \mathrm{NWW}(8, 5)$ na mocy wzoru (8.8). Ze wzoru (8.7) $\mathrm{NWW}(8, 5) = \frac{8 \cdot 5}{NWD(8,5)}$, ale $\mathrm{NWD}(8, 5) = \mathrm{NWD}(5, 8 - 5) = \mathrm{NWD}(3, 5) = \mathrm{NWD}(3, 2) = \mathrm{NWD}(2, 1) = 1$, więc $\mathrm{NWW}(8, 5) = 40$ i $\mathrm{NWW}(8, 9, 15) = 120$. Z twierdzenia 8.36 mamy dodatkowo, że liczba całkowita a jest podzielna przez każdą z liczb: 6, 8, 15 wtedy i tylko wtedy, gdy $120 \mid a$, a zatem, gdy $a = 120t$ dla $t \in \mathbb{Z}$. Stąd jeśli liczby 6, 8, 15 są dzielnikami liczby całkowitej a, to każdy dzielnik liczby 120 jest też dzielnikiem a. Ponadto

$$D_{120} = \{1, 120; 2, 60; 3, 40; 4, 30; 5, 24; 6, 20, 8, 15; 10, 12\},$$

więc jeśli 6, 8 i 15 są dzielnikami liczby całkowitej a, to liczby: 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60 i 120 też są dzielnikami liczby a.

Ćwiczenie 8.48. Metodą podaną w przykładzie 8.47 wyznacz najmniejszą wspólną wielokrotność liczb: 30, 42, 70 i 105. Opisz wszystkie liczby całkowite a podzielne przez każdą z liczb 30, 42, 70 i 105.

Stwierdzenie 8.49. *Jeśli liczba całkowita a jest względnie pierwsza z każdą z liczb całkowitych $a_1, \ldots, a_n$, to liczby a i $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ też są względnie pierwsze.*

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista. Niech $\mathrm{NWD}(a, a_1) = \mathrm{NWD}(a, a_2) = 1$ i $d = \mathrm{NWD}(a, a_1 a_2)$. Wtedy $d \in \mathbb{N}$, $d \mid a$ i $d \mid a_1 a_2$. Ponadto $\mathrm{NWD}(d, a_1)$ jest wspólnym dzielnikiem liczb względnie pierwszych a i a_1, więc $\mathrm{NWD}(d, a_1) = 1$

i z zasadniczego twierdzenia arytmetyki, $d \mid a_2$. Zatem d jest wspólnym dzielnikiem liczb względnie pierwszych a i a_2, skąd $d = 1$, czyli $\mathrm{NWD}(a, a_1a_2) = 1$ i teza zachodzi dla $n = 2$.

Załóżmy, że teza zachodzi dla pewnej liczby naturalnej n i weźmy liczby całkowite $a, a_1, \ldots, a_n, a_{n+1}$ takie, że $\mathrm{NWD}(a, a_i) = 1$ dla $i = 1, \ldots, n, n+1$. Wtedy z założenia indukcyjnego $\mathrm{NWD}(a, a_1 \cdot \ldots \cdot a_n) = 1$, ale $\mathrm{NWD}(a, a_{n+1}) = 1$, więc z kroku dla $n = 2$:
$\mathrm{NWD}(a, (a_1 \cdot \ldots \cdot a_n) \cdot a_{n+1}) = 1$, czyli teza zachodzi dla liczby $n+1$. □

Twierdzenie 8.50. *Jeżeli każde dwie liczby spośród liczb naturalnych $a_1, a_2, \ldots, a_n$ (gdzie $n \geqslant 2$) są względnie pierwsze, to*

$$\mathrm{NWW}(a_1, a_2, \ldots, a_n) = a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

Dowód. Zastosujemy indukcję względem $n \geqslant 2$. Dla $n = 2$ teza wynika od razu z twierdzenia 3.30. Załóżmy, że teza zachodzi dla pewnego naturalnego $n \neq 2$ i niech każde dwie liczby spośród liczb naturalnych $a_1, a_2, \ldots, a_n, a_{n+1}$ będą względnie pierwsze. Wtedy z założenia indukcyjnego $\mathrm{NWW}(a_1, a_2, \ldots, a_n) = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, więc na mocy twierdzenia 8.37, $\mathrm{NWW}(a_1, a_2, \ldots, a_n, a_{n+1}) = \mathrm{NWW}(a_1 \cdot a_2 \cdot \ldots \cdot a_n, a_{n+1})$. Ponadto ze stwierdzenia 8.49 liczby $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ i a_{n+1} są względnie pierwsze, więc na mocy kroku dla $n = 2$, $\mathrm{NWW}(a_1 \cdot a_2 \cdot \ldots \cdot a_n, a_{n+1}) = a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}$, czyli $\mathrm{NWW}(a_1, a_2, \ldots, a_n, a_{n+1}) = a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}$, a zatem teza zachodzi dla liczby $n + 1$. □

Z Twierdzeń 8.36 i 8.50 wynika od razu następujący

Wniosek 8.51. *Niech każde dwie liczby spośród liczb naturalnych $a_1, a_2, \ldots, a_n$ (gdzie $n \geqslant 2$) będą względnie pierwsze. Wówczas liczba całkowita a jest wspólną wielokrotnością tych liczb wtedy i tylko wtedy, gdy a jest podzielna przez iloczyn tych liczb.*

Twierdzenie 8.52. *Dla dowolnych liczb naturalnych a, b, n:*

$$a^n \mid b^n \iff a \mid b.$$

Dowód. Jeżeli $a \mid b$, to istnieje $t \in \mathbb{Z}$ takie, że $b = a \cdot t$, skąd $b^n = a^n \cdot t^n$, ale $t^n \in \mathbb{Z}$, więc $a^n \mid b^n$. Na odwrót, załóżmy, że $a^n \mid b^n$.

Niech $d = \mathrm{NWD}(a, b)$. Wtedy z twierdzenia 8.32 istnieją względnie pierwsze liczby naturalne x i y takie, że $a = d \cdot x$ oraz $b = d \cdot y$. Zatem $d^n \cdot x^n \mid d^n \cdot y^n$, skąd ze stwierdzenia 8.8, $x^n \mid y^n$, więc też $x \mid y^n$. Ponadto ze stwierdzenia 8.49 mamy, że $\mathrm{NWD}(x, y^n) = 1$, więc $x = 1$. Zatem $a = d$, skąd $a \mid b$. □

Twierdzenie 8.53. *Pierwiastek n-tego stopnia z liczby naturalnej a jest liczbą wymierną wtedy i tylko wtedy, gdy liczba a jest n-tą potęgą pewnej liczby naturalnej.*

Dowód. Implikacja $\Leftarrow$ jest oczywista. Na odwrót, niech n-tego stopnia pierwiastek z liczby naturalnej a będzie liczbą wymierną. Wtedy istnieją liczby naturalne x i y takie, że $a = \frac{x^n}{y^n}$, skąd $a \cdot y^n = x^n$. Zatem $y^n \mid x^n$ i z twierdzenia 8.52, $y \mid x$, czyli $k = \frac{x}{y}$ jest liczbą naturalną oraz $a = k^n$. □

Przykład 8.54. Wyznaczymy liczbę naturalną k taką, że $k < \sqrt{311} < k+1$. Ponieważ $17^2 = 289$ i $18^2 = 324$, więc $17^2 < 311 < 18^2$, skąd $17 < \sqrt{311} < 18$ i na mocy twierdzenia 8.53 liczba $\sqrt{311}$ jest niewymierna.

Ćwiczenie 8.55. W oparciu o twierdzenie 8.53 wykaż niewymierność następujących liczb rzeczywistych: $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{145}$, $\sqrt{288}$, $\sqrt[3]{5}$, $\sqrt[3]{242}$.

Ćwiczenie 8.56. Udowodnij, że jeżeli k jest liczbą naturalną i $343 < k < 512$, to $\sqrt[3]{k}$ nie jest liczbą wymierną.

Przykład 8.57. Znajdziemy wszystkie liczby naturalne n takie, że liczba $3^{n-1}+5^{n-1}$ dzieli liczbę 3^n+5^n. Jeśli $n \in \mathbb{N}$, to liczba $3^{n-1}+5^{n-1}$ dzieli liczbę 3^n+5^n wtedy i tylko wtedy, gdy $k \cdot (3^{n-1}+5^{n-1}) = 3^n+5^n$ dla pewnego $k \in \mathbb{N}$. Zauważmy, że $3 \cdot (3^{n-1}+5^{n-1}) = 3^n+3 \cdot 5^{n-1} < 3^n+5^n$, więc $3 < k$. Ponadto $5 \cdot (3^{n-1}+5^{n-1}) = 5 \cdot 3^{n-1}+5^n > 3^n+5^n$, więc $k < 5$. Wobec tego $3 < k < 5$, czyli $k = 4$ oraz $4 \cdot (3^{n-1}+5^{n-1}) = 3^n+5^n$. Stąd $3^{n-1} = 5^{n-1}$, a zatem $n - 1 = 0$ i $n = 1$, bo $3^m < 5^m$ dla każdego $m \in \mathbb{N}$. Ponadto $3^0 + 5^0 = 2$ jest dzielnikiem liczby $8 = 3^1 + 5^1$. Zatem $3^{n-1} + 5^{n-1}$ dzieli liczbę $3^n + 5^n$ wtedy i tylko wtedy, gdy $n = 1$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Przykład 8.58. Niech m, n będą względnie pierwszymi liczbami naturalnymi. Zbadamy jakie wartości może przyjąć największy wspólny dzielnik liczb $m+m$ i m^2-mn+n^2. Ponieważ m^2-mn+ $+n^2 = (m+n)^2-3mn$, więc na mocy stwierdzenia 8.23 mamy, że $\mathrm{NWD}(m+n, m^2-mn+n^2) = \mathrm{NWD}(m+n, 3mn)$. Ponadto ze stwierdzenia 8.23 uzyskujemy, że $\mathrm{NWD}(m+n, m) = \mathrm{NWD}(m, n) = 1$ i $\mathrm{NWD}(m+n, n) = \mathrm{NWD}(m, n) = 1$, więc na mocy stwierdzenia 8.49 jest $\mathrm{NWD}(m+n, mn) = 1$. Dalej, jeśli $3 \nmid m+n$, to $\mathrm{NWD}(3, m+n) = 1$ i wtedy na mocy stwierdzenia 8.49 mamy, że $\mathrm{NWD}(m+n, 3mn) = 1$. Jeśli $3 \mid m+n$, to $m+n = 3t$ dla pewnego $t \in \mathbb{N}$, przy czym $\mathrm{NWD}(t, mn) = 1$, gdyż $\mathrm{NWD}(m+n, mn) = 1$ i $m+n = 3t$, więc na mocy twierdzenia 8.46 uzyskujemy, że $\mathrm{NWD}(m+n, 3mn) =$ $= 3 \cdot \mathrm{NWD}(t, mn) = 3 \cdot 1 = 3$. Podsumowując uzyskaliśmy, że jeśli $3 \mid m+n$, to $\mathrm{NWD}(m+n, m^2-mn+n^2) = 3$, a jeśli $3 \nmid m+n$, to $\mathrm{NWD}(m+n, m^2-mn+n^2) = 1$.

Przykład 8.59. Niech $a_n = 100+n^2$ dla liczby naturalnej n. Zbadamy jaką największą wartość może przyjąć największy wspólny dzielnik dwóch kolejnych wyrazów ciągu (a_n). Zauważmy, że $a_{n+1} - a_n =$ $= 2n+1$, więc jeśli $d_n = \mathrm{NWD}(a_{n+1}, a_n)$, to $d_n \mid n^2+100$ i $d_n \mid 2n+1$. Ale $4 \cdot (n^2+100) = (2n-1)(2n+1)+401$, więc $d_n \mid 401$, skąd $d_n \leqslant 401$. Ponadto $a_{201} - a_{200} = 2 \cdot 200 + 1 = 401$ i $a_{200} = 200^2 + 100 = 100 \cdot 401$, więc $401 \mid a_{200}$ i $401 \mid a_{201}$, skąd $d_{200} \geqslant 401$ i ostatecznie $d_{200} = 401$. Wobec tego największą wartością $\mathrm{NWD}(a_{n+1}, a_n)$ jest liczba 401.

Rozdział 9

Liczby pierwsze

Nie wiadomo, kiedy zdefiniowano pojęcie liczby pierwszej, jednak sygnałem sugerującym pewną świadomość zróżnicowania tych liczb jest kość Ishango - znalezisko datowane na górny paleolit, na którym znajdują się znaki reprezentujące liczby pierwsze między 10 a 20. Aby znaleźć kolejny znak tej świadomości, trzeba udać się do Mezopotamii i poczekać na drugie tysiąclecie p.n.e. Niektóre tabliczki z tego okresu zawierają rozwiązania pewnych problemów arytmetycznych, których rozwiązanie wymaga dobrej znajomości rozkładu na czynniki pierwsze. Do tego samego tysiąclecia należy również papirus Rhinda, który zawiera pewne rozwinięcia liczb postaci $2/n$ na ułamki łańcuchowe, co sugeruje, że Egipcjanie byli przynajmniej świadomi różnicy między liczbami pierwszymi a złożonymi.

Pierwszym niezaprzeczalnym śladem prawdziwych badań nad liczbami pierwszymi są „Elementy" Euklidesa, napisane między IV a III wiekiem p.n.e., które dają pełny obraz ówczesnej wiedzy matematycznej. Praca ta zawiera kilka fundamentalnych wyników, w tym twierdzenie o nieskończoności zbioru liczb pierwszych. Euklides udowadnia również możliwość rozłożenia dowolnej liczby całkowitej większej od jeden na iloczyn liczb pierwszych. Sito Eratostenesa - prosty algorytm służący do określania, które liczby są pierwsze, pochodzi również ze starożytnej Grecji.

Kolejne stulecia charakteryzowały się pewnym brakiem zaintereso-

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

wania badaniem liczb pierwszych i przez pewien czas nie pojawiały się na ten temat żadne szczególne wyniki. Zainteresowanie nimi odrodziło się w XVII wieku wraz z pracami Pierre'a de Fermata. Udowodnił on, między innymi, że wszystkie liczby pierwsze postaci $4k + 1$ można zapisać jako sumę kwadratów dwóch liczb naturalnych. Przypuszczał również, że wszystkie liczby postaci $2^{2^n} + 1$ (nazywane teraz liczbami Fermata na jego cześć) są pierwsze. Sam Fermat sprawdził swoje przypuszczenie do $n = 4$, ale Euler wykazał, że $2^{2^5} + 1$ jest liczbą złożoną. Do tej pory nie są znane żadne inne liczby Fermata, o których wiadomo, że są pierwsze.

Inne wyniki uzyskał Euler w XVIII wieku: wykazał on, między innymi, rozbieżność nieskończonego szeregu odwrotności wszystkich liczb pierwszych. Badał on również wzór pokazujący związek między liczbami pierwszymi a szeregiem harmonicznym. W korespondencji Eulera z Christianem Goldbachem ten ostatni sformułował także słynną hipotezę Goldbacha, do dziś nieudowodnioną, mówiącą o tym, że każda parzysta liczba naturalna większa od 2 jest sumą dwóch liczb pierwszych.

Od początku XIX wieku uwaga wielu matematyków skierowana była na badanie asymptotycznego rozkładu liczb pierwszych, czyli na badanie zachowania się funkcji zliczającej liczby pierwsze mniejsze lub równe x. Legendre i Gauss niezależnie przypuszczali, że ta funkcja to w przybliżeniu $x/\ln x$, gdzie $\ln x$ oznacza logarytm naturalny z x. W 1859 roku Bernhard Riemann połączył ten problem z badaniem funkcji zeta Riemanna, funkcji zmiennej zespolonej; podejście to doprowadziło do dowodu hipotezy, przeprowadzonego niezależnie przez Hadamarda i de la Vallée Poussina w 1896 roku. Fakt ten jest obecnie znany jako **twierdzenie o liczbach pierwszych**, i jest to kluczowy wynik tak zwanej **Analitycznej teorii liczb**.

Badanie liczb pierwszych było częścią jedynie matematyki teoretycznej aż do lat 70. XX wieku, kiedy opracowano koncepcję kryptosystemu z kluczem publicznym. Pierwszy algorytm tego typu, **RSA**, w rzeczywistości wykorzystuje trudność rozkładu na czynniki dużych liczb, które są iloczynem dwóch liczb pierwszych. Z tego powodu poszukiwanie coraz większych liczb pierwszych nabrało dużego znaczenia.

Wiele ciekawych informacji o liczbach pierwszych, historii ich badania, i problemach z nimi związanymi można znaleźć w książce [36].

9.1 Określenie i podstawowe własności liczb pierwszych

Przez dzielnik liczby naturalnej n będziemy rozumieli od tej pory liczbę naturalną dzielącą n. Przypomnijmy, że D_n oznacza zbiór wszystkich dzielników liczby n.

Definicja 9.1. Liczbę naturalną p nazywamy **liczbą pierwszą**, jeżeli p ma dokładnie dwa dzielniki. Liczbę naturalną $n > 1$, która nie jest pierwsza, nazywamy **liczbą złożoną**. Zbiór wszystkich liczb pierwszych oznaczamy przez $\mathbb{P}$.

Uwaga 9.2. Liczba 1 nie jest ani pierwsza ani złożona, gdyż ze stwierdzenia 8.12 mamy, że $D_1 = \{1\}$, to znaczy liczba 1 posiada dokładnie jeden dzielnik.

Uwaga 9.3. Na mocy przykładu 8.2 każda liczba naturalna $n > 1$ posiada co najmniej dwa różne dzielniki: 1 i n. Wynika stąd, że **liczba naturalna $n > 1$ jest liczbą pierwszą wtedy i tylko wtedy, gdy jedynymi jej dzielnikami są 1 i n.**

Uwaga 9.4. Wobec uwagi 9.3 liczba naturalna $n > 1$ jest liczbą złożoną wtedy i tylko wtedy, gdy n posiada dzielnik d taki, że $1 < d < n$. Zatem, gdy $n = d \cdot k$ dla pewnego naturalnego $k > 1$. Stąd **każda liczba złożona n jest postaci $n = a \cdot b$ dla pewnych liczb naturalnych $a, b > 1$.**

Uwaga 9.5. Liczba 2 jest jedyną parzystą liczbą pierwszą. Rzeczywiście, każda liczba parzysta n jest postaci $n = 2k$ dla pewnego naturalnego k. Jeżeli $k > 1$, to z uwagi 9.4 n jest liczbą złożoną. Natomiast dla $k = 1$ mamy, że $n = 2$, więc z przykładu 8.2 i ze stwierdzenia 8.12 $D_2 = \{1, 2\}$, czyli liczba 2 jest pierwsza. Zatem 2 jest też najmniejszą liczbą pierwszą.

Przykład 9.6. Fakt, że 2 jest jedyną parzystą liczbą pierwszą jest częstym motywem różnych zadań o liczbach pierwszych.

Zilustrujemy to na przykładzie wyznaczenia wszystkich liczb pierwszych p i q takich, że liczby $7p+q$ i $pq+11$ też są pierwsze. Jeśli liczby p i q są nieparzyste, to liczba $pq+11$ jest parzysta i większa od 2, co prowadzi do sprzeczności. Zatem $2 \mid p$ lub $2 \mid q$, skąd na mocy uwagi 9.5 mamy, że $p = 2$ lub $q = 2$.

Niech $p = 2$. Wtedy $q+14, 2q+11 \in \mathbb{P}$. Jeśli $3 \nmid q$, to z twierdzenia o dzieleniu z resztą $q = 3k+1$ lub $q = 3k+2$ dla pewnego $k \in \mathbb{N}_0$. W pierwszym przypadku $q+14 = 3 \cdot (k+5) \notin \mathbb{P}$, a w drugim $2q+11 = 3 \cdot (2k+5) \notin \mathbb{P}$. Zatem $3 \mid q$, skąd $q = 3$ i wtedy $q+14 = 2q+11 = 17 \in \mathbb{P}$.

Niech $q = 2$. Wtedy $7p+2, 2p+11 \in \mathbb{P}$. Jeśli $3 \nmid p$, to z twierdzenia o dzieleniu z resztą $p = 3k+1$ lub $p = 3k+2$ dla pewnego $k \in \mathbb{N}_0$. W pierwszym przypadku $7p+2 = 3 \cdot (7k+3) \notin \mathbb{P}$, a w drugim $2p+11 = 3 \cdot (2k+5) \notin \mathbb{P}$. Zatem $3 \mid p$, skąd $p = 3$ i wtedy $7p+2 = 23 \in \mathbb{P}$ oraz $2p+11 = 17 \in \mathbb{P}$.

Wobec tego ostatecznie $p = 2$ i $q = 3$ lub $p = 3$ i $q = 2$.

Ćwiczenie 9.7. Wyznacz wszystkie liczby pierwsze p i q takie, że $p - 1 = q^2$.

Twierdzenie 9.8. *Każda liczba naturalna $n > 1$ posiada co najmniej jeden dzielnik będący liczbą pierwszą.*

Dowód. Dla liczby naturalnej $n > 1$ oznaczmy przez A zbiór wszystkich jej dzielników większych od 1. Wtedy zbiór A jest niepusty, bo z przykładu 8.2, $n \in A$. Zatem z zasady minimum w zbiorze A istnieje liczba najmniejsza p. Wtedy $p > 1$ oraz $p \mid n$. Jeżeli d jest dzielnikiem p i $d > 1$, to ze stwierdzenia 8.8, $d \in A$ oraz ze stwierdzenia 8.12, $d \leqslant p$. Zatem z minimalności p jest $d = p$. Stąd p jest liczbą pierwszą. □

Twierdzenie 9.9. *Zbiór wszystkich liczb pierwszych jest nieskończony.*

Dowód. Załóżmy, że tak nie jest. Wówczas $p_1 = 2, p_2, \ldots, p_n$ są wszystkimi różnymi liczbami pierwszymi. Niech $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Wtedy

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

a jest liczbą naturalną większą od 1, więc z twierdzenia 9.8 istnieje liczba pierwsza p dzieląca a. Ponadto $p_1, p_2, \ldots, p_n$ są wszystkimi liczbami pierwszymi, więc $p = p_i$ dla pewnego $i = 1, 2, \ldots, n$. Zatem $p_i \mid (p_1 \cdot \ldots \cdot p_i \cdot \ldots \cdot p_n + 1)$ oraz oczywiście $p_i \mid (p_1 \cdot \ldots \cdot p_i \cdot \ldots \cdot p_n)$, więc ze stwierdzenia 8.8, $p_i \mid 1$, skąd ze stwierdzenia 8.12, $p_i \leqslant 1$ i mamy sprzeczność. Przypuszczenie, że zbiór wszystkich liczb pierwszych jest skończony doprowadziło nas do sprzeczności. Zatem ten zbiór jest nieskończony. □

Twierdzenie 9.10. *Każda liczba złożona n ma dzielnik pierwszy p taki, że $p^2 \leqslant n$.*

Dowód. Niech n będzie liczbą złożoną. Wtedy z uwagi 9.4 istnieją liczby naturalne a, b takie, że $1 < a \leqslant b$ oraz $n = a \cdot b$. Zatem z twierdzenia 9.8 istnieje liczba pierwsza p dzieląca liczbę a, ale $a \mid n$, więc ze stwierdzenia 8.8, $p \mid n$. Ponadto $p \leqslant a$ ze stwierdzenia 8.12, więc $p^2 \leqslant a^2 \leqslant a \cdot b = n$, czyli $p^2 \leqslant n$. □

Przykład 9.11. Uzasadnimy, że 101 jest liczbą pierwszą. Zauważmy, że $10^2 < 101 < 11^2$. Łatwo zauważyć, że liczbami pierwszymi nie większymi od 10 są jedynie: 2, 3, 5 i 7. Z cech podzielności przez 2, 3 i 5 od razu wynika, że żadna z tych liczb nie dzieli liczby 101. Ponadto, $101 = 14 \cdot 7 + 3$, czyli $[101]_7 = 3$ i $7 \nmid 101$. Wobec tego na mocy twierdzenia 9.10, 101 jest liczbą pierwszą.

9.2 Sito Eratostenesa

Już w starożytności znany był algorytm wyznaczania wszystkich liczb pierwszych zawartych w ciągu $2, 3, \ldots, n$ dla ustalonej liczby naturalnej $n > 1$. Polega on na wykreślaniu z tego ciągu liczb złożonych i nazywa się **sitem Eratostenesa**. Oto ten algorytm:

SITO ERATOSTENESA. Wyznaczamy najpierw największą liczbę naturalną s taką, że $s^2 \leqslant n$. Następnie wypisujemy wszystkie liczby $2, 3, \ldots, n$. Najmniejsza z nich $p_1 = 2$ jest liczbą pierwszą. Wykreślamy teraz wszystkie liczby tego ciągu większe od 2 i podzielne

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

przez 2. Najmniejszą liczbą niewykreśloną i większą od p_1 jest $p_2 = 3$. Liczbę p_2 pozostawiamy, wykreślamy natomiast wszystkie liczby większe od p_2 i podzielne przez p_2. Najmniejszą z liczb niewykreślonych i większą od p_2 jest $p_3 = 5$. Wykreślamy zatem wszystkie liczby większe od p_3 i podzielne przez p_3. Proces kolejnych wykreśleń powtarzamy do chwili, aż dojdziemy do największej niewykreślonej liczby p_k takiej, że $p_k \leqslant s$. Gdy z ciągu wykreślimy liczby większe od p_k i podzielne przez p_k, wówczas wszystkie niewykreślone liczby będą liczbami pierwszymi.

Uzasadnienie poprawności sita Eratostenesa. Zauważmy najpierw, że w tym algorytmie wykreślamy jedynie liczby złożone, a więc nie wykreślimy nigdy liczby pierwszej $p \leqslant n$. Przypuśćmy, że wśród niewykreślonych liczb istnieje liczba złożona a. Wtedy $1 < a \leqslant n$. Wówczas z twierdzenia 4.8 istnieje liczba pierwsza p dzieląca a i taka, że $p^2 \leqslant a$. Stąd $p^2 \leqslant n$, więc z maksymalności s jest, że $p \leqslant s$, ale dla $p \leqslant s$ wykreśliliśmy wszystkie liczby większe od p i podzielne przez p, a więc też wykreśliliśmy liczbę a, więc mamy sprzeczność. □

Przykład 9.12. Zastosujemy sito Eratostenesa do wyznaczenia wszystkich liczb pierwszych $\leqslant 100$. Tutaj $s = 10$, bo $10^2 = 100 < 11^2$.
2, 3, ~~4~~, 5, ~~6~~, 7 ~~8~~ ~~9~~ ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~, 31, ~~32~~, ~~33~~, ~~34~~, ~~35~~, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~, 41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, ~~49~~, ~~50~~, ~~51~~, ~~52~~, 53, ~~54~~, ~~55~~, ~~56~~, ~~57~~, ~~58~~, 59, ~~60~~, 61, ~~62~~, ~~63~~, ~~64~~, ~~65~~, ~~66~~, 67, ~~68~~, ~~69~~, ~~70~~, 71, ~~72~~, 73, ~~74~~, ~~75~~, ~~76~~, ~~77~~, ~~78~~, 79, ~~80~~, ~~81~~, ~~81~~, ~~82~~, 83, ~~84~~, ~~85~~, ~~86~~, ~~87~~, ~~88~~, 89, ~~90~~, ~~91~~, ~~92~~, ~~93~~, ~~94~~, ~~95~~, ~~96~~, 97, ~~98~~, ~~99~~, ~~100~~. Otrzymujemy, że $p_k = 7$.
Wszystkie liczby pierwsze $\leqslant 100$:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

9.3 Rozkładanie liczb naturalnych na czynniki pierwsze

Stwierdzenie 9.13. *Niech p będzie liczbą pierwszą i niech $a \in \mathbb{Z}$. Wówczas:*

$$\mathrm{NWD}(p, a) = 1 \iff p \nmid a. \tag{9.1}$$

Dowód. Z definicji liczby pierwszej mamy, że $D_p = \{1, p\}$. Stąd, jeżeli p nie dzieli a, to $D(p, a) = \{1\}$, więc $\mathrm{NWD}(p, a) = 1$. Jeżeli zaś $p \mid a$, to $D(p, a) = \{1, p\}$, więc wtedy $\mathrm{NWD}(p, a) = p > 1$. Zatem $\mathrm{NWD}(p, a) = 1 \iff p \nmid a$. □

Twierdzenie 9.14. *Jeżeli liczba pierwsza p dzieli iloczyn liczb całkowitych $a_1, a_2, \ldots, a_n$, to $p \mid a_i$ dla pewnego $i = 1, \ldots, n$.*

Dowód. Załóżmy, że tak nie jest dla pewnej liczby pierwszej p. Wtedy istnieje liczba naturalna $n \geqslant 2$ i istnieją liczby całkowite $a_1, a_2, \ldots, a_n$, które nie dzielą się przez p, ale $p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_n)$. Na mocy stwierdzenia 9.13, $\mathrm{NWD}(p, a_i) = 1$ dla $i = 1, \ldots, n$. Zatem ze stwierdzenia 8.49, $\mathrm{NWD}(p, a_1 \cdot a_2 \cdot \ldots \cdot a_n) = 1$, co przeczy temu, że $p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_n)$. □

Uwaga 9.15. Niech $p_1, p_2, \ldots, p_s$ będą różnymi liczbami pierwszymi i niech $\alpha_1, \alpha_2, \ldots, \alpha_s$ będą liczbami naturalnymi. Wówczas jedynymi dzielnikami pierwszymi liczby $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ są liczby: $p_1, p_2, \ldots, p_s$. Rzeczywiście, $p_i \mid a$, gdyż $\alpha_i > 0$ dla $i = 1, \ldots, s$. Jeżeli zaś p jest liczbą pierwszą dzielącą a, to z twierdzenia 9.14, $p \mid p_i$ dla pewnego $i = 1, \ldots, s$, skąd z pierwszości p i p_i, $p = p_i$.

Uwaga 9.16. Niech $p, p_1, \ldots, p_s$ będą różnymi liczbami pierwszymi. Wówczas nie istnieją liczby całkowite nieujemne $\alpha_1, \ldots, \alpha_s$ takie, że $p \mid p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, bo inaczej z twierdzenia 9.14, $p \mid p_i^{\alpha_i}$ dla pewnego $i = 1, \ldots, s$. Stąd z uwagi 9.15 mamy, że $\alpha_i = 0$, więc $p \mid 1$, czyli $p = 1$ i mamy sprzeczność.

Twierdzenie 9.17. *Niech $p_1, p_2, \ldots, p_s$ będą różnymi liczbami pierwszymi i niech $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_s$ będą nieujemnymi liczbami całkowitymi. Wówczas: $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$ wtedy i tylko wtedy, gdy $(\alpha_1, \ldots, \alpha_s) = (\beta_1, \ldots, \beta_s)$.*

Dowód. Załóżmy, że $(\alpha_1, \ldots, \alpha_s) = (\beta_1, \ldots, \beta_s)$. Wtedy $\alpha_i = \beta_i$ dla każdego $i = 1, \ldots, s$, więc $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$. Na odwrót, załóżmy, że $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$. Wystarczy udowodnić, że $\alpha_i = \beta_i$ dla każdego $i = 1, \ldots, s$. Gdyby tak nie było, to dla pewnego $i = 1, \ldots, s$ mielibyśmy $\alpha_i \neq \beta_i$. Bez zmniejszania ogólności możemy zakładać, że $i = 1$ oraz $\alpha_1 > \beta_1$. Wtedy $\alpha_1 - \beta_1$ jest liczbą naturalną i po skróceniu przez $p_1^{\beta_1}$ uzyskamy, że $p_1 \mid p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$, co przeczy uwadze 9.16. □

Twierdzenie 9.18. (o jednoznaczności rozkładu). *Każda liczba naturalna $n > 1$ może być przedstawiona w postaci*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \tag{9.2}$$

gdzie $k, \alpha_1, \ldots, \alpha_k$ są liczbami naturalnymi, zaś $p_1 < p_2 < \ldots < p_k$ są liczbami pierwszymi. Przedstawienie liczby n w postaci (9.2) *jest jednoznaczne, to znaczy jeżeli $n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$, gdzie $l, \beta_1, \ldots, \beta_l$ są liczbami naturalnymi, zaś $q_1 < q_2 < \ldots < q_l$ są liczbami pierwszymi, to $k = l$ oraz $\alpha_i = \beta_i$ i $p_i = q_i$ dla $i = 1, 2, \ldots, k$.*

Dowód. Załóżmy, że istnieją liczby naturalne $n > 1$, których nie można zapisać w postaci (9.2). Wtedy z zasady minimum istnieje wśród nich liczba najmniejsza $n_0 > 1$. Z twierdzenia 9.8 istnieje najmniejsza liczba pierwsza p_1, która dzieli liczbę n_0. Zatem $n_0 = p_1 \cdot n_1$ dla pewnej liczby naturalnej $n_1 < n_0$. Jeśli $n_1 = 1$, to $n_0 = p_1^1$ wbrew założeniu. Zatem $n_1 > 1$, więc z minimalności liczby n_0 istnieją liczby pierwsze $q_1 < p_2 < \ldots < p_s$ oraz istnieją liczby naturalne $\gamma_1, \gamma_2, \ldots, \gamma_s$ takie, że $n_1 = q_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$. Z określenia liczby p_1 wynika, że $p_1 \leqslant q_1$. Jeżeli $p_1 = q_1$, to $n_0 = p_1^{\gamma_1 + 1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$, wbrew założeniu. Jeśli zaś $p_1 < q_1$, to $n_0 = p_1^1 \cdot q_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots p_s^{\gamma_s}$, wbrew założeniu. Zatem każdą liczbę naturalną $n > 1$ można zapisać w postaci (9.2).

Niech teraz przy oznaczeniach naszego twierdzenia

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot \ldots \cdot q_l^{\beta_l}.$$

Wtedy z uwagi 9.15 mamy, że $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_l\}$, więc $k = l$ oraz kolejno: $p_1 = q_1$, $p_2 = q_2$,..., $p_k = q_k$ oraz z twierdzenia 9.17 $\alpha_i = \beta_i$ dla $i = 1, 2, \ldots, k$. □

Przedstawienie liczby naturalnej $n > 1$ w postaci (9.2) nazywamy jej **rozkładem kanonicznym**.

Liczba 1 nie posiada rozkładu kanonicznego, ale dla dowolnych różnych liczb pierwszych $p_1, \ldots, p_s$ mamy, że $1 = p_1^0 \cdot \ldots \cdot p_s^0$.

Przykład 9.19. Stosując szkolny sposób rozkładania liczby naturalnej na czynniki pierwsze uzyskamy:

1176	2		2100	2
588	2		1050	2
294	2		525	3
147	3	i	175	5
49	7		35	5
7	7		7	7
1			1	

Stąd mamy rozkłady kanoniczne liczb 1176 i 2100: $1176 = 2^3 \cdot 3^1 \cdot 7^2$ i $2100 = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^1$.

Stwierdzenie 9.20. *Liczby całkowite $a_1, a_2, \ldots, a_n$, gdzie $n \geqslant 2$, nie są względnie pierwsze wtedy i tylko wtedy, gdy istnieje liczba pierwsza p będąca ich wspólnym dzielnikiem.*

Dowód. Jeżeli istnieje liczba pierwsza p będąca wspólnym dzielnikiem liczb $a_1, \ldots .a_n$, to $\mathrm{NWD}(a_1, \ldots, a_n) \geqslant p > 1$, więc liczby te nie są względnie pierwsze. Na odwrót, załóżmy, że liczby $a_1, \ldots, a_n$ nie są względnie pierwsze. Wtedy $\mathrm{NWD}(a_1, \ldots, a_n) = d > 1$. Zatem z twierdzenia 9.8 istnieje liczba pierwsza p będąca dzielnikiem d, ale wtedy ze stwierdzenia 8.8 liczba p jest wspólnym dzielnikiem liczb $a_1, \ldots, a_n$. □

Z uwagi 9.16 oraz z twierdzeń 9.17 i 9.18 wynika od razu następujące

Stwierdzenie 9.21. *Liczby naturalne $a_1, a_2, \ldots, a_n$ większe od 1 nie są względnie pierwsze wtedy i tylko wtedy, gdy istnieje liczba pierwsza występująca w rozkładzie kanonicznym każdej z tych liczb.*

Z omawianą tematyką ściśle wiąże się słynna **hipoteza ABC**, znana również jako hipoteza Oesterlé-Massera, którą krótko przedstawimy. Pojawiła się ona w wyniku dyskusji Josepha Oesterlé i Davida Massera w 1985 roku. Dotyczy trójek (a, b, c) względnie pierwszych liczb naturalnych (stąd nazwa), takich, że $a + b = c$. Hipoteza ta głosi,

że iloczyn różnych czynników pierwszych liczby $a \cdot b \cdot c$ oznaczany przez $rad(abc)$ jest zwykle niewiele mniejszy niż c. Mówiąc precyzyjniej, dla każdej liczby rzeczywistej $\varepsilon > 0$ istnieje tylko skończenie wiele trójek (a, b, c) względnie pierwszych liczb naturalnych, takich, że $a + b = c$ oraz

$$rad(abc)^{1+\varepsilon} < c.$$

Wykazano, że z prawdziwości hipotezy ABC wynika rozwiązanie wielu słynnych problemów matematycznych. Profesor Dorian Goldfeld stwierdził w [14], że hipoteza ABC jest najważniejszym nierozwiązanym problemem w analizie diofantycznej oraz, że to nie tylko kwestia użyteczności, ale i matematycznego piękna. Zainteresowanych Czytelników odsyłamy do tego artykułu po dodatkowe informacje.

9.4 Postać i liczba dzielników liczby naturalnej

Twierdzenie 9.22. (o postaci dzielników). *Niech $p_1, p_2, \ldots, p_k$ będą różnymi liczbami pierwszymi, zaś $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}_0$. Liczba naturalna d jest dzielnikiem liczby $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ wtedy i tylko wtedy, gdy $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots p_k^{\beta_k}$, gdzie $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, 2, \ldots, k$.*

Dowód. Załóżmy, że $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots p_k^{\beta_k}$, gdzie $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, 2, \ldots, k$. Wtedy $\gamma_i = \alpha_i - \beta_i \in \mathbb{N}_0$ dla $i = 1, \ldots, k$, skąd $m = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k} \in \mathbb{N}$ oraz $d \cdot m = n$, czyli $d \mid n$.

Na odwrót, załóżmy, że liczba naturalna d dzieli n. Wtedy $n = d \cdot m$ dla pewnego $m \in \mathbb{N}$. Jeżeli p jest liczbą pierwszą dzielącą d lub m, to p dzieli n, więc z uwagi 9.16, $p \in \{p_1, \ldots, p_k\}$. Zatem z twierdzenia 9.18 oraz z uwagi 9.16 istnieją $\beta_1, \ldots, \beta_k, \gamma_1, \ldots, \gamma_k \in \mathbb{N}_0$ takie, że $d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$ i $m = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k}$. Stąd $p_1^{\beta_1+\gamma_1} \cdot \ldots \cdot p_k^{\beta_k+\gamma_k} = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Zatem z twierdzenia 9.17, $\beta_i + \gamma_i = \alpha_i$, skąd $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, \ldots, k$. □

Liczbę wszystkich dzielników liczby naturalnej n będziemy oznaczali przez $\tau(n)$.

Stwierdzenie 9.23. (o liczbie dzielników). *Niech $p_1, p_2, \ldots, p_k$ będą różnymi liczbami pierwszymi, zaś $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}_0$. Wówczas*

$$\tau\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right) = (1+\alpha_1) \cdot (1+\alpha_2) \cdot \ldots \cdot (1+\alpha_k). \tag{9.3}$$

Dowód. Z twierdzeń 9.17 i 9.22 wynika od razu, że liczba wszystkich dzielników liczby $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ jest równa liczbie wszystkich ciągów $(\beta_1, \ldots, \beta_k)$ takich, że $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, \ldots, k$, czyli $\tau(n) = (1+\alpha_1) \cdot (1+\alpha_2) \cdot \ldots \cdot (1+\alpha_k)$. □

Przykład 9.24. Obliczymy liczbę dzielników liczby $n = 6^{26} \cdot 10^{90} \cdot 15^{78}$. Mamy, że $6 = 2 \cdot 3$, $10 = 2 \cdot 5$ oraz $15 = 3 \cdot 5$. Zatem $n = 2^{116} \cdot 3^{104} \cdot 5^{168}$, więc ze stwierdzenia 9.23, $\tau(n) = 117 \cdot 105 \cdot 169 = 2076165$. Z twierdzenia 9.22 wynika, że wszystkimi dzielnikami liczby n są liczby $d = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma}$, gdzie $\alpha = 0, 1, \ldots, 116$, $\beta = 0, 1, \ldots, 104$ i $\gamma = 0, 1, \ldots, 168$.

Przykład 9.25. Dla dowolnej liczby pierwszej p i dla dowolnego $n \in \mathbb{N}_0$ na mocy twierdzenia 9.22 mamy, że wszystkimi dzielnikami liczby p^n są liczby: $1, p, p^2, \ldots, p^n$, czyli

$$D_{p^n} = \{1, p, p^2, \ldots, p^n\} \text{ dla każdego } p \in \mathbb{P}.$$

W szczególności wynika stąd, że **dla każdej liczby naturalnej** m **istnieje liczba naturalna posiadająca dokładnie** m **dzielników** (na przykład p^{m-1} dla $p \in \mathbb{P}$).

Przykład 9.26. Podamy kilka uwag dotyczących rozwiązywania równania $\tau(x) = m$ dla danej liczby naturalnej $m > 1$. Chodzi tu zatem o wyznaczenie wszystkich liczb naturalnych x, które posiadają dokładnie m dzielników. Ponieważ $m > 1$, więc $x > 1$, bo $\tau(1) = 1$. Z twierdzenia 9.18 wynika, że istnieją różne liczby pierwsze $p_1, \ldots, p_s$ i istnieją liczby naturalne $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_s$ takie, że $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. Zatem na mocy stwierdzenia 9.23,

$$m = (1+\alpha_1) \cdot (1+\alpha_2) \cdot \ldots \cdot (1+\alpha_s). \tag{9.4}$$

Ponadto $\alpha_i \geqslant 1$, więc $1 + \alpha_i \geqslant 2$ dla $i = 1, 2, \ldots, s$, skąd otrzymujemy ograniczenie na s w zależności od m:

$$2^s \leqslant m. \tag{9.5}$$

Ponadto ze wzoru (9.4) wynika, że każda z liczb $1+\alpha_i$ jest dzielnikiem liczby m oraz

$$1 + \alpha_1 \leqslant 1 + \alpha_2 \leqslant \ldots \leqslant 1 + \alpha_s. \tag{9.6}$$

Te obserwacje bardzo ułatwiają rozwiązywanie równania $\tau(x) = m$. Rozważmy na przykład przypadek $m = 6$. Wówczas z (9.5) wynika, że $s = 1$ lub $s = 2$. Jeśli $s = 1$, to z (9.4), $1 + \alpha_1 = 6$, więc $x = p^5$ dla $p \in \mathbb{P}$. Jeśli $s = 2$, to z (9.4), $(1 + \alpha_1) \cdot (1 + \alpha_2) = 6$. A ponieważ $D_6 = \{1, 2, 3, 6\}$ i $1 + \alpha_1 \leqslant 1 + \alpha_2$, więc $1 + \alpha_1 = 2$ i $1 + \alpha_2 = 3$, skąd $x = p_1 \cdot p_2^2$ dla różnych liczb pierwszych p_1 i p_2. Podsumowując, **liczba naturalna x posiada dokładnie 6 dzielników wtedy i tylko wtedy, gdy x jest 5-tą potęgą pewnej liczby pierwszej lub x jest iloczynem liczby pierwszej i kwadratu innej liczby pierwszej**.

Twierdzenie 9.27. *Niech $p_1, \ldots, p_s$ będą różnymi liczbami pierwszymi, $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ oraz niech $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Wówczas a jest n-tą potęgą pewnej liczby naturalnej wtedy i tylko wtedy, gdy $n \mid \alpha_i$ dla każdego $i = 1, \ldots, s$.*

Dowód. Jeżeli $n \mid \alpha_i$ dla $i = 1, \ldots, s$, to dla każdego $i = 1, \ldots, s$ istnieje nieujemna liczba całkowita β_i taka, że $\alpha_i = n \cdot \beta_i$. Stąd $k = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$ jest liczbą naturalną i $a = k^n$.

Na odwrót, załóżmy, że $a = k^n$ dla pewnej liczby naturalnej k. Wtedy $k|a$, więc z twierdzenia 9.22 istnieją nieujemne liczby całkowite $\beta_1, \ldots, \beta_s$ takie, że $k = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$. Zatem $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} = p_1^{n \cdot \beta_1} \cdot \cdot \ldots \cdot p_s^{n \cdot \beta_s}$, skąd z twierdzenia 9.17, $\alpha_i = n \cdot \beta_i$, czyli $n|\alpha_i$ dla każdego $i = 1, \ldots, s$. □

Twierdzenie 9.28. *Jeżeli p jest liczbą pierwszą, to $p \mid \binom{p}{k}$ dla każdego $k = 1, \ldots, p-1$.*

Dowód. Niech k będzie dowolną ustaloną liczbą naturalną mniejszą od p. Oznaczmy $\binom{p}{k} = n_k$. Wtedy z kombinatoryki wiadomo, że n_k jest liczbą podzbiorów k-elementowych zbioru p-elementowego, czyli n_k jest liczbą całkowitą. Ponadto wiadomo, że $n_k = \frac{p!}{k!\cdot(p-k)!}$, więc $p! = n_k \cdot k! \cdot (p-k)!$. Ponadto ze stwierdzenia 8.12 mamy, że p nie dzieli j dla $j = 1, \ldots, p-1$. Zatem z twierdzenia 9.14 mamy, że p nie dzieli $k!$ oraz p nie dzieli $(p-k)!$. Ponadto $p! = 1 \cdot 2 \cdot \ldots \cdot p$, więc $p \mid p!$. Zatem z twierdzenia 9.14, $p \mid n_k$. □

Twierdzenie 9.29. (małe twierdzenie Fermata). *Dla dowolnej liczby pierwszej p i dla dowolnej liczby naturalnej n liczba $n^p - n$ jest podzielna przez p.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje liczba pierwsza p i istnieje liczba naturalna n taka, że p nie dzieli $n^p - n$. Wówczas z zasady minimum istnieje najmniejsza taka liczba naturalna m, że p nie dzieli liczby $m^p - m$, ale $1^p - 1 = 0$ i $p \mid 0$, więc $m > 1$. Zatem istnieje liczba naturalna s taka, że $m = s + 1$. Ponadto $s < m$, więc z minimalności m wynika, że $p \mid s^p - s$. Ze wzoru Newtona $(s+1)^p = s^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} \cdot s^k$. Zatem $m^p - m = (s+1)^p - (s+1) = (s^p - s) + l$, gdzie liczba naturalna l jest na mocy twierdzenia 9.28 podzielna przez p. Stąd ze stwierdzenia 8.8, $p \mid (m^p - m)$ i mamy sprzeczność. □

9.5 Wzory na NWD i NWW

Niech $x_1, \ldots, x_k$ $(k \geqslant 2)$ będą dowolnymi liczbami rzeczywistymi. Wtedy w zbiorze $\{x_1, \ldots, x_k\}$ istnieje liczba najmniejsza, którą oznaczamy przez $\min\{x_1, \ldots, x_k\}$ i istnieje liczba największa, którą oznaczamy przez $\max\{x_1, \ldots, x_k\}$. Oczywiście dla każdego $i = 1, \ldots, k$:

$$\min\{x_1, \ldots, x_k\} \leqslant x_i \leqslant \max\{x_1, \ldots, x_k\} \tag{9.7}$$

Na przykład $\min\{0, 1, 2, 0, 2\} = 0$ i $\max\{0, 1, 2, 0, 2\} = 2$.

Twierdzenie 9.30. *Niech $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_s \in \mathbb{N}_0$ i niech $p_1, \ldots, p_s$ będą różnymi liczbami pierwszymi. Wówczas zachodzą wzory:*

$$\mathrm{NWD}(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},\ p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s, \beta_s\}}, \tag{9.8}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$$\mathrm{NWW}(p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s},\ p_1^{\beta_1}\cdot\ldots\cdot p_s^{\beta_s}) = p_1^{\max\{\alpha_1,\beta_1\}}\cdot\ldots\cdot p_s^{\max\{\alpha_s,\beta_s\}}. \quad (9.9)$$

Dowód. Oznaczmy prawą stronę wzoru (9.8) przez D. Ponadto, niech $a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ oraz $b = p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_s^{\beta_s}$. Na mocy twierdzenia 9.22, d jest wspólnym dzielnikiem liczb a i b wtedy i tylko wtedy, gdy $d = p_1^{\delta_1}\cdot\ldots\cdot p_s^{\delta_s}$ dla pewnych $\delta_1,\ldots,\delta_s\in\mathbb{N}_0$ takich, że $\delta_i\leqslant\alpha_i$ oraz $\delta_i\leqslant\beta_i$ dla $i=1,2,\ldots,s$. Stąd d jest wspólnym dzielnikiem liczb a i b wtedy i tylko wtedy, gdy $d = p_1^{\delta_1}\cdot\ldots\cdot p_s^{\delta_s}$ dla pewnych $\delta_1,\ldots,\delta_s\in\mathbb{N}_0$ takich, że $\delta_i\leqslant\min\{\alpha_i,\beta_i\}$ dla $i=1,2,\ldots,s$. Zatem największym wspólnym dzielnikiem liczb a i b jest liczba D, co kończy dowód wzoru (9.8).

Oznaczmy prawą stronę wzoru (9.8) przez m. Wtedy z (9.7) i z twierdzenia 9.22 mamy, że m jest wspólną wielokrotnością liczb a i b. Zatem z twierdzenia 8.36, $\mathrm{NWW}(a,b)\mid m$. Wobec tego, na mocy twierdzenia 9.22, istnieją $\gamma_1,\ldots,\gamma_s\in\mathbb{N}_0$ takie, że $\mathrm{NWW}(a,b) = p_1^{\gamma_1}\cdot\ldots\cdot p_s^{\gamma_s}$ oraz $\gamma_i\leqslant\max\{\alpha_i,\beta_i\}$ dla $i=1,\ldots,s$. Ponadto, $a\mid\mathrm{NWW}(a,b)$ i $b\mid\mathrm{NWW}(a,b)$, więc z twierdzenia 9.22, $\alpha_i\leqslant\gamma_i$ oraz $\beta_i\leqslant\gamma_i$, skąd $\max\{\alpha_i,\beta_i\}\leqslant\gamma_i$ dla $i=1,\ldots,s$. Wobec tego $\gamma_i\leqslant\max\{\alpha_i,\beta_i\}$ i $\max\{\alpha_i,\beta_i\}\leqslant\gamma_i$, skąd $\gamma_i=\max\{\alpha_i,\beta_i\}$ dla $i=1,\ldots,s$, a zatem $\mathrm{NWW}(a,b)=m$, co kończy dowód wzoru (9.9). □

Przykład 9.31. Obliczmy $\mathrm{NWD}(1176,2100)$ i $\mathrm{NWW}(1176,2100)$. Z przykładu 9.19 wiemy, że $1176 = 2^3\cdot3\cdot7^2$ oraz $2100 = 2^2\cdot3\cdot5^2\cdot7$. Zatem $1176 = 2^3\cdot3^1\cdot5^0\cdot7^2$ i $2100 = 2^2\cdot3^1\cdot5^2\cdot7^1$. Stąd na mocy twierdzenia 9.30 mamy, że $\mathrm{NWD}(1176,2100) = 2^2\cdot3^1\cdot5^0\cdot7^1 = 84$ oraz $\mathrm{NWW}(1176,2100) = 2^3\cdot3^1\cdot5^2\cdot7^2 = 29400$.

Twierdzenie 9.30 można uogólnić na większą liczbę liczb naturalnych. Mianowicie zachodzi następujące twierdzenie:

Twierdzenie 9.32. *Niech $\alpha_{i1},\ldots,\alpha_{is}\in\mathbb{N}_0$ dla $i=1,\ldots,k$ i niech $p_1,\ldots,p_s$ będą różnymi liczbami pierwszymi. Niech $a_i = p_1^{\alpha_{i1}}\cdot\ldots\cdot p_s^{\alpha_{is}}$ dla $i=1,\ldots,k$. Wówczas zachodzą wzory:*

(a) $\mathrm{NWD}(a_1,\ldots,a_k) = p_1^{\min\{\alpha_{11},\alpha_{21},\ldots,\alpha_{k1}\}}\cdot\ldots\cdot p_s^{\min\{\alpha_{1s},\alpha_{2s},\ldots,\alpha_{ks}\}}$,

(b) $\mathrm{NWW}(a_1,\ldots,a_k) = p_1^{\max\{\alpha_{11},\alpha_{21},\ldots,\alpha_{k1}\}}\cdot\ldots\cdot p_s^{\max\{\alpha_{1s},\alpha_{2s},\ldots,\alpha_{ks}\}}$.

Dowód. Oznaczmy prawą stronę wzoru (a) przez D. Wtedy z (9.7) oraz z twierdzenia 9.22 mamy, że D jest wspólnym dzielnikiem liczb

$a_1, \ldots, a_k$. Jeżeli d jest wspólnym dzielnikiem liczb $a_1, \ldots, a_k$, to z twierdzenia 9.22, $d = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$ dla pewnych nieujemnych liczb całkowitych $\beta_1, \ldots, \beta_s$ takich, że $\beta_i \leqslant \alpha_{ji}$ dla $j = 1, 2, \ldots, k$, skąd $\beta_i \leqslant \min\{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ki}\}$ dla $i = 1, 2, \ldots, s$. Zatem $d \leqslant D$, czyli $D = \mathrm{NWD}(a_1, \ldots, a_k)$, co kończy dowód (a).

Oznaczmy prawą stronę wzoru (b) przez m. Wtedy z (9.7) i z twierdzenia 9.22 mamy, że m jest wspólną wielokrotnością liczb $a_1, \ldots, a_k$. Niech $n = \mathrm{NWW}(a_1, \ldots, a_k)$. Wtedy z twierdzenia 8.36, $n \mid m$. Zatem z twierdzenia 9.22, $n = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$ dla pewnych nieujemnych liczb całkowitych $\gamma_1, \ldots, \gamma_s$ takich, że $\gamma_i \leqslant \max\{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ki}\}$ dla $i = 1, \ldots, s$. Ponadto $a_j \mid n$, więc z twierdzenia 9.22 mamy, że $\alpha_{ji} \leqslant \gamma_i$ dla $i = 1, 2, \ldots, k$. Stąd $\max\{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ki}\} \leqslant \gamma_i$ dla $i = 1, \ldots, s$. Zatem ostatecznie $\gamma_i = \max\{\alpha_{1i}, \ldots, \alpha_{ki}\}$, skąd $n = m$, czyli $m = \mathrm{NWW}(a_1, \ldots, a_k)$. □

Przykład 9.33. Obliczymy na mocy twierdzenia 9.32, $\mathrm{NWW}(2, 3, 4, 5, 6, 7, 8, 9, 10)$. Najpierw wypisujemy wszystkie liczby pierwsze występujące w rozkładach kanonicznych tych liczb, są nimi: 2, 3, 5, i 7. Stąd kolejno, $2 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^0$, $3 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0$, $4 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^0$, $5 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0$, $6 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0$, $7 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1$, $8 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^0$, $9 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0$ i $10 = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0$. Z twierdzenia 9.32, $\mathrm{NWW}(2, 3, 4, 5, 6, 7, 8, 9, 10) = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4}$, gdzie

$$\alpha_1 = \max\{1, 0, 2, 0, 1, 0, 3, 0, 1\} = 3,$$

$$\alpha_2 = \max\{0, 1, 0, 0, 1, 0, 0, 2, 0\} = 2,$$

$$\alpha_3 = \max\{0, 0, 0, 1, 0, 0, 0, 0, 1\} = 1,$$

$$\alpha_4 = \max\{0, 0, 0, 0, 0, 1, 0, 0, 0\} = 1.$$

Wobec tego

$$\mathrm{NWW}(2, 3, 4, 5, 6, 7, 8, 9, 10) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 2520.$$

Przykład 9.34. Zastosujemy twierdzenie 9.32 do obliczenia, $\mathrm{NWD}(36, 48, 63)$ i $\mathrm{NWW}(36, 48, 63)$. Najpierw rozkładamy na czynniki pierwsze liczby 36, 48 i 63:

$$\begin{array}{r|l} 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}, \quad \begin{array}{r|l} 48 & 2 \\ 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}, \quad \begin{array}{r|l} 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}.$$

Liczby pierwsze występujące w rozkładach kanonicznych naszych liczb to: 2, 3 i 7. Patrząc na „słupki" naszych rozkładów na czynniki pierwsze i stosując twierdzenie 9.32, uzyskujemy, że $\mathrm{NWD}(36, 48, 63) = 2^0 \cdot 3^1 \cdot 7^0 = 3$ oraz $\mathrm{NWW}(36, 48, 63) = 2^4 \cdot 3^2 \cdot 7^1 = 1008$.

Uwaga 9.35. Dla dowolnych liczb naturalnych a, b, c istnieją różne liczby pierwsze $p_1, p_2, \ldots, p_s$ i istnieją nieujemne liczby całkowite $\alpha_i, \beta_i, \gamma_i$ dla $i = 1, 2, \ldots, s$ takie, że $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, $b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$ i $c = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$. Rzeczywiście, jeśli $a = b = c = 1$, to wystarczy przyjąć $s = 1$, $p_1 = 2$, $\alpha_1 = \beta_1 = \gamma_1 = 0$, w przeciwnym przypadku istnieje niepusty skończony zbiór $\{p_1, p_2, \ldots, p_s\}$ liczb pierwszych złożony z czynników pierwszych liczb a, b i c. Jeśli liczba pierwsza p_i nie dzieli liczby a, to w jej rozkładzie umieszczamy p_i z wykładnikiem 0. Analogicznie postępujemy dla liczb b i c. Wobec tego, na mocy twierdzenia o jednoznaczności rozkładu i tego, że $1 = p_1^0 \cdot \ldots \cdot p_s^0$ uzyskujemy, że istnieją nieujemne liczby całkowite $\alpha_i, \beta_i, \gamma_i$ dla $i = 1, 2, \ldots, s$ takie, że $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, $b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$ i $c = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$.

Powtarzając powyższe rozumowanie możemy uogólnić naszą obserwację na dowolną liczbę liczb naturalnych większą od 3.

Twierdzenie 9.32 i uwaga 9.35 umożliwiają szybkie dowodzenie różnych własności NWD i NWW liczb naturalnych. Na przykład wychodząc z oczywistego faktu, że $x + y = \min\{x, y\} + \max\{x, y\}$ dla dowolnych liczb rzeczywistych można podać nowy dowód twierdzenia 8.44.

Przykład 9.36. Pokażemy, opierając się na twierdzeniu 9.32, że dla dowolnych $a, b, c \in \mathbb{N}$:

$$\mathrm{NWD}(ab, ac, bc) \cdot \mathrm{NWW}(a, b, c) = abc. \tag{9.10}$$

W tym celu na mocy uwagi 9.35 znajdujemy różne liczby pierwsze $p_1, \ldots, p_s$ oraz nieujemne liczby całkowite $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_s, \gamma_1, \ldots,$

γ_s takie, że $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, $b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$, $c = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$. Z twierdzenia 9.32 mamy, że lewa strona wzoru (9.10) jest iloczynem liczb postaci $p_1^{\min\{\alpha_i+\beta_i,\alpha_i+\gamma_i,\beta_i+\gamma_i\}+\max\{\alpha_i,\beta_i,\gamma_i\}}$ dla $i = 1, \ldots, s$ oraz $a \cdot b \cdot c = p_1^{\alpha_1+\beta_1+\gamma_1} \cdot \ldots \cdot p_s^{\alpha_s+\beta_s+\gamma_s}$. Wystarczy zatem wykazać, że dla dowolnych nieujemnych liczb całkowitych α, β, γ zachodzi równość:

$$\min\{\alpha+\beta, \alpha+\gamma, \beta+\gamma\} + \max\{\alpha, \beta, \gamma\} = \alpha+\beta+\gamma.$$

Bez zmniejszania ogólności możemy zakładać, że $\alpha \leqslant \beta \leqslant \gamma$ i wówczas $\min\{\alpha+\beta, \alpha+\gamma, \beta+\gamma\} = \alpha+\beta$ oraz $\max\{\alpha, \beta, \gamma\} = \gamma$, więc ta równość jest prawdziwa.

9.6 Wykładnik p-adyczny

Stwierdzenie 9.37. *Dla dowolnych liczb naturalnych n i $g > 1$ zachodzi nierówność: $g^n > n$.*

Dowód. Z nierówności Bernoulliego (5.1) mamy, że $g^n = (1+(g-1))^n \geqslant$ $\geqslant 1 + n(g-1) \geqslant 1 + n > n$, bo $g \geqslant 2$. □

Niech p będzie liczbą pierwszą oraz $n \in \mathbb{N}$. Wtedy na mocy stwierdzeń 8.12 i 9.37 mamy, że zbiór $\{\alpha \in \mathbb{N}_0 : p^\alpha \mid n\}$ jest ograniczony z góry (przez liczbę n). Ponadto ten zbiór zawiera 0, więc z zasady maksimum w tym zbiorze istnieje liczba największa. Nazywamy ją **wykładnikiem p-adycznym liczby** n i oznaczmy symbolem $\alpha_p(n)$. Wobec tego:

$$\alpha_p(n) = \max\{\alpha \in \mathbb{N}_0 : p^\alpha \mid n\}. \tag{9.11}$$

Równoważnie:

$$\alpha_p(n) \in \mathbb{N}_0 \text{ i } p^{\alpha_p(n)} \mid n \text{ oraz } p^{\alpha_p(n)+1} \nmid n. \tag{9.12}$$

Uwaga 9.38. Niech $a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gdzie $p_1, \ldots, p_k$ są różnymi liczbami pierwszymi oraz $\alpha_1, \ldots, \alpha_k \in \mathbb{N}_0$. Wówczas na mocy uwagi 9.16, $\alpha_p(a) = 0$ dla wszystkich liczb pierwszych $p \notin \{p_1, \ldots, p_k\}$ oraz na mocy twierdzenia 9.22, $\alpha_{p_i}(a) = \alpha_i$ dla $i = 1, \ldots, k$.

Przykład 9.39. Dla każdej liczby naturalnej n mamy, że $\frac{(2n)!}{n!} = (n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)$, skąd $\frac{(2n)!}{n!} = 2^n\cdot 1\cdot 3\cdot\ldots\cdot(2n-1)$ na mocy wzoru (1.13). Wobec tego $2^n \mid \frac{(2n)!}{n!}$ i $2^{n+1} \nmid \frac{(2n)!}{n!}$, czyli $\alpha_2(\frac{(2n)!}{n!}) = n$.

Następujące stwierdzenia podają podstawowe własności wykładnika p-adycznego.

Stwierdzenie 9.40. *Dla dowolnych liczb naturalnych a, b:*
(i) $a \mid b$ wtedy i tylko wtedy, gdy $\alpha_p(a) \leqslant \alpha_p(b)$ dla każdego $p \in \mathbb{P}$,
(ii) $a = b$ wtedy i tylko wtedy, gdy $\alpha_p(a) = \alpha_p(b)$ dla każdego $p \in \mathbb{P}$.

Dowód. (i). Na mocy twierdzenia 9.18 istnieją różne liczby pierwsze $p_1, \ldots, p_k$ i nieujemne liczby całkowite α_i, β_i dla $i = 1, \ldots, k$ takie, że $a = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$ i $b = p_1^{\beta_1}\cdot\ldots\cdot p_k\beta_k$. Jeśli $a \mid b$, to na mocy twierdzenia 9.22, $\alpha_i \leqslant \beta_i$ dla $i = 1, \ldots, k$. Stąd i z uwagi 9.38,$\alpha_p(a) \leqslant \alpha_p(b)$ dla każdego $p \in \mathbb{P}$. Na odwrót, załóżmy, że $\alpha_p(a) \leqslant \alpha_p(b)$ dla każdego $p \in \mathbb{P}$. Wtedy na mocy uwagi 9.38, $\alpha_i \leqslant \beta_i$ dla $i = 1, \ldots, k$, więc z twierdzenia 9.22, $a \mid b$.

(ii). Na mocy stwierdzenia 8.12, $a = b$ wtedy i tylko wtedy, gdy $a \mid b$ i $b \mid a$. Zatem z (i), $a = b$ wtedy i tylko wtedy, gdy dla każdego $p \in \mathbb{P}$ jest $\alpha_p(a) \leqslant \alpha_p(b)$ i $\alpha_p(b) \leqslant \alpha_p(a)$, czyli gdy $\alpha_p(a) = \alpha_p(b)$ dla każdego $p \in \mathbb{P}$. □

Stwierdzenie 9.41. *Dla dowolnych liczb naturalnych a, b i dla dowolnej liczby pierwszej p:*
(i) $\alpha_p(a+b) \geqslant \min\{\alpha_p(a), \alpha_p(b)\}$,
(ii) jeśli $\alpha_p(a) \neq \alpha_p(b)$, to $\alpha_p(a+b) = \min\{\alpha_p(a), \alpha_p(b)\}$.

Dowód. Niech $\alpha = \min\{\alpha_p(a), \alpha_p(b)\}$. Wtedy $p^\alpha \mid a$ i $p^\alpha \mid b$, skąd $p^\alpha \mid a+b$ i z definicji wykładnika p-adycznego mamy, że $\alpha \leqslant \alpha_p(a+b)$, co dowodzi (i). Jeśli dodatkowo $\alpha_p(a) \neq \alpha_p(b)$, to bez zmniejszania ogólności możemy zakładać, że $\alpha_p(a) < \alpha_p(b)$. Wtedy $\alpha = \min\{\alpha_p(a), \alpha_p(b)\} = \alpha_p(a) \leqslant \alpha_p(a+b)$. Jeśli $\alpha_p(a+b) > \alpha$, to $p^{\alpha+1} \mid a+b$. Ale $p^{\alpha+1} \mid b$, gdyż $\alpha_p(b) \geqslant \alpha+1$, więc $p^{\alpha+1} \mid a$, skąd $p^{\alpha_p(a)+1} \mid a$, co prowadzi do sprzeczności. Wobec tego $\alpha_p(a+b) = \min\{\alpha_p(a), \alpha_p(b)\}$. □

Stwierdzenie 9.42. *Dla dowolnych $a, n, a_1, a_2, \ldots, a_n \in \mathbb{N}$ i dla dowolnej liczby pierwszej p:*
(i) $\alpha_p(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = \alpha_p(a_1) + \alpha_p(a_2) + \ldots + \alpha_p(a_n)$,
(ii) $\alpha_p(a^n) = n \cdot \alpha_p(a)$,
(iii) $\alpha_p(\mathrm{NWD}(a_1, \ldots, a_n)) = \min\{\alpha_p(a_1), \ldots, \alpha_p(a_n)\}$,
(iv) $\alpha_p(\mathrm{NWW}(a_1, \ldots, a_n)) = \max\{\alpha_p(a_1), \ldots, \alpha_p(a_n)\}$.

Dowód. (i). Na mocy (9.12), $a_i = p^{\alpha_p(a_i)} b_i$, gdzie $b_i \in \mathbb{N}$ oraz $p \nmid b_i$ dla każdego $i = 1, 2, \ldots, n$. Zatem $a_1 \cdot \ldots \cdot a_n = p^{\alpha_p(a_1)+\ldots+\alpha_p(a_n)} b$, gdzie $b = b_1 \cdot \ldots \cdot b_n$ nie jest podzielne przez p na mocy twierdzenia 9.14. Stąd $\alpha_p(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = \alpha_p(a_1) + \alpha_p(a_2) + \ldots + \alpha_p(a_n)$. Podstawiając $a = a_1 = \ldots = a_n$ otrzymujemy od razu wzór (ii).

(iii) oraz (iv) wynikają od razu z uwag 9.35, 9.38 i z twierdzenia 9.32. □

Przykład 9.43. Udowodnimy, że dla dowolnych $a, b, c \in \mathbb{N}$ zachodzi wzór:

$$\mathrm{NWD}(a, \mathrm{NWW}(b, c)) = \mathrm{NWW}(\mathrm{NWD}(a, b), \mathrm{NWD}(a, c)). \qquad (9.13)$$

Oznaczmy przez L i przez P lewą i prawą stronę wzoru (9.13) odpowiednio. Na mocy stwierdzenia 9.40 wystarczy wykazać, że $\alpha_p(L) = \alpha_p(P)$ dla każdego $p \in \mathbb{P}$. Ponadto, na mocy stwierdzenia 9.42:
$\alpha_p(L) = \min\{\alpha_p(a), \max\{\alpha_p(b), \alpha_p(c)\}\}$ oraz
$\alpha_p(P) = \max\{\min\{\alpha_p(a), \alpha_p(b)\}, \min\{\alpha_p(a), \alpha_p(c)\}\}$, więc wystarczy wykazać, że dla dowolnych $x, y, z \in \mathbb{N}_0$ zachodzi wzór:

$$\min\{x, \max\{y, z\}\} = \max\{\min\{x, y\}, \min\{x, z\}\}.$$

Zauważmy, że lewa i prawa strona tego wzoru jest symetryczna względem y i z. Możemy zatem bez zmniejszania ogólności zakładać, że $y \leqslant z$. Wtedy $\min\{x, \max\{y, z\}\} = \min\{x, z\}$, więc jeśli $x \leqslant y$, to $\min\{x, \max\{y, z\}\} = x = \max\{x, x\} = \max\{\min\{x, y\}, \min\{x, z\}\}$, a jeśli $y \leqslant x \leqslant z$, to
$\min\{x, \max\{y, z\}\} = x = \max\{y, x\} = \max\{\min\{x, y\}, \min\{x, z\}\}$.
Ostatnim przypadkiem jest: $y \leqslant z \leqslant x$. Wtedy $\min\{x, \max\{y, z\}\} = z = \max\{y, z\} = \max\{\min\{x, y\}, \min\{x, z\}\}$.

Przykład 9.44. Udowodnimy, że dla dowolnych $a, b, c \in \mathbb{N}$ zachodzi wzór:

$$\mathrm{NWW}(a, \mathrm{NWD}(b, c)) = \mathrm{NWD}(\mathrm{NWW}(a, b), \mathrm{NWW}(a, c)). \qquad (9.14)$$

Oznaczmy przez L i przez P lewą i prawą stronę wzoru (9.14) odpowiednio. Na mocy stwierdzenia 9.40 wystarczy wykazać, że $\alpha_p(L) = \alpha_p(P)$ dla każdego $p \in \mathbb{P}$, ale na mocy stwierdzenia 9.42:
$\alpha_p(L) = \max\{\alpha_p(a), \min\{\alpha_p(b), \alpha_p(c)\}\}$ oraz
$\alpha_p(P) = \min\{\max\{\alpha_p(a), \alpha_p(b)\}, \max\{\alpha_p(a), \alpha_p(c)\}\}$, więc wystarczy wykazać, że dla dowolnych $x, y, z \in \mathbb{N}_0$ zachodzi wzór:

$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\}.$$

Analizujemy kolejno wszystkie możliwe przypadki:
1. $x \leqslant y \leqslant z$. Wtedy $\max\{x, \min\{y, z\}\} = \max\{x, y\} = y$ oraz $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, z\} = y$.
2. $x \leqslant z \leqslant y$. Wtedy $\max\{x, \min\{y, z\}\} = \max\{x, z\} = z$ oraz $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, z\} = z$.
3. $y \leqslant x \leqslant z$. Wtedy $\max\{x, \min\{y, z\}\} = \max\{x, y\} = x$ oraz $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{x, z\} = x$.
4. $y \leqslant z \leqslant x$. Wtedy $\max\{x, \min\{y, z\}\} = \max\{x, y\} = x$ oraz $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{x, x\} = x$.
5. $z \leqslant x \leqslant y$. Wtedy $\max\{x, \min\{y, z\}\} = \max\{x, z\} = x$ oraz $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, x\} = x$.
6. $z \leqslant y \leqslant x$. Wtedy $\max\{x, \min\{y, z\}\} = \max\{x, z\} = x$ oraz $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{x, x\} = x$.

Zatem w każdym przypadku

$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\},$$

co kończy dowód.

Następne twierdzenie odgrywa dużą rolę w rozwiązywaniu tak zwanych równań diofantycznych.

Twierdzenie 9.45. *Niech $s \geqslant 2$ oraz $a_1, a_2, \ldots, a_s, c$ i n będą liczbami naturalnymi, przy czym każde dwie spośród liczb $a_1, a_2, \ldots, a_s$ są względnie pierwsze. Jeżeli $a_1 \cdot a_2 \cdot \ldots \cdot a_s = c^n$, to istnieją liczby naturalne c_i takie, że $a_i = c_i^n$ dla każdego $i = 1, 2, \ldots, s$.*

Dowód. Ustalmy dowolne $i = 1, 2, \ldots, s$. Jeśli $a_i = 1$, to wystarczy wziąć $c_i = 1$. Niech dalej $a_i > 1$. Weźmy dowolną liczbę pierwszą p dzielącą a_i. Na mocy stwierdzenia 9.20 mamy, że $p \nmid a_j$, skąd $\alpha_p(a_j) = 0$ dla wszystkich $j \in \{1, \ldots, s\} \setminus \{i\}$. Zatem na mocy stwierdzenia 9.42, $\alpha_p(a_i) = \alpha_p(a_1 \cdot \ldots \cdot a_s) = \alpha_p(c^n) = n\alpha_p(c)$. Z dowolności p oraz na mocy twierdzenia 9.27, a_i jest n-tą potęgą pewnej liczby naturalnej. □

Z podstawowych własności liczb rzeczywistych wynika, że dla dowolnej liczby rzeczywistej x istnieje największa liczba całkowita k taka, że $k \leqslant x$. Odwołując się do osi liczbowej, możemy zatem powiedzieć, że k jest najbliższą liczbą całkowitą, która leży po lewej stronie liczby x. Liczbę k będziemy oznaczali symbolem $\lfloor x \rfloor$ i nazywali **częścią całkowitą liczby rzeczywistej** x. (W literaturze można spotkać inne oznaczenie $\lfloor x \rfloor$ przez $E(x)$). Przykładowo mamy: $\lfloor \pi \rfloor = \lfloor 3,14\ldots \rfloor = 3$, $\lfloor -\pi \rfloor = \lfloor -3,14\ldots \rfloor = -4$, $\lfloor 6 \rfloor = 6$, $\lfloor \frac{27}{4} \rfloor = \lfloor 6\frac{3}{4} \rfloor = 6$.

Wprost z definicji części całkowitej liczby rzeczywistej mamy, że:

$$\lfloor x \rfloor \in \mathbb{Z} \quad \text{oraz} \quad \lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1 \quad \text{dla każdego } x \in \mathbb{R}. \tag{9.15}$$

Ponadto, jeśli liczba całkowita k spełnia nierówności $k \leqslant x < k+1$, to oczywiście $k = \lfloor x \rfloor$.

Stwierdzenie 9.46. *Dla dowolnych liczb rzeczywistych x i y zachodzą wzory:*

(i) $x = \lfloor x \rfloor \iff x \in \mathbb{Z}$,

(ii) $\lfloor x + k \rfloor = \lfloor x \rfloor + k$ *dla każdego* $k \in \mathbb{Z}$,

(iii) jeżeli $x \leqslant y$, *to* $\lfloor x \rfloor \leqslant \lfloor y \rfloor$,

(iv) $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor$,

(v) $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$ *dla każdego* $n \in \mathbb{N}$.

Dowód. (i). Niech $x \in \mathbb{Z}$. Ponieważ $x \leqslant x$, więc x jest największą liczbą całkowitą nie większą od x, czyli $x = \lfloor x \rfloor$. Jeżeli zaś $x = \lfloor x \rfloor$, to $x \in \mathbb{Z}$ na mocy (9.15).

(ii). Weźmy dowolne $k \in \mathbb{Z}$. Wtedy na mocy (9.15), $\lfloor x \rfloor + k \in \mathbb{Z}$ oraz $\lfloor x \rfloor + k \leqslant x + k < (x+k)+1$, więc na mocy (9.15), $\lfloor x+k \rfloor = \lfloor x \rfloor + k$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

(*iii*). Niech $x \leqslant y$. Wtedy na mocy (9.15), $\lfloor x \rfloor \leqslant x$, więc $\lfloor x \rfloor \leqslant y$, ale $\lfloor x \rfloor \in \mathbb{Z}$ i $\lfloor y \rfloor$ jest największą liczbą całkowitą nie większą od y, więc $\lfloor x \rfloor \leqslant \lfloor y \rfloor$.

(*iv*). Na mocy (9.15) mamy, że $\lfloor x \rfloor \leqslant x$ i $\lfloor y \rfloor \leqslant y$, więc $\lfloor x \rfloor + \lfloor y \rfloor \leqslant x + y$, ale $\lfloor x \rfloor + \lfloor y \rfloor \in \mathbb{Z}$ i $\lfloor x + y \rfloor$ jest największą liczbą całkowitą nie większą od $x + y$, więc $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor$.

(*v*). Ze wzoru (9.15) wynika, że $\frac{x}{n} = \left\lfloor \frac{x}{n} \right\rfloor + \alpha$, dla pewnej liczby rzeczywistej α takiej, że $0 \leqslant \alpha < 1$. Zatem $0 \leqslant n\alpha < n$ i $x = n \cdot \left\lfloor \frac{x}{n} \right\rfloor + n\alpha$, skąd na mocy (*ii*) mamy, że $\lfloor x \rfloor = n \cdot \left\lfloor \frac{x}{n} \right\rfloor + \lfloor n\alpha \rfloor$. Ponadto $\lfloor n\alpha \rfloor \leqslant n\alpha < n$, więc $\lfloor n\alpha \rfloor < n$. Wobec tego $\frac{\lfloor x \rfloor}{n} = \left\lfloor \frac{x}{n} \right\rfloor + \beta$, gdzie $0 \leqslant \beta = \frac{\lfloor n\alpha \rfloor}{n} < 1$. Stąd na mocy (*ii*) mamy, że $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor + \lfloor \beta \rfloor = \left\lfloor \frac{x}{n} \right\rfloor + 0$, czyli $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$. □

Lemat 9.47. *Niech $x \geqslant 0$ będzie dowolną liczbą rzeczywistą, zaś m liczbą naturalną. Wówczas liczba k wszystkich liczb naturalnych nie większych od x i podzielnych przez m jest równa $k = \left\lfloor \frac{x}{m} \right\rfloor$.*

Dowód. Ogólna postać liczby naturalnej podzielnej przez m to lm, gdzie $l \in \mathbb{N}$. Możliwe są tylko dwa przypadki:

1. $0 \leqslant x < m$. Wtedy $lm \geqslant m > x$ dla $l \in \mathbb{N}$, więc nie ma liczby naturalnej $\leqslant x$ podzielnej przez m. Ponadto wtedy $0 \leqslant \frac{x}{m} < 1$, więc $\left\lfloor \frac{x}{m} \right\rfloor = 0$. Zatem w tym przypadku teza zachodzi.

2. $x \geqslant m$. Wówczas $\frac{x}{m} \geqslant 1$, więc ze stwierdzenia 9.46, $k = \left\lfloor \frac{x}{m} \right\rfloor \geqslant$ $\geqslant 1$, czyli $k \in \mathbb{N}$. Ale $k = \left\lfloor \frac{x}{m} \right\rfloor \leqslant \frac{x}{m}$, zatem $km \leqslant x$. Wobec tego $m, 2m, 3m, ..., km$ są liczbami naturalnymi podzielnymi przez m i nie większymi od x. Ponadto $k + 1 = \left\lfloor \frac{x}{m} \right\rfloor + 1 > \frac{x}{m}$, czyli $m\,(k+1) > x$. Stąd $m, 2m, 3m, \ldots, km$ to wszystkie liczby naturalne $\leqslant x$ i podzielne przez m. Zatem jest ich dokładnie $k = \left\lfloor \frac{x}{m} \right\rfloor$. □

Lemat 9.48. *Niech $n \in \mathbb{N}$ oraz niech p będzie liczbą pierwszą. Wówczas:*

$$n! = p^{\left\lfloor \frac{n}{p} \right\rfloor} \cdot \left\lfloor \frac{n}{p} \right\rfloor ! \cdot N, \tag{9.16}$$

gdzie N jest iloczynem wszystkich liczb naturalnych $\leqslant n$, które nie są podzielne przez p. W szczególności $p \nmid N$.

Dowód. Z lematu 9.47 wiemy, że liczba k wszystkich liczb naturalnych $\leqslant n$ i podzielnych przez p wynosi $k = \left\lfloor \frac{n}{p} \right\rfloor$. Stąd to liczby: $p, 2p, \ldots, kp$. Oznaczmy przez N iloczyn wszystkich liczb naturalnych $\leqslant n$, które nie dzielą się przez p. Wtedy $n! = (p \cdot 2p \cdot \ldots \cdot kp) \cdot N = p^k \cdot k! \cdot N$, czyli $n! = p^{\left\lfloor \frac{n}{p} \right\rfloor} \cdot \left\lfloor \frac{n}{p} \right\rfloor! \cdot N$. Z twierdzenia 9.14 mamy, że $p \nmid N$. □

Twierdzenie 9.49. *Dla każdego $n \in \mathbb{N}$ liczba pierwsza p wchodzi do rozkładu liczby $n!$ na czynniki pierwsze z wykładnikiem*

$$\alpha_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots. \tag{9.17}$$

Dowód. Zastosujemy indukcję względem $n \in \mathbb{N}$. Jeśli $n < p$, to $p \nmid k$ dla każdego $k = 1, 2, \ldots, n$, więc na mocy twierdzenia 9.14, $p \nmid n!$, skąd $\alpha_p(n!) = 0$. Ponadto wtedy $\frac{n}{p} < 1$, więc $\frac{n}{p^k} < 1$ dla $k \in \mathbb{N}$, skąd $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ dla $k \in \mathbb{N}$, czyli $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots = 0$. Zatem dla takich n wzór (9.17) zachodzi.

Niech teraz $n \geqslant p$ będzie taką liczbą naturalną, że dla każdej liczby naturalnej $m < n$ wzór (9.17) zachodzi. Ponieważ $\frac{n}{p} < n$, więc $m = \left\lfloor \frac{n}{p} \right\rfloor < n$ i $m \in \mathbb{N}$. Z lematu 9.48, $n! = p^m \cdot m! \cdot N$, gdzie $N \in \mathbb{N}$ i $p \nmid N$. Stąd na mocy stwierdzenia 9.42 i założenia indukcyjnego, $\alpha_p(n!) = m + \alpha_p(m!) + 0 = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \ldots$. Ponadto dla $k \in \mathbb{N}$ na mocy stwierdzenia 9.46 jest $\left\lfloor \frac{m}{p^k} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p^k} \right\rfloor = \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$, więc $\alpha_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots$. □

Przykład 9.50. Udowodnimy, że $2^n \nmid n!$ dla każdego $n \in \mathbb{N}$. W tym celu wystarczy pokazać, że $\alpha_2(n!) < n$. Z twierdzenia 9.49 otrzymujemy, że $\alpha_2(n!) = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{8} \rfloor + \ldots$. Skąd na mocy (9.15) i stwierdzenia 9.37 wynika, że $\alpha_2(n!) < \frac{n}{2} + \frac{n}{4} + \ldots$. Ponadto ze szkolnego wzoru $\frac{n}{2} + \frac{n}{4} + \ldots = \frac{\frac{n}{2}}{1 - \frac{1}{2}} = n$, więc rzeczywiście $\alpha_2(n!) < n$.

Ćwiczenie 9.51. Niech $p, q \in \mathbb{P}$. Udowodnij, że jeżeli $p > q$, to $\alpha_p(n!) \leqslant \alpha_q(n!)$ dla każdego $n \in \mathbb{N}$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Ćwiczenie 9.52. Udowodnij, że dla każdej liczby naturalnej n liczba $\binom{2n}{n}$ jest parzysta.

Ćwiczenie 9.53. Udowodnij, że dla każdej liczby naturalnej k liczba $\binom{2^{k+1}}{2^k}$ daje resztę 2 z dzielenia przez 4.

Ćwiczenie 9.54. Udowodnij, że dla każdej liczby pierwszej p i dla dowolnych liczb naturalnych m i n z tego, że $m \leqslant n$ wynika, że $\alpha_p(m!) \leqslant \alpha_p(n!)$.

Przykład 9.55. Wyznaczymy wszystkie liczby naturalne n takie, że zapis dziesiętny liczby $n!$ kończy się dokładnie tysiącem zer. Ponieważ $10 = 2 \cdot 5$, więc na mocy twierdzenia 9.49 i ćwiczenia 9.51 należy rozwiązać równanie: $1000 = \lfloor \frac{n}{5} \rfloor + \lfloor \frac{n}{5^2} \rfloor + \ldots$. Najpierw szacujemy prawą stronę tego równania uzyskując, że jest ona mniejsza niż $\frac{n}{5} + \frac{n}{5^2} + \ldots = \frac{\frac{n}{5}}{1-\frac{1}{5}} = \frac{n}{4}$, więc $n > 4000$. Dalej, $\lfloor \frac{4004}{5} \rfloor = 800 = \lfloor \frac{4000}{5} \rfloor$, więc na mocy stwierdzenia 9.46 (v) i twierdzenia 9.49 mamy, że $\alpha_5(4004!) = \alpha_5(4000!) < 1000$. Obliczmy tą metodą $\alpha_5(4005!) = 801 + 160 + 32 + 6 + 1 = 1000$. Dla $k = 0, 1, 2, 3, 4$ mamy, że $\lfloor \frac{4005+k}{5} \rfloor = 801$, więc $\alpha_5(n!) = 1000$ dla $n \in \{4005, 4006, 4007, 4008, 4009\}$. Ponadto dla $n \geqslant 4010$ na mocy zadania 9.54 mamy $\alpha_5(n!) \geqslant \alpha_5(4010) = 802 + 160 + 32 + 6 + 1 = 1001$. Wobec tego ostatecznie uzyskujemy, że $n \in \{4005, 4006, 4007, 4008, 4009\}$.

Ćwiczenie 9.56. Iloma zerami kończy się liczba 12000!?

9.7 Problemy związane z liczbami pierwszymi

Teoria liczb obfituje w wiele bardzo trudnych problemów, które jest łatwo sformułować, dlatego budzą one zainteresowanie nie tylko zawodowych matematyków. W tym paragrafie przedstawimy tylko niektóre z nich, natomiast po dodatkowe, bardziej rozbudowane informacje odsyłamy, na przykład, do monografii [16].

Hipoteza Goldbacha jest jednym z najstarszych i najbardziej znanych nierozwiązanych problemów w teorii liczb i całej matematyce. Została ona postawiona przez niemieckiego matematyka Ch. Goldbacha w liście do L. Eulera 7 czerwca 1742 roku i postuluje, że każda parzysta liczba naturalna większa od 2 jest sumą dwóch liczb pierwszych. Pierwszy duży krok w kierunku udowodnienia hipotezy Goldbacha wykonał I. M. Winogradow w 1937 roku pokazując, że każda dostatecznie duża (czyli większa od pewnej ustalonej liczby n_0 nazywanej stałą Winogradowa) liczba nieparzysta jest sumą trzech liczb pierwszych. Następny ważny wynik pochodzi od J. R. Chena, który w 1973 roku pokazał, że każda dostatecznie duża liczba parzysta jest sumą liczby pierwszej i iloczynu co najwyżej dwóch liczb pierwszych. Problem dokładnego oszacowania stałej Winogradowa zajmuje matematyków do dziś - w 2002 roku M. Ch. Liu, T. Wang uzyskali, że $n_0 \leqslant 2 \cdot 10^{1346}$, zaś O. Ramare i Y. Saouter wykazali w 2003 roku, że $n_0 \leqslant 1,13256 \cdot 10^{22}$. Warto wspomnieć, że w 2015 roku peruwiański matematyk H. A. Helfgott przedstawił dowód (niestety nieopublikowany w recenzowanym czasopiśmie, ale szeroko akceptowany) słabej wersji hipotezy Goldbacha, która głosi, że każda nieparzysta liczba naturalna większa od 5 jest sumą trzech liczb pierwszych.

Twierdzenie Dirichleta o postępie arytmetycznym głosi, że dla dowolnych względnie pierwszych liczb naturalnych a i b w ciągu arytmetycznym o pierwszym wyrazie b i różnicy a występuje nieskończenie wiele liczb pierwszych. Twierdzenie to udowodnił w 1837 roku P. G. L. Dirichlet wykorzystując zaawansowany aparat matematyczny. Uwspółcześnioną modyfikację dowodu Dirichleta można znaleźć w monografii [27], a w opinii W. Sierpińskiego tego twierdzenia, poza pewnymi szczególnymi przypadkami (patrz na przykład ćwiczenia 10.40 i 10.41), nie da się udowodnić metodami elementarnymi. Warto wspomnieć, że w 2004 roku T. Tao i B. Green udowodnili, że istnieją dowolnie długie, ale skończone, ciągi arytmetyczne złożone z różnych liczb pierwszych. Między innymi za to osiągnięcie T. Tao otrzymał w 2006 roku Medal Fieldsa. Najdłuższym obecnie znanym postępem arytmetycznym złożonym z samych liczb pierwszych jest postęp liczący 27 wyrazów, z których pierwszy jest równy 224584605939537911, a jego

różnicą jest $81292139 \cdot 223092870$. Postęp ten został znaleziony w 2019 roku przez R. Gahana w ramach projektu PrimeGrid, o którym informacje można znaleźć w internecie.

Liczby bliźniacze to dwie liczby pierwsze różniące się o 2. Początkowe pary liczb bliźniaczych: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$. Problem istnienia nieskończenie wielu par liczb bliźniaczych jest ciągle otwarty. Największymi obecnie znanymi liczbami bliźniaczymi są, odkryte w 2016 roku: $2996863034895 \cdot 2^{1290000} \pm 1$. Jeden z najciekawszych wyników w tej tematyce uzyskał w 1966 roku J. R. Chen pokazując, że istnieje nieskończenie wiele liczb pierwszych p takich, że $p+2$ jest liczbą pierwszą lub $p+2$ jest iloczynem dwóch liczb pierwszych.

W roku 1845 J. Bertrand postawił następującą hipotezę (nazywaną **postulatem Bertranda**): dla każdej liczby naturalnej $n > 1$ istnieje co najmniej jedna liczba pierwsza p taka, że $n < p < 2n$. Bertrand sprawdził swoje przypuszczenie dla wszystkich $n \leqslant 3 \cdot 10^6$. Pełny dowód taj hipotezy przedstawił jako pierwszy P. L. Czebyszew w 1852 roku. Od tej pory to twierdzenie nazywa się **twierdzeniem Czebyszewa**. Jego elementarny dowód można znaleźć w wydanej po polsku, interesującej książce [2].

Bardzo starym i otwartym problemem dotyczącym liczb pierwszych jest kwestia istnienia nieskończenie wielu liczb pierwszych postaci n^2+1 dla $n \in \mathbb{N}$. W 2022 roku J. Merikoski pokazał, że istnieje nieskończenie wiele liczb postaci n^2+1, których największy dzielnik jest większy niż $n^{1,279}$. Zastąpienie wykładnika liczbą 2 dawałoby pozytywne rozwiązanie tego problemu. W 1978 roku H. Iwaniec pokazał, że dla nieskończenie wielu liczb naturalnych n liczba n^2+1 ma co najwyżej dwa dzielniki pierwsze. Odnotujmy też, że H. Iwaniec oraz J. Friendlander w 1998 roku udowodnili, że istnieje nieskończenie wiele liczb pierwszych p postaci x^2+y^4 gdzie $x, y \in \mathbb{N}$. W tym duchu D. R. Heath-Brown udowodnił w 2001 roku, że istnieje nieskończenie wiele liczb pierwszych postaci x^3+2y^3, gdzie $x, y \in \mathbb{N}$.

Rozdział 10

Kongruencje i ich zastosowania

Najprościej rzecz ujmując, **Arytmetyka modularna** jest zbiorem metod, które pozwalają rozwiązywać problemy dotyczące liczb całkowitych. Metody te wynikają z badania reszt otrzymywany w wyniku dzielenia przez siebie liczb całkowitych.

Chociaż początki tej teorii sięgają starożytności, historycy na ogół kojarzą narodziny arytmetyki modularnej z rokiem 1801 - datą publikacji książki *Disquisitiones arithmeticae* autorstwa Carla Friedricha Gaussa. Zaprezentowane tam podejście umożliwiło udowodnienie słynnych hipotez i uproszczenie dowodów ważnych wyników. Konsekwencje idei Gaussa można znaleźć także w innych dziedzinach matematyki poza czystą teorią liczb, takich jak algebra czy geometria.

W wieku 19 lat Gauss udowodnił prawo wzajemności reszt kwadratowych oraz skonstruował za pomocą cyrkla i linijki siedemnastokąt foremny, problem ten pozostawał nierozwiązany od starożytności. Wreszcie w 1801 r. opublikował *Disquisitiones arithmeticae* (Badania arytmetyczne) i otrzymał przydomek księcia matematyków.

Kongruencje dotyczyły najpierw liczb całkowitych, następnie wielomianów, a później bardziej skomplikowanych systemów algebraicznych w tym tak zwanych liczb całkowitych Gaussa.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

10.1 Kongruencje

Definicja 10.1. Niech $a, b \in \mathbb{Z}$ i niech $m \in \mathbb{N}$. Mówimy, że a przystaje do b modulo m i piszemy $a \equiv b \pmod{m}$, jeżeli $m \mid a - b$. W przeciwnym przypadku piszemy $a \not\equiv b \pmod{m}$. Otrzymaną w ten sposób relację nazywamy **kongruencją** (według modułu m).

Wprost z definicji kongruencji i ze stwierdzenia 8.13 wynika od razu następujące

Stwierdzenie 10.2. *Dla dowolnych liczb całkowitych a i b i dla dowolnej liczby naturalnej m następujące warunki są równoważne:*
(i) $a \equiv b \pmod{m}$,
(ii) $m \mid a - b$,
(iii) $[a]_m = [b]_m$.

Stwierdzenie 10.3. *Każda kongruencja według modułu m jest relacją równoważności w zbiorze $\mathbb{Z}$ wszystkich liczb całkowitych.*

Dowód. Niech $a, b, c \in \mathbb{Z}$. Ponieważ $[a]_m = [a]_m$, więc na mocy stwierdzenia 10.2, $a \equiv a \pmod{m}$. Załóżmy, że $a \equiv b \pmod{m}$. Wtedy $[a]_m = [b]_m$, więc $[b]_m = [a]_m$ i ze stwierdzenia 10.2, $b \equiv a \pmod{m}$. Załóżmy, że $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$. Wtedy ze stwierdzenia 10.2, $[a]_m = [b]_m$ i $[b]_m = [c]_m$, więc $[a]_m = [c]_m$ i ze stwierdzenia 10.2, $a \equiv c \pmod{m}$. □

Dla liczb naturalnych m oznaczmy przez $\mathbb{Z}_m$ zbiór wszystkich reszt z dzielenia przez m. Zatem:

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}. \tag{10.1}$$

Stwierdzenie 10.4. *Każda kongruencja według modułu m posiada dokładnie m klas abstrakcji:*

$$r + m\mathbb{Z} = \{qm + r : q \in \mathbb{Z}\} = \{a \in \mathbb{Z} : [a]_m = r\}, \quad \text{gdzie } r \in \mathbb{Z}_m. \tag{10.2}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Niech $a \in \mathbb{Z}$. Wtedy z twierdzenia o dzieleniu z resztą $a = qm + r$ dla pewnego $q \in \mathbb{Z}$ i dla pewnego $r = 0, 1, \ldots, m-1$. Zatem $[a]_m = r$, czyli $a \equiv r \pmod{m}$ i wobec tego $a \in r + m\mathbb{Z}$ oraz $a + m\mathbb{Z} = r + m\mathbb{Z}$. Stąd $\mathbb{Z} = \bigcup_{r=0}^{m-1} (r + m\mathbb{Z})$. Niech $r, s \in \{0, 1, \ldots, m-1\}$ będą takie, że $r + m\mathbb{Z} = s + m\mathbb{Z}$. Wtedy na mocy stwierdzenia 10.2, $[r]_m = [s]_m$, ale $[r]_m = r$ i $[s]_m = s$, więc $r = s$. Wobec tego zbiory (10.2) są parami różne i jest ich dokładnie $1 + (m-1) = m$. □

Dużą zaletą kongruencji jest to, że posiadają one podobne własności jak relacja równości. Wyraża to następujące

Twierdzenie 10.5. *Niech $m, n \in \mathbb{N}$ i niech $a, b, c \in \mathbb{Z}$ oraz niech $a_i, b_i \in \mathbb{Z}$ dla $i = 1, \ldots, n$. Wówczas:*

(i) jeżeli $a \equiv b \pmod{m}$, to $a + c \equiv b + c \pmod{m}$,

(ii) jeżeli $a \equiv b \pmod{m}$, to $a \cdot c \equiv b \cdot c \pmod{m}$,

(iii) jeżeli $a_i \equiv b_i \pmod{m}$ dla $i = 1, \ldots, n$, to $a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n \pmod{m}$,

(iv) jeżeli $a_i \equiv b_i \pmod{m}$ dla $i = 1, \ldots, n$, to $a_1 \cdot \ldots \cdot a_n \equiv b_1 \cdot \ldots \cdot b_n \pmod{m}$,

(v) jeżeli $a \equiv b \pmod{m}$, to $a^n \equiv b^n \pmod{m}$,

(vi) jeżeli $a \equiv b \pmod{m}$, to $f(a) \equiv f(b) \pmod{m}$ dla każdej funkcji $f\colon \mathbb{Z} \to \mathbb{Z}$ postaci $f(x) = c_0 + c_1 x + \ldots + c_s x^s$, gdzie $s \in \mathbb{N}_0$ oraz $c_0, c_1, \ldots, c_s \in \mathbb{Z}$.

Dowód. Dowody punktów $(iii)-(vi)$ wynikają natychmiast z twierdzeń 2.30 i 2.32 oraz z wniosku 2.31 i ze stwierdzenia 10.2. Natomiast punkty (i) oraz (ii) wynikają z (iii) i (iv) oraz z tego, że $c \equiv c \pmod{m}$. □

Skracanie kongruencji jest bardziej subtelne niż skracanie równości. Mówi o tym następujące

Twierdzenie 10.6. *Niech $m, n \in \mathbb{N}$ i niech $a, b, c \in \mathbb{Z}$. Wówczas:*

(i) $n \cdot a \equiv n \cdot b \pmod{mn}$ wtedy i tylko wtedy, gdy $a \equiv b \pmod{m}$,

(ii) jeżeli $n \mid m$ i $a \equiv b \pmod{m}$, to $a \equiv b \pmod{n}$,

(iii) jeżeli $\mathrm{NWD}(c, m) = 1$, to $a \cdot c \equiv b \cdot c \pmod{m}$ wtedy i tylko wtedy, gdy $a \equiv b \pmod{m}$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. (*i*). Niech $n \cdot a \equiv n \cdot b \pmod{mn}$. Wtedy $mn \mid na - nb$. Zatem $n(a-b) = mnk$ dla pewnego $k \in \mathbb{Z}$ i po skróceniu przez n, $a - b = mk$, skąd $m \mid a-b$, czyli $a \equiv b \pmod{m}$. Na odwrót, niech $a \equiv b \pmod{m}$. Wtedy $m \mid a - b$, więc $a - b = km$ dla pewnego $k \in \mathbb{Z}$, skąd $na - nb = mnk$, więc $mn \mid na - nb$. Zatem $n \cdot a \equiv n \cdot b \pmod{mn}$.

(*ii*). Z założeń wynika, że $n \mid m$ i $m \mid a - b$. Zatem ze stwierdzenia 8.8, $n \mid a - b$, czyli $a \equiv b \pmod{n}$.

(*iii*). Niech $\mathrm{NWD}(c, m) = 1$ i $a \cdot c \equiv b \cdot c \pmod{m}$. Wtedy mamy, że $m \mid ac - bc$, czyli $m \mid c(a - b)$, więc z zasadniczego twierdzenia arytmetyki, $m \mid a - b$, a zatem $a \equiv b \pmod{m}$. Implikacja odwrotna wynika od razu z twierdzenia 10.5 (ii). □

Twierdzenie 10.7. *Niech każde dwie liczby spośród liczb naturalnych $m_1, m_2, \ldots, m_s$ będą względnie pierwsze i niech $a, b \in \mathbb{Z}$. Wówczas równoważne są warunki:*

(i) $a \equiv b \pmod{m_i}$ *dla każdego* $i = 1, 2, \ldots, s$,

(ii) $a \equiv b \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_s}$.

Dowód. (*i*) $\Rightarrow$ (*ii*). Z założenia $m_i \mid a - b$ dla każdego $i = 1, 2, \ldots, s$. Zatem z wniosku 8.51, $m_1 \cdot m_2 \cdot \ldots \cdot m_s \mid a - b$, skąd

$$a \equiv b \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_s}.$$

Implikacja odwrotna wynika od razu z twierdzenia 10.6 (ii). □

Lemat 10.8. *Jeżeli liczba całkowita a jest względnie pierwsza z liczbą naturalną m, to istnieje liczba całkowita x taka, że $ax \equiv 1 \pmod{m}$. Dodatkowo, dla $y \in \mathbb{Z}$: $ay \equiv 1 \pmod{m}$ wtedy i tylko wtedy, gdy $y \equiv x \pmod{m}$.*

Dowód. Ponieważ $\mathrm{NWD}(a, m) = 1$, więc z twierdzenia 8.28, $ax + my = 1$ dla pewnych $x, y \in \mathbb{Z}$. Stąd $m \mid ax - 1$, czyli $ax \equiv 1 \pmod{m}$.

Niech teraz $y \in \mathbb{Z}$. Jeśli $ay \equiv 1 \pmod{m}$, to ze stwierdzenia 10.3, $ay \equiv ax \pmod{m}$ i z twierdzenia 10.6 (iii), $y \equiv x \pmod{m}$. Jeżeli zaś $y \equiv x \pmod{m}$, to ze stwierdzenia 10.2 (ii), $ay \equiv ax \pmod{m}$, więc ze stwierdzenia 10.3, $ay \equiv 1 \pmod{m}$. □

10.2 Zastosowania kongruencji

Twierdzenie 10.9. (chińskie o resztach). *Niech każde dwie liczby spośród liczb naturalnych $m_1, m_2, \ldots, m_s$ będą względnie pierwsze i niech $r_1, r_2, \ldots, r_s \in \mathbb{Z}$. Wówczas istnieje $r \in \mathbb{Z}$ takie, że $r \equiv r_i \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, s$. Ponadto dla dowolnego $x \in \mathbb{Z}$: $x \equiv r_i \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, s$ wtedy i tylko wtedy, gdy $x \equiv r \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_s}$.*

Dowód. Oznaczmy: $M = m_1 \cdot m_2 \cdot \ldots \cdot m_s$ i niech $M_i = \frac{M}{m_i}$ dla $i = 1, 2, \ldots, s$. Wtedy $m_i \mid M_j$ dla wszystkich $i \neq j$ oraz na mocy stwierdzenia 8.49, $\mathrm{NWD}(M_i, m_i) = 1$. Zatem z lematu 10.8 dla każdego $i = 1, 2, \ldots, s$ istnieje $x_i \in \mathbb{Z}$ takie, że $M_i x_i \equiv 1 \pmod{m_i}$. Niech $r = M_1 x_1 r_1 + M_2 x_2 r_2 + \ldots + M_s x_s r_s$. Wtedy $m_i \mid r - M_i x_i r_i$, skąd $r \equiv M_i x_i r_i \pmod{m_i}$ dla $i = 1, 2, \ldots, s$. Ponadto $M_i x_i \equiv 1 \pmod{m_i}$, więc na mocy twierdzenia 10.5 (ii), $M_i x_i r_i \equiv r_i \pmod{m_i}$, a zatem na mocy stwierdzenia 10.3, $r \equiv r_i \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, s$.

Ostatnia część naszego twierdzenia wynika od razu z twierdzenia 10.7. □

Przykład 10.10. Znajdziemy wszystkie liczby całkowite x takie, że $[x]_5 = 2$, $[x]_6 = 3$ i $[x]_{11} = 7$. Oczywiście $x \equiv 2 \pmod 5$ i $x \equiv 3 \equiv \pmod 6$ i $x \equiv 7 \pmod{11}$. Przy oznaczeniach dowodu twierdzenia chińskiego o resztach, $m_1 = 5$ i $M_1 = 6 \cdot 11 = 66$, $m_2 = 6$ i $M_2 = 5 \cdot \cdot 11 = 55$, $m_3 = 11$ i $M_3 = 5 \cdot 6 = 30$. Dla x_1 mamy kongruencję: $66x_1 \equiv 1 \pmod 5$, ale $66 \equiv 1 \pmod 5$, więc $x_1 \equiv 1 \pmod 5$ i możemy przyjąć $x_1 = 1$.

Dla x_2 mamy kongruencję: $55x_2 \equiv 1 \pmod 6$, ale $55 \equiv 1 \pmod 6$, więc $x_2 \equiv 1 \pmod 6$ i możemy przyjąć $x_2 = 1$.

Dla x_3 mamy: $30x_3 \equiv 1 \pmod{11}$, ale $30 \equiv 8 \pmod{11}$, więc $8x_3 \equiv \equiv 1 \pmod{11}$. Zatem $8x_3 \equiv -10 \pmod{11}$ i z twierdzenia 10.6 (iii), $4x_3 \equiv -5 \pmod{11}$. Stąd $4x_3 \equiv 6 \pmod{11}$ i znowu z twierdzenia 10.6 (iii), $2x_3 \equiv 3 \pmod{11}$. Zatem $2x_3 \equiv -8 \pmod{11}$, więc z twierdzenia 10.6 (iii), $x_3 \equiv -4 \pmod{11}$. Możemy zatem przyjąć $x_3 = -4$.

Wobec tego $x \equiv M_1 x_1 r_1 + M_2 x_2 r_2 + M_3 x_3 r_3 \pmod{5 \cdot 6 \cdot 11}$, ale $M_1 x_1 r_1 + M_2 x_2 r_2 + M_3 x_3 r_3 = 66 \cdot 1 \cdot 2 + 55 \cdot 1 \cdot 3 - 30 \cdot 4 \cdot 7 = -543$ oraz

$5 \cdot 6 \cdot 11 = 330$, więc $x \equiv 117 \pmod{330}$. Wobec tego $x = 330k + 117$ dla $k \in \mathbb{Z}$.

Definicja 10.11. Funkcję $\varphi\colon \mathbb{N} \to \mathbb{N}$ taką, że $\varphi(n)$ jest liczbą wszystkich liczb naturalnych $k \leqslant n$, które są względnie pierwsze z n, nazywamy **funkcją Eulera**.

Przykład 10.12. Wprost z definicji mamy, że $\varphi(1) = 1$ oraz $\varphi(n) < n$ i $\varphi(n) \in \mathbb{N}$ dla wszystkich liczb naturalnych $n > 1$, gdyż $\mathrm{NWD}(n, n) = n > 1$. Ponadto dla liczby pierwszej p każda z liczb $1, 2, \ldots, p-1$ nie jest podzielna przez p, a więc każda z tych liczb jest względnie pierwsza z p na mocy stwierdzenia 9.13, ale $\mathrm{NWD}(p, p) > 1$, więc stąd $\varphi(p) = p - 1$. W szczególności: $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, itd. Zauważmy, że wszystkimi liczbami naturalnymi $k \leqslant 4$, które są względnie pierwsze z liczbą 4 są jedynie 1 i 3. Zatem $\varphi(4) = 2$. Podobnie uzyskujemy, że na przykład $\varphi(6) = 2$.

Twierdzenie 10.13. (Eulera). *Jeżeli liczba całkowita a jest względnie pierwsza z liczbą naturalną m, to*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{10.3}$$

Dowód. Dla $m = 1$ teza jest oczywista. Niech dalej $m > 1$. Oznaczmy $s = \varphi(m)$. Wtedy $s \in \mathbb{N}$. Niech $r_1, r_2, \ldots, r_s$ będą wszystkimi liczbami naturalnymi względnie pierwszymi z liczbą m i nie większymi od m. Ponieważ $\mathrm{NWD}(m, m) = m > 1$, więc każda z tych liczb należy do zbioru $\mathbb{Z}_m$. Ponadto $\mathrm{NWD}(0, m) = m > 1$, więc $X = \{r_1, r_2, \ldots, r_s\}$ jest zbiorem wszystkich liczb ze zbioru $\mathbb{Z}_m$, które są względnie pierwsze z liczbą m. Ponadto $\mathrm{NWD}(a, m) = 1$, więc na mocy stwierdzenia 8.49, $\mathrm{NWD}(a \cdot r_i, m) = 1$ dla każdego $i = 1, \ldots, s$. Z twierdzenia o dzieleniu z resztą istnieją liczby całkowite $q_1, q_2, \ldots, q_s$ takie, że $a \cdot r_i = q_i \cdot m + [ar_i]_m$, skąd na mocy stwierdzenia 8.23 (v), $\mathrm{NWD}([ar_i]_m, m) = \mathrm{NWD}(ar_i, m)$, a zatem $\mathrm{NWD}([ar_i]_m, m) = 1$ dla każdego $i = 1, 2, \ldots, s$. Weźmy dowolne $i, j = 1, 2, \ldots, s$ takie, że $[ar_i]_m = [ar_j]_m$. Wtedy ze stwierdzenia 10.2, $ar_i \equiv ar_j \pmod{m}$. Stąd $r_i \equiv r_j \pmod{m}$ na mocy twierdzenia 10.6 (iii). Zatem ze stwierdzenia

10.2, $[r_i]_m = [r_j]_m$, ale $r_i, r_j \in \mathbb{Z}_m$, więc $r_i = r_j$, skąd $i = j$. To oznacza, że zbiór $\{[ar_1]_m, [ar_2]_m, \ldots [ar_s]_m\}$ ma dokładnie s-elementów. Dodatkowo, jak pokazaliśmy, ten zbiór jest podzbiorem s-elementowego zbioru X. Wobec tego

$$\{[ar_1]_m, [ar_2]_m, \ldots [ar_s]_m\} = \{r_1, r_2, \ldots, r_s\}.$$

Stąd $[ar_1]_m \cdot [ar_2]_m \cdot \ldots \cdot [ar_s]_m = r_1 \cdot r_2 \cdot \ldots \cdot r_s$, ale $ar_i \equiv [ar_i]_m \pmod{m}$ dla każdego $i = 1, 2, \ldots, s$, więc na mocy twierdzenia 10.5 (iv), $(ar_1) \cdot (ar_2) \cdot \ldots \cdot (ar_s) \equiv [ar_1]_m \cdot [ar_2]_m \cdot \ldots \cdot [ar_s]_m \pmod{m}$, czyli $a^s \cdot (r_1 \cdot r_2 \cdot \ldots \cdot r_s) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_s \pmod{m}$. Ponadto na mocy stwierdzenia 8.49 liczby $r_1 \cdot r_2 \cdot \ldots \cdot r_s$ i m są względnie pierwsze, więc na mocy twierdzenia 10.6 (iii), $a^s \equiv 1 \pmod{m}$, czyli $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Z twierdzenia Eulera łatwo wyprowadzić małe twierdzenie Fermata. Rzeczywiście, jeśli $a \in \mathbb{Z}$ i $p \in \mathbb{P}$, to na mocy stwierdzenia 9.13, $\mathrm{NWD}(a, p) = 1$ wtedy i tylko wtedy, gdy $p \nmid a$. Jeśli zatem $p \nmid a$, to z przykładu 10.12, $\varphi(p) = p - 1$ i z twierdzenia Eulera, $a^{p-1} \equiv 1 \pmod{p}$, skąd po pomnożeniu obu stron tej kongruencji przez a uzyskujemy, że $a^p \equiv a \pmod{p}$, czyli $p \mid a^p - a$. Dodatkowo, jeśli $p \mid a$, to $p \mid a^p$, więc $p \mid a^p - a$. Wobec tego $p \mid a^p - a$ dla każdego $a \in \mathbb{Z}$. Udowodniliśmy zatem następujące

Twierdzenie 10.14. *Dla dowolnej liczby całkowitej a niepodzielnej przez liczbę pierwszą p zachodzi wzór:*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{10.4}$$

Uwaga 10.15. Niech $m > 1$ będzie liczbą naturalną. Wtedy $\mathrm{NWD}(m, m) = \mathrm{NWD}(0, m) = m > 1$, więc

$$\{k \in \mathbb{N} : k \leqslant n \text{ i } \mathrm{NWD}(k, m) = 1\} = \mathbb{Z}_m^*,$$

gdzie

$$\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m : \mathrm{NWD}(k, m) = 1\}.$$

Zatem dla $m > 1$: $\varphi(m) = |\mathbb{Z}_m^*|$.

Twierdzenie 10.16. *Jeżeli liczby naturalne m i n są względnie pierwsze, to $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.*

Dowód. Jeśli $m = 1$ lub $n = 1$, to teza jest oczywista, bo $\varphi(1) = 1$. Niech dalej $m > 1$ i $n > 1$. Niech $F\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ będzie funkcją określoną wzorem

$$F(a) = ([a]_m, [a]_n). \tag{10.5}$$

Z twierdzenia chińskiego o resztach wynika, że funkcja F jest „na". Ponadto $|\mathbb{Z}_{mn}| = mn$ i $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$, więc ta funkcja jest bijekcją. Weźmy dowolne $a \in \mathbb{Z}_{mn}$. Jeżeli $\mathrm{NWD}(a, m) = \mathrm{NWD}(a, n) = 1$, to ze stwierdzenia 8.49, $\mathrm{NWD}(a, mn) = 1$. Na odwrót, jeśli $\mathrm{NWD}(a, mn) = 1$, to $\mathrm{NWD}(a, m) = \mathrm{NWD}(a, n) = 1$, bo $\mathrm{NWD}(a, m) \mid \mathrm{NWD}(a, mn)$ i $\mathrm{NWD}(a, m) \mid \mathrm{NWD}(a, mn)$. Wobec tego $a \in \mathbb{Z}^*_{mn}$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, m) = \mathrm{NWD}(a, n) = 1$. Ponadto na mocy stwierdzenia 8.23 (v), $\mathrm{NWD}(a, m) = \mathrm{NWD}([a]_m, m)$ i $\mathrm{NWD}(a, n) = \mathrm{NWD}([a]_n, n)$, więc $a \in \mathbb{Z}^*_{mn}$ wtedy i tylko wtedy, gdy $F(a) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$. Zatem zbiory $\mathbb{Z}^*_{mn}$ i $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$ są równoliczne. Stąd i z uwagi 10.15, $\varphi(mn) = |\mathbb{Z}^*_{mn}| = |\mathbb{Z}^*_m| \cdot |\mathbb{Z}^*_n| = \varphi(m) \cdot \varphi(n)$. □

Wniosek 10.17. *Jeżeli każde dwie liczby spośród liczb naturalnych $m_1, m_2, \ldots, m_s$ $(s \geqslant 2)$ są względnie pierwsze, to*

$$\varphi(m_1 \cdot m_2 \cdot \ldots \cdot m_s) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_s).$$

Dowód. Dla $s = 2$ teza wynika z twierdzenia 10.16. Załóżmy, że teza zachodzi dla pewnego naturalnego $s \geqslant 2$ i niech każde dwie spośród liczb $m_1, \ldots, m_s, m_{s+1} \in \mathbb{N}$ będą względnie pierwsze. Wtedy ze stwierdzenia 8.49 liczby m_{s+1} i $m_1 \cdot \ldots \cdot m_s$ są względnie pierwsze, więc z twierdzenia 10.16, $\varphi(m_1 \cdot \ldots \cdot m_s \cdot m_{s+1}) = \varphi(m_1 \cdot \ldots \cdot m_s) \cdot \varphi(m_{s+1})$. Ponadto z założenia indukcyjnego $\varphi(m_1 \cdot m_2 \cdot \ldots \cdot m_s) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_s)$, więc $\varphi(m_1 \cdot \ldots \cdot m_s \cdot m_{s+1}) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_s) \cdot \varphi(m_{s+1})$. Zatem teza zachodzi też dla liczby $s + 1$. Na mocy zasady indukcji mamy zatem, że teza zachodzi dla każdej liczby naturalnej $s \geqslant 2$. □

Twierdzenie 10.18. *Niech $p_1, p_2, \ldots, p_s$ będą różnymi liczbami pierwszymi i niech $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$. Wtedy zachodzi wzór:*

$$\varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1).$$

Dowód. Niech $p \in \mathbb{P}$ i $k \in \mathbb{N}$. Na mocy stwierdzenia 9.21 i uwagi 9.16 liczba całkowita a jest względnie pierwsza z liczbą p^k wtedy i tylko wtedy, gdy $p \nmid a$. Wobec tego $\varphi(p^k) = p^k - x$, gdzie x jest liczbą liczb naturalnych $\leqslant p^k$ podzielnych przez p. Ponieważ takie liczby są postaci pn dla $n = 1, \ldots, p^{k-1}$, więc $x = p^{k-1}$ i mamy, że $\varphi(p^k) = p^k - p^{k-1} = = p^{k-1}(p-1)$. Zatem nasze twierdzenie zachodzi dla $s = 1$.

Niech teraz $s \geqslant 2$. Wówczas na mocy stwierdzenia 9.21 i uwagi 9.16 każde dwie liczby spośród liczb $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ są względnie pierwsze. Zatem z pierwszej części naszego dowodu i z wniosku 10.17, $\varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1)$. □

Wniosek 10.19. *Dla dowolnej liczby naturalnej $n > 2$ liczba $\varphi(n)$ jest parzysta.*

Dowód. Jeśli $n > 2$ i n posiada nieparzysty dzielnik pierwszy p, to z twierdzenia 10.18 mamy, że wtedy $p - 1 \mid \varphi(n)$, a ponieważ liczba $p - 1$ jest parzysta, więc liczba $\varphi(n)$ też jest parzysta. Pozostaje zatem przypadek, gdy $n = 2^k$ dla pewnego $k \in \mathbb{N}$. Ponieważ $n > 2$, więc $k \geqslant 2$. Z twierdzenia 10.18, $\varphi(n) = 2^{k-1} \cdot (2-1) = = 2^{k-1}$, skąd $\varphi(n)$ jest parzyste, bo $k - 1 \geqslant 1$. □

Uwaga 10.20. Inny dowód wniosku 10.19 można uzyskać wprost z definicji fukcji Eulera wykorzystując to, że dla $n > 2$ zbiór A wszystkich liczb naturalnych $k \leqslant n$ względnie pierwszych z n jest sumą rozłączną dwóch równolicznych podzbiorów: $A_1 = \{k \in A : k < \frac{n}{2}\}$ i $A_2 = \{n - k : k \in A_1\}$.

Twierdzenie 10.21. *Niech $p_1, \ldots, p_s$ będą różnymi liczbami pierwszymi i niech $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$ oraz niech $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ i niech $\xi(m) = \mathrm{NWW}(p_1^{\alpha_1 - 1}(p_1 - 1), \ldots, p_s^{\alpha_s - 1}(p_s - 1))$. Wtedy dla każdej liczby całkowitej a względnie pierwszej z liczbą m zachodzi wzór:*

$$a^{\xi(m)} \equiv 1 \pmod{m}.$$

Dowód. Ponieważ liczby a i m są względnie pierwsze, więc względnie pierwsze są też liczby a i $p_i^{\alpha_i}$ dla $i = 1, \ldots, s$. Stąd i z twierdzenia Eulera i z twierdzenia 10.18 dla $m_i =$

$p_i^{\alpha_i-1}(p_i-1)$ mamy, że $a^{m_i} \equiv 1 \pmod{p_i^{\alpha_i}}$ przy $i = 1, \ldots, s$. Ponadto $m_i \mid \mathrm{NWW}(m_1, \ldots, m_s)$, więc z twierdzenia 10.5 (v), $a^{\xi(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$ dla każdego $i = 1, \ldots, s$. Zatem z twierdzenia 10.7, $a^{\xi(m)} \equiv 1 \pmod{m}$. □

Przykład 10.22. Niech $a \in \mathbb{Z}$ będzie takie, że $\mathrm{NWD}(a, 12) = 1$. Ponieważ $12 = 3 \cdot 2^2$, więc z twierdzenia 10.18, $\varphi(12) = 2 \cdot 2 = 4$, więc z twierdzenia Eulera $a^4 \equiv 1 \pmod{12}$, ale $\xi(12) = \mathrm{NWW}(2, 2) = 2$, więc z twierdzenia 10.21, $a^2 \equiv 1 \pmod{12}$.

Przykład 10.23. Niech a będzie nieparzystą liczbą całkowitą i niech $\alpha \geqslant 3$ będzie liczbą naturalną. Wtedy na mocy twierdzenia Eulera i twierdzenia 10.18 mamy, że $a^{2^{\alpha-1}} \equiv 1 \pmod{2^\alpha}$. Przez indukcję względem $\alpha \geqslant 3$ pokażemy, że $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$. Dla $\alpha = 3$ teza wynika z zadania 22.13. Przypuśćmy, że $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ dla pewnej liczby naturalnej $\alpha \geqslant 3$. Wtedy $a^{2^{\alpha-2}} = 1 + K \cdot 2^\alpha$ dla pewnego $K \in \mathbb{Z}$, skąd $a^{2^{\alpha-1}} = (1 + K \cdot 2^\alpha)^2 = 1 + K \cdot 2^{\alpha+1} + 2^{2\alpha}$, a ponieważ $2\alpha \geqslant \alpha + 1$, więc $a^{2^{\alpha-1}} \equiv 1 \pmod{2^{\alpha+1}}$. Zatem wtedy teza zachodzi też dla liczby $\alpha + 1$ i na mocy zasady indukcji $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ dla dowolnego $\alpha = 3, 4, \ldots$.

Teraz przez indukcję pokażemy, że $3^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$ dla dowolnego $\alpha = 4, 5, \ldots$. Dla $\alpha = 4$ teza zachodzi, bo wtedy $3^{2^{\alpha-3}} = 9$ i $1 + 2^{\alpha-1} = 9$. Przypuśćmy, że teza zachodzi dla pewnej liczby naturalnej $\alpha \geqslant 4$. Wtedy $3^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + L \cdot 2^\alpha$ dla pewnego $L \in \mathbb{Z}$. Stąd $3^{2^{\alpha-2}} = (1 + 2^{\alpha-1} + L \cdot 2^\alpha)^2 = (1 + 2^{\alpha-1})^2 + (1 + 2^{\alpha-1}) \cdot L \cdot 2^{\alpha+1} + L^2 \cdot 2^{2\alpha}$, więc $3^{2^{\alpha-2}} \equiv (1 + 2^{\alpha-1})^2 \pmod{2^{\alpha+1}}$. Ale $(1 + 2^{\alpha-1})^2 = 1 + 2^\alpha + 2^{2(\alpha-1)}$ i $2(\alpha - 1) \geqslant \alpha + 1$, gdyż $\alpha \geqslant 4$, więc $3^{2^{\alpha-2}} \equiv 1 + 2^\alpha \pmod{2^{\alpha+1}}$, co dowodzi naszej tezy dla liczby $\alpha + 1$.

Uwaga 10.24. W związku z twierdzeniami 10.13 i 10.21 można postawić dwa naturalne problemy związane z liczbą naturalną m:

1. Dla danej liczby całkowitej a względnie pierwszej z m wyznaczyć najmniejszą liczbę naturalną $w = w_m(a)$ taką, że $a^w \equiv 1 \pmod{m}$.

2. Obliczyć najmniejszą liczbę naturalną $\lambda(m)$ o tej własności, że $a^{\lambda(m)} \equiv 1 \pmod{m}$ dla każdej liczby całkowitej a względnie pierwszej z m.

Zauważmy, że na mocy twierdzenia 10.13 i zasady minimum istnieją $w_m(a)$ oraz $\lambda(m)$. Ponadto, jeżeli $b \in \mathbb{Z}$ i $b \equiv a \pmod{m}$, to $\mathrm{NWD}(b, m) = 1$ oraz $a^s \equiv b^s \pmod{m}$ dla każdego $s \in \mathbb{N}$, skąd wynika, że wtedy $w_m(b) = w_m(a)$.

Następujące stwierdzenie grupuje podstawowe własności funkcji λ i w_m.

Stwierdzenie 10.25. *Dla dowolnej liczby naturalnej $m > 1$ i dla dowolnej liczby całkowitej a względnie pierwszej z m oraz dla dowolnej liczby naturalnej k:*

(i) $a^k \equiv 1 \pmod{m} \iff w_m(a) \mid k$,

(ii) $w_m(a) \mid \lambda(m)$ *i* $w_m(a) \mid \varphi(m)$,

(iii) $c^k \equiv 1 \pmod{m}$ *dla każdej liczby całkowitej c względnie pierwszej z m wtedy i tylko wtedy, gdy* $\lambda(m) \mid k$,

(iv) $\lambda(m) \mid \varphi(m)$.

Dowód. (i). Niech $w = w_m(a)$ dzieli k. Wtedy $k = wn$ dla pewnego $n \in \mathbb{N}$. Ale $a^w \equiv 1 \pmod{m}$, więc po podniesieniu tej kongruencji stronami do potęgi n uzyskamy, że $a^k \equiv 1 \pmod{m}$. Na odwrót, przypuśćmy, że $a^k \equiv 1 \pmod{m}$. Z twierdzenia o dzieleniu z resztą wynika, że $k = qw + r$ dla pewnych $q, r \in \mathbb{N}_0$ takich, że $r < w$. Stąd i z pierwszej części dowodu, $1 \equiv a^k \equiv a^{qw} \cdot a^r \equiv a^r \pmod{m}$, czyli $a^r \equiv 1 \pmod{m}$. Z minimalności w wynika, że $r \notin \mathbb{N}$, więc $r = 0$ i $w \mid k$.

(ii). Wynika od razu z (i) oraz z definicji funkcji λ i z twierdzenia 10.13.

(iii). Niech $\lambda(m) \mid k$. Wtedy $k = n\lambda(m)$ dla pewnego $n \in \mathbb{N}$. Weźmy dowolne $c \in \mathbb{Z}$ takie, że $\mathrm{NWD}(c, m) = 1$. Wtedy $c^{\lambda(m)} \equiv 1 \pmod{m}$, więc po podniesieniu tej kongruencji stronami do potęgi n uzyskamy, że $c^k \equiv 1 \pmod{m}$. Na odwrót, przypuśćmy, że $c^k \equiv 1 \pmod{m}$ dla każdej liczby całkowitej c względnie pierwszej z m. Z twierdzenia o dzieleniu z resztą wynika, że $k = q\lambda(m) + r$ dla pewnych $q, r \in \mathbb{N}_0$ takich, że $r < \lambda(m)$. Stąd i z pierwszej części dowodu punktu (iii), $1 \equiv c^k \equiv c^{q\lambda(m)} \cdot c^r \equiv c^r \pmod{m}$, czyli $c^r \equiv 1 \pmod{m}$. Z określenia $\lambda(m)$ wynika zatem, że $r \notin \mathbb{N}$, więc $r = 0$ i $\lambda(m) \mid k$.

(iv). Wynika od razu z (iii) oraz z twierdzenia 10.13.

□

Twierdzenie 10.26. *Załóżmy, że $s \geqslant 2$ i liczby naturalne $m_1, m_2, \ldots, m_s$ są parami względnie pierwsze. Wówczas zachodzi wzór:*

$$\lambda(m_1 \cdot m_2 \cdot \ldots \cdot m_s) = \mathrm{NWW}(\lambda(m_1), \lambda(m_2), \ldots, \lambda(m_s)).$$

Dowód. Ze stwierdzenia 8.49 wynika, że liczba całkowita c jest względnie pierwsza z liczbą $m = m_1 \cdot m_2 \cdot \ldots \cdot m_s$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(c, m_i) = 1$ dla każdego $i = 1, 2, \ldots, s$. Oznaczmy $M = \mathrm{NWW}(\lambda(m_1), \lambda(m_2), \ldots, \lambda(m_s))$ i weźmy dowolne $c \in \mathbb{Z}$ takie, że $\mathrm{NWD}(c, m) = 1$. Wtedy $c^{\lambda(m_i)} \equiv 1 \pmod{m_i}$ oraz $\lambda(m_i) \mid M$ dla $i = 1, 2, \ldots, s$. Zatem $c^M \equiv 1 \pmod{m_i}$ dla $i = 1, 2, \ldots, s$ na mocy twierdzenia 10.5. Stąd i z twierdzenia 10.7 otrzymujemy, że $c^M \equiv 1 \pmod{m}$. Zatem $\lambda(m) \mid M$ na mocy stwierdzenia 10.25. Dalej, dla $i = 1, 2, \ldots, s$ mamy, że $m_i \mid m$, a ponieważ $c^{\lambda(m)} \equiv 1 \pmod{m}$, więc $c^{\lambda(m)} \equiv 1 \pmod{m_i}$ i wobec tego $\lambda(m_i) \mid \lambda(m)$ na mocy stwierdzenia 10.25. Stąd i z twierdzenia 8.36 wynika, że $M \mid \lambda(m)$. Ale pokazaliśmy też, że $\lambda(m) \mid M$, więc $\lambda(m) = M$, co kończy dowód. □

Z twierdzenia 10.26 uzyskujemy od razu następujący wniosek, który sprowadza problem obliczania $\lambda(m)$ do problemu obliczania $\lambda(p^k)$ dla $p \in \mathbb{P}$ i $k \in \mathbb{N}$.

Wniosek 10.27. *Niech $p_1, \ldots, p_s$ będą różnymi liczbami pierwszymi i niech $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$. Wówczas:*

$$\lambda(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = \mathrm{NWW}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})).$$

Twierdzenie 10.28. *Dla dowolnej liczby naturalnej $\alpha \geqslant 3$ mamy, że $\lambda(2^\alpha) = 2^{\alpha-2}$. Ponadto $\lambda(2) = 1$ i $\lambda(2^2) = 2$.*

Dowód. Oczywiście $\lambda(2) = 1$ i $\lambda(4) = 2$ na mocy stwierdzenia 10.25, gdyż $\varphi(2) = 1$ i $\varphi(4) = 2$. Z zadania 22.13 wynika, że $\lambda(8) = 2 = 2^{3-2}$. Niech $\alpha \geqslant 4$. Na mocy przykładu 10.23 i stwierdzenia 10.25 mamy, że $\lambda(2^\alpha) \mid 2^{\alpha-2}$. Zatem $\lambda(2^\alpha) = 2^k$ dla pewnej liczby naturalnej $k \leqslant \alpha - 2$. Dodatkowo z przykładu 10.23 uzyskujemy, że $3^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$, więc $k > \alpha - 3$. Wobec tego $k = \alpha - 2$. □

Wyznaczenie $\lambda(p^k)$ dla nieparzystych liczb pierwszych p jest bardziej skomplikowane. W podrozdziale 21.2 udowodnimy, że $\lambda(p^k) = \varphi(p^k) = p^{k-1}(p-1)$ dla liczb pierwszych $p > 2$ i dla każdego $k \in \mathbb{N}$. Zakończy to rozwiązanie Problemu 2 z uwagi 10.24 (por. uwaga 21.20).

Ćwiczenie 10.29. Udowodnij przez indukcję, że $2^{2\cdot 3^k} \equiv 1 + 3^{k+1} \pmod{3^{k+2}}$ dla każdego $k \in \mathbb{N}$ i wywnioskuj stąd, że $\lambda(3^\alpha) = \varphi(3^\alpha) = w_{3^\alpha}(2) = 2 \cdot 3^{\alpha-1}$ dla każdego $\alpha \in \mathbb{N}$.

Definicja 10.30. Każdą funkcję $f\colon \mathbb{Z} \to \mathbb{Z}$ postaci $f(x) = c_0 + c_1 x + \ldots + c_s x^s$, gdzie $s \in \mathbb{N}_0$ oraz $c_0, c_1, \ldots, c_s \in \mathbb{Z}$ są ustalone, nazywamy **wielomianem o współczynnikach całkowitych**.
Jeżeli $m \in \mathbb{N}$ i $a \in \mathbb{Z}$ są takie, że $f(a) \equiv 0 \pmod{m}$, to mówimy, że liczba a **spełnia kongruencję**

$$f(x) \equiv 0 \pmod{m}. \tag{10.6}$$

Jeżeli zaś $f(a) \not\equiv 0 \pmod{m}$, to mówimy, że liczba a **nie spełnia kongruencji** (10.6).

Jeżeli liczba całkowita a spełnia kongruencję (10.6) i $b \equiv a \pmod{m}$, to na mocy twierdzenia 10.5 (vi), liczba całkowita b też spełnia kongruencję (10.6). Z tego powodu **rozwiązaniem kongruencji** (10.6) nazywamy taką klasę abstrakcji $\{a+km : k \in \mathbb{Z}\}$ relacji przystawania modulo m o reprezentancie a, że $f(a) \equiv 0 \pmod{m}$. Ponieważ mamy dokładnie m takich klas, więc każda kongruencja postaci (10.6) posiada co najwyżej m rozwiązań. W praktyce, zamiast wypisywać klasy postaci $\{a + km : k \in \mathbb{Z}\}$ będziemy pisali po prostu, że $x \equiv a \pmod{m}$.

Termin **rozwiązać kongruencję** postaci (10.6) oznacza tyle samo co **wyznaczyć wszystkie klasy jej rozwiązań**. Czasami, szczególnie w przypadku układów kongruencji, termin **rozwiązać kongruencję** będzie oznaczał: wyznaczyć wszystkie liczby całkowite spełniające tę kongruencję.

Przykład 10.31. Zauważmy, że równanie $(2x-1)(3x-1) = 0$ nie posiada pierwiastków całkowitych. Pokażemy, że dla każdej liczby

naturalnej m kongruencja

$$(2x-1)(3x-1) \equiv 0 \pmod{m}$$

posiada rozwiązanie. Rzeczywiście, m można przedstawić w postaci $m = 2^k(2s-1)$ dla pewnych $k \in \mathbb{N}_0$ i $s \in \mathbb{N}$. Ponadto,

$$(2s-1)(3s-1) \equiv 0 \pmod{2s-1}$$

i na mocy lematu 10.8 istnieje $a \in \mathbb{Z}$ takie, że $3a \equiv 1 \pmod{2^k}$, skąd $(2a-1)(3a-1) \equiv 0 \pmod{2^k}$. Z twierdzenia chińskiego o resztach istnieje $r \in \mathbb{Z}$ takie, że $r \equiv s \pmod{2s-1}$ i $r \equiv a \pmod{2^k}$. Zatem z twierdzenia 10.5 (vi), $(2r-1)(3r-1) \equiv 0 \pmod{2s-1}$ oraz $(2r-1)(3s-1) \equiv 0 \pmod{2^k}$. Wobec tego na mocy twierdzenia 10.7 mamy, że $(2r-1)(3r-1) \equiv 0 \pmod{m}$.

Twierdzenie 10.32. (Lagrange'a). *Niech p będzie liczbą pierwszą, niech $n \in \mathbb{N}$ i niech $c_0, c_1, \ldots, c_n \in \mathbb{Z}$, przy czym $p \nmid c_n$. Wówczas kongruencja*

$$c_0 + c_1x + \ldots + c_nx^n \equiv 0 \pmod{p}$$

posiada co najwyżej n-rozwiązań.

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ mamy, że $p \nmid c_1$ i nasza kongruencja przybiera postać $c_1x + c_0 \equiv 0 \pmod{p}$. Jeżeli $a, b \in \mathbb{Z}$ i $c_1a + c_0 \equiv 0 \pmod{p}$ oraz $c_1b + c_0 \equiv 0 \pmod{p}$, to po odjęciu stronami tych kongruencji uzyskamy, że $c_1(a-b) \equiv 0 \pmod{p}$. Stąd na mocy twierdzenia 10.6 (iii), $a - b \equiv 0 \pmod{p}$, czyli $a \equiv b \pmod{p}$. Zatem nasza kongruencja posiada co najwyżej jedno rozwiązanie i teza zachodzi dla $n = 1$.

Przypuśćmy teraz, że teza zachodzi dla pewnej liczby naturalnej n i niech $c_0, c_1, \ldots, c_n, c_{n+1} \in \mathbb{Z}$ będą takie, że $p \nmid c_{n+1}$. Jeśli kongruencja $f(x) \equiv 0 \pmod{p}$, gdzie $f(x) = c_0 + c_1x + \ldots + c_nx^n + c_{n+1}x^{n+1}$, nie posiada rozwiązania, to teza zachodzi dla liczby $n+1$. Niech zatem istnieje $a \in \mathbb{Z}$ takie, że $f(a) \equiv 0 \pmod{p}$. Zauważmy, że

$$x^k - a^k = (x-a)(x^{k-1} + x^{k-2}a + \ldots + xa^{k-2} + a^{k-1})$$

dla $k = 2, 3, \ldots, n+1$, więc stąd $f(x) - f(a) = (x-a)g(x)$, gdzie $g(x) = c_1 + c_2(x+a) + \ldots + c_n(x^{n-1} + x^{n-2}a + \ldots + xa^{n-2} + a^{n-1}) + c_{n+1}(x^n + x^{n-1}a + \ldots + xa^{n-1} + a^n)$. Stąd $g(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} + c_{n+1}x^n$ dla pewnych $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}$. Jeśli teraz $b \in \mathbb{Z}$ i $b \not\equiv a \pmod{p}$ oraz $f(b) \equiv 0 \pmod{p}$, to $(b-a)g(b) \equiv 0 \pmod{p}$ i $p \nmid b-a$, więc $g(b) \equiv 0 \pmod{p}$ na mocy twierdzenia 10.6 (iii). Wynika stąd, że liczba rozwiązań kongruencji $f(x) \equiv 0 \pmod{p}$ różnych od rozwiązania $x \equiv a \pmod{p}$ jest nie większa niż liczba rozwiązań kongruencji $g(x) \equiv 0 \pmod{p}$, czyli na mocy założenia indukcyjnego, nie większa niż n. Wobec tego liczba rozwiązań kongruencji $f(x) \equiv 0 \pmod{p}$ jest nie większa niż $n+1$. Zatem teza zachodzi dla liczby $n+1$. □

Wniosek 10.33. *Dla dowolnej nieparzystej liczby pierwszej p kongruencje $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ oraz $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ posiadają dokładnie $\frac{p-1}{2}$ rozwiązań.*

Dowód. Z twierdzenia 10.14 wynika, że klasy $k+p\mathbb{Z}$ dla $k = 1, \ldots, p-1$ są rozwiązaniami kongruencji $x^{p-1} - 1 \equiv 0 \pmod{p}$. Ponadto $p \nmid 0^{p-1} - 1$, więc ta kongruencja posiada dokładnie $p-1$ rozwiązań. Niech teraz n i m oznaczają liczbę rozwiązań kongruencji $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ oraz $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ odpowiednio. Z twierdzenia 10.32 mamy, że $n \leqslant \frac{p-1}{2}$ i $m \leqslant \frac{p-1}{2}$. Przypuśćmy, że $m \neq \frac{p-1}{2}$ lub $n \neq \frac{p-1}{2}$. Wtedy $m+n < \frac{p-1}{2} + \frac{p-1}{2} = p-1$, czyli $m+n < p-1$. Dalej, dla każdego $k = 1, 2, \ldots, p-1$ mamy, że $p \mid k^{p-1} - 1$ oraz $k^{p-1} - 1 = (k^{\frac{p-1}{2}} - 1) \cdot (k^{\frac{p-1}{2}} + 1)$, więc $p \mid k^{\frac{p-1}{2}} - 1$ lub $p \mid k^{\frac{p-1}{2}} + 1$ ponieważ $p \in \mathbb{P}$ i liczba p jest nieparzysta. Ponadto, jeśli $k^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ i $k^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, to $1 \equiv -1 \pmod{p}$, skąd $p \mid 2$ i $p = 2$, co przeczy temu, że $p > 2$. Wobec tego każda z $p-1$ klas $1+p\mathbb{Z}, \ldots, (p-1)+p\mathbb{Z}$ jest rozwiązaniem dokładnie jednej z kongruencji $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ i $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, skąd wynika, że suma liczby rozwiązań tych kongruencji, czyli liczba $n+m$ jest nie mniejsza niż $p-1$, co prowadzi do sprzeczności i kończy dowód. □

Twierdzenie 10.34. (Wilsona). *Dla dowolnej liczby pierwszej p zachodzi wzór: $(p-1)! \equiv -1 \pmod{p}$.*

Dowód. Dla $p = 2$, $(p-1)! = 1! = 1 \equiv -1 \pmod 2$, więc teza zachodzi. Niech dalej $p > 2$. Wtedy p jest nieparzyste. Zauważmy, że wielomian $g(x) = (x-1)(x-2)\cdot\ldots\cdot(x-(p-1))$ można zapisać w postaci $g(x) = x^{p-1} + c_{p-2}x^{p-2} + \ldots + c_1x + c_0$, gdzie $c_0 = (-1)^{p-1}(p-1)! = (p-1)!$, gdyż $p-1$ jest liczbą parzystą. Ponadto $g(a) = 0$ dla każdego $a = 1, 2, \ldots, p-1$, skąd $g(a) \equiv 0 \pmod p$ dla $a = 1, 2, \ldots, p-1$. Z twierdzenia 10.14 mamy, że $a^{p-1} - 1 \equiv 0 \pmod p$ dla każdego $a = 1, 2, \ldots, p-1$. Stąd $g(a) - a^{p-1} + 1 \equiv 0 \pmod p$, czyli $c_{p-2}a^{p-2} + \ldots + c_1a + (p-1)! + 1 \equiv 0 \pmod p$ dla każdego $a = 1, 2, \ldots, p-1$. Stąd na mocy twierdzenia Lagrange'a, $p \mid c_i$ dla $i = 1, 2, \ldots, p-2$ oraz $p \mid (p-1)! + 1$, skąd $(p-1)! \equiv -1 \pmod p$. □

Ćwiczenie 10.35. Wykorzystując to, że $437 = 19 \cdot 23$ udowodnij opierając się na twierdzeniu Wilsona, że $18! \equiv -1 \pmod{437}$.

Przykład 10.36. Korzystając z twierdzenia Wilsona pokażemy, że dla dowolnej liczby pierwszej $p > 2$ zachodzi wzór:

$$1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p. \tag{10.7}$$

Dla $p = 3$ nasz wzór przybiera postać: $1^2 \equiv (-1)^2 \pmod 3$, a więc jest prawdziwy. Niech dalej $p > 3$. Ponieważ liczba p jest nieparzysta, więc liczby $p - (2k-1)$ dla $k = 1, \ldots, \frac{p-1}{2}$ są wszystkimi liczbami parzystymi zawartymi w ciągu $1, 2, \ldots, p-1$. Ponadto, $p - (2k-1) \equiv -(2k-1) \pmod p$ dla $k = 1, \ldots, \frac{p-1}{2}$, więc po pomnożeniu tych kongruencji stronami uzyskamy, że

$$2 \cdot 4 \cdot \ldots \cdot (p-1) \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdot \ldots \cdot (p-2) \pmod p.$$

Teraz mnożąc obie strony otrzymanej kongruencji przez $1 \cdot 3 \cdot \ldots \cdot (p-2)$ i uwzględniając twierdzenie Wilsona otrzymamy, że $-1 \equiv (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \pmod p$. Dalej, $-(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{2}}$, więc po pomnożeniu obu stron ostatniej kongruencji przez $(-1)^{\frac{p+1}{2}}$ uzyskamy wzór (10.7).

Wniosek 10.37. *Jeżeli p jest liczbą pierwszą i $p \equiv 1 \pmod 4$, to $p \mid a^2 + 1$ dla $a = (\frac{p-1}{2})!$.*

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Dla $i = 1, 2, \ldots, \frac{p-1}{2}$ mamy, że $p - i \equiv -i \pmod{p}$ oraz $p - i \geqslant p - \frac{p-1}{2} = \frac{p+1}{2} = \frac{p-1}{2} + 1$ i $p - i \leqslant p - 1$. Ponadto, jeśli $j \in \{\frac{p-1}{2} + 1, \ldots, p-1\}$, to $p - j \in \{1, \ldots, \frac{p-1}{2}\}$ oraz $j = p - (p - j)$. Wobec tego $(p-1)! = [1 \cdot (p-1)] \cdot [2 \cdot (p-2)] \cdot \ldots \cdot \left[\frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right)\right] \equiv$ $\equiv (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)^2 \pmod{p}$. Dodatkowo $p \equiv 1 \pmod{4}$, więc $\frac{p-1}{2}$ jest liczbą naturalną parzystą, a zatem $a^2 \equiv (p-1)! \pmod{p}$. Stąd i z twierdzenia Wilsona mamy tezę. □

Twierdzenie 10.38. (Fermata o dwóch kwadratach). *Każda liczba pierwsza p postaci $4k + 1$ jest sumą kwadratów dwóch liczb naturalnych.*

Dowód. Oczywiście liczba pierwsza nie jest kwadratem liczby całkowitej. Wystarczy zatem wykazać, że p jest sumą kwadratów dwóch liczb całkowitych. Ponieważ $p > 1$, więc istnieje największa liczba naturalna k taka, że $k \leqslant \sqrt{p}$. Wtedy $k + 1 > \sqrt{p}$, więc $(k+1)^2 > p$. Ponadto $k \neq \sqrt{p}$, więc $k < \sqrt{p}$, ale $p > 1$, więc $\sqrt{p} < p$, skąd $k < p$. Zatem $A = \{0, 1, \ldots, k\} \subseteq \mathbb{Z}_p$ i $|A| = k + 1$, skąd $|A \times A| = (k+1)^2 > p$.

Niech $a = (\frac{p-1}{2})!$. Wtedy $p \nmid a$ i z wniosku 10.37, $a^2 \equiv -1 \pmod{p}$. Rozważmy funkcję $f\colon A \times A \to \mathbb{Z}_p$ daną wzorem: $f(x, y) = [x - ay]_p$. Ponieważ $|A \times A| = (k+1)^2 > p = |\mathbb{Z}_p|$, więc f nie jest różnowartościowa. Zatem istnieją różne pary $(x_1, y_1), (x_2, y_2) \in A \times A$ takie, że $f(x_1, y_1) = f(x_2, y_2)$, czyli $[x_1 - ay_1]_p = [x_2 - ay_2]_p$. Stąd $x_1 - ay_1 \equiv x_2 - ay_2 \pmod{p}$, czyli $x \equiv ay \pmod{p}$, gdzie $x = x_1 - x_2$ i $y = y_1 - y_2$. Jeśli $x = 0$, to $ay \equiv 0 \pmod{p}$, więc z twierdzenia 10.6 (iii), $y \equiv 0 \pmod{p}$. Zatem $y_1 \equiv y_2 \pmod{p}$, skąd $[y_1]_p = [y_2]_p$. Ponadto $y_1, y_2 \in A \subseteq \mathbb{Z}_p$, więc $y_1 = y_2$. Wobec tego $x_1 = x_2$ i $y_1 = y_2$, co przeczy temu, że $(x_1, y_1) \neq (x_2, y_2)$. Zatem $x \neq 0$. Dalej, $x \equiv ay \pmod{p}$, więc po podniesieniu do kwadratu, $x^2 \equiv a^2 y^2 \pmod{p}$. Dodatkowo $a^2 \equiv -1 \pmod{p}$, więc $x^2 \equiv -y^2 \pmod{p}$. Zatem $p \mid x^2 + y^2$. Ponadto $x \neq 0$, więc $x^2 + y^2 = pm$ dla pewnego $m \in \mathbb{N}$. Dodatkowo $x_1, x_2, y_1, y_2 \in \{0, 1, \ldots, k\}$, więc $|x_1 - x_2|, |y_1 - y_2| \leqslant k < \sqrt{p}$, skąd $x^2, y^2 < p$, czyli $mp = x^2 + y^2 < 2p$. Zatem $mp < 2p$, skąd $m = 1$ i $p = x^2 + y^2$. □

Przykład 10.39. Udowodnimy, że jeżeli $p \in \mathbb{P}$ i $p \equiv 3 \pmod 4$, to dla dowolnych liczb całkowitych x i y zachodzi wzór:

$$p \mid x^2 + y^2 \iff (p \mid x \text{ i } p \mid y). \tag{10.8}$$

Implikacja $\Leftarrow$ jest oczywista. Dla dowodu implikacji przeciwnej załóżmy nie wprost, że $p \mid x^2 + y^2$, ale $p \nmid x$ lub $p \nmid y$ dla pewnych $x, y \in \mathbb{Z}$. Bez utraty ogólności możemy zakładać, że $p \nmid x$. Jeśli $p \mid y$, to $p \mid y^2$ i $p \mid x^2 + y^2$, skąd $p \mid x^2$, więc $p \mid x$, wbrew założeniu. Zatem $p \nmid y$ i $p \nmid x$, więc $y^{p-1} \equiv 1 \pmod p$ i $x^{p-1} \equiv 1 \pmod p$ na mocy twierdzenia 10.14. Dalej, ponieważ $p \equiv 3 \pmod 4$, więc liczba naturalna $\frac{p-1}{2}$ jest nieparzysta, skąd $(-1)^{\frac{p-1}{2}} = -1$. Ponadto $x^2 \equiv -y^2 \pmod p$, skąd po podniesieniu obu stron tej kongruencji do potęgi $\frac{p-1}{2}$ uzyskamy, że $x^{p-1} \equiv -y^{p-1} \pmod p$, ale $y^{p-1} \equiv 1 \pmod p$ i $x^{p-1} \equiv 1 \pmod p$, więc $1 \equiv -1 \pmod p$, czyli $p \mid 2$, co prowadzi do sprzeczności i kończy uzasadnienie wzoru (10.8).

Ćwiczenie 10.40. Udowodnij, że dla dowolnej liczby naturalnej n każdy dzielnik pierwszy liczby $[(n+1)!]^2 + 1$ przystaje do 1 modulo 4 i wyprowadź stąd, że liczb pierwszych postaci $4k+1$ jest nieskończenie wiele.

Ćwiczenie 10.41. Udowodnij, że dla dowolnej liczby naturalnej n pewien dzielnik pierwszy liczby $[(n+3)!]^2 + 3$ przystaje do 3 modulo 4 i wyprowadź stąd, że liczb pierwszych postaci $4k+3$ jest nieskończenie wiele.

Ćwiczenie 10.42. Niech a, b, c oraz d będą liczbami naturalnymi. Udowodnij, że liczba $a^{4b+d} - a^{4c+d}$ jest podzielna przez 240.

Ćwiczenie 10.43. Niech a, b, c będą liczbami całkowitymi takimi, że $a + b + c = 0$. Udowodnij, że $|a^{1999} + b^{1999} + c^{1999}|$ nie jest liczbą pierwszą.

Ćwiczenie 10.44. Niech a, b, c będą liczbami całkowitymi takimi, że $(a-b)(b-c)(c-a) = a + b + c$. Udowodnij, że $27 \mid a + b + c$.

Rozdział 11

Rozwiązywanie kongruencji

11.1 Uwagi ogólne

Niech m i n będą liczbami naturalnymi i niech f będzie wielomianem o współczynnikach całkowitych stopnia n. Przypomnijmy, że liczba całkowita a spełnia kongruencję

$$f(x) \equiv 0 \pmod{m}, \tag{11.1}$$

jeżeli $f(a) \equiv 0 \pmod{m}$. Wówczas na mocy twierdzenia 10.5 (vi) każda liczba całkowita b taka, że $b \equiv a \pmod{m}$ też spełnia tę kongruencję. Z tego powodu **rozwiązaniem kongruencji** (11.1) nazywamy każdą klasę abstrakcji

$$a + m\mathbb{Z} = \{a + km : k \in \mathbb{Z}\}$$

relacji przystawania według modułu m taką, że $f(a) \equiv 0 \pmod{m}$. W praktyce, rozwiązanie $a + m\mathbb{Z}$ zapisujemy wzorem: $x \equiv a \pmod{m}$. Stopień wielomianu f nazywamy **stopniem kongruencji** (11.1). Kongruencje stopnia pierwszego nazywamy też **kongruencjami liniowymi**, zaś kongruencje stopnia drugiego nazywamy **kongruencjami kwadratowymi**.

Z twierdzenia o dzieleniu z resztą wynika, że zbiór $\mathbb{Z}$ wszystkich liczb całkowitych jest sumą parami rozłącznych m -klas modulo m:

$$\mathbb{Z} = (0 + m\mathbb{Z}) \cup (1 + m\mathbb{Z}) \cup \ldots \cup ((m-1) + m\mathbb{Z}). \tag{11.2}$$

Z tego powodu dowolna kongruencja modulo m posiada co najwyżej m-rozwiązań. Termin **rozwiązać kongruencję** oznacza zatem: **wyznaczyć wszystkie klasy modulo m rozwiązań tej kongruencji**.

W procesie rozwiązywania kongruencji bardzo często zastępujemy kongruencję prostszą lub układem mniej złożonych kongruencji. W naturalny sposób powstaje wtedy problem zapisu klasy $a + d\mathbb{Z}$ przy pomocy klas $a + m\mathbb{Z}$, gdzie $d \in \mathbb{N}$ i $d \mid m$. Mówi o tym następujące

Stwierdzenie 11.1. *Niech d będzie naturalnym dzielnikiem liczby naturalnej m. Wówczas dla każdego $a \in \mathbb{Z}$ klasa $a + d\mathbb{Z}$ jest sumą $\frac{m}{d}$ parami rozłącznych klas modulo m:*

$$a + d\mathbb{Z} = (a + m\mathbb{Z}) \cup ((a + d) + m\mathbb{Z}) \cup \ldots \cup ((a + (m/d - 1) \cdot d) + m\mathbb{Z}).$$

Dowód. Weźmy dowolną liczbę całkowitą b należącą do prawej strony dowodzonego wzoru. Wtedy $b \in (a + id) + m\mathbb{Z}$ dla pewnego $i = 0, 1, \ldots, \frac{m}{d}$. Stąd $b \equiv a + id \pmod{m}$, a ponieważ $d \mid m$, więc z twierdzenia 10.6 (ii), $b \equiv a + id \pmod{d}$. Ponadto $a + id \equiv a \pmod{d}$, więc $b \equiv a \pmod{d}$, czyli $b \in a + d\mathbb{Z}$. Na odwrót, niech $b \in a + d\mathbb{Z}$. Wtedy $b \equiv a \pmod{d}$. Zatem $d \mid b - a$, skąd $b - a = kd$ dla pewnego $k \in \mathbb{Z}$. Z twierdzenia o dzieleniu z resztą $k = q \cdot \frac{m}{d} + r$ dla pewnych liczb całkowitych q i r takich, że $r \in \{0, 1, \ldots, \frac{m}{d} - 1\}$. Zatem $b - a = qm + rd$, skąd $b - (a + rd) = qm$, czyli $b \equiv a + rd \pmod{m}$, a więc $b \in (a + rd) + m\mathbb{Z}$. To kończy dowód naszego wzoru.

Pozostaje do wykazania, że klasy $(a + id) + m\mathbb{Z}$ oraz $(a + jd) + m\mathbb{Z}$ są różne dla wszystkich różnych $i, j \in \{0, 1, \ldots, \frac{m}{d} - 1\}$. Bez zmniejszania ogólności możemy zakładać, że $i < j$. Przypuśćmy, że $(a + id) + m\mathbb{Z} = (a + jd) + m\mathbb{Z}$. Wtedy $a + jd \equiv a + id \pmod{m}$, skąd $(j - i)d \equiv 0 \pmod{m}$ i z twierdzenia 10.6 (i), $j - i \equiv 0 \pmod{\frac{m}{d}}$, czyli $\frac{m}{d} | j - i$. Ponadto $0 < j - i < \frac{m}{d}$, więc mamy sprzeczność. □

Uwaga 11.2. W praktyce zamiast klasy $a + d\mathbb{Z}$ piszemy $x \equiv a \pmod{d}$ i dla wielokrotności m liczby d zapisujemy to przy pomocy wzoru: $x \equiv a, a + d, a + 2d, \ldots, a + (\frac{m}{d} - 1)d \pmod{m}$. Czasami mówi się, że stwierdzenie 11.1 podaje metodę podnoszenia rozwiązań kongruencji według modułu d do rozwiązań tej kongruencji według modułu m (oczywiście, gdy $d \mid m$).

Przykład 11.3. Na mocy stwierdzenia 11.1 mamy, że : $1 + 2\mathbb{Z} = (1+8\mathbb{Z}) \cup (3+8\mathbb{Z}) \cup (5+8\mathbb{Z}) \cup (7+8\mathbb{Z})$. Wobec tego $x \equiv 1 \pmod 2$ wtedy i tylko wtedy, gdy $x \equiv 1, 3, 5, 7 \pmod 8$.

Odnotujmy jeszcze kilka praktycznych faktów dotyczących rozwiązywania kongruencji. Pierwszy z nich wynika od razu z twierdzenia 10.6:

Twierdzenie 11.4. *Niech m i s będą liczbami naturalnymi i niech a będzie liczbą całkowitą względnie pierwszą z liczbą m. Wówczas dla dowolnej liczby całkowitej c następujące warunki są równoważne:*

(i) c spełnia kongruencję (11.1),

(ii) c spełnia kongruencję $sf(x) \equiv 0 \pmod{ms}$,

(iii) c spełnia kongruencję $af(x) \equiv 0 \pmod m$.

Przykład 11.5. Rozwiążemy kongruencję: $12x \equiv 15 \pmod{17}$. Możemy ją zapisać w postaci $3 \cdot (4x - 5) \equiv 0 \pmod{17}$. Ponieważ $\mathrm{NWD}(3, 17) = 1$, więc nasz problem sprowadza się do rozwiązania kongruencji $4x-5 \equiv 0 \pmod{17}$. Ponieważ $\mathrm{NWD}(4, 17) = 1$, więc zgodnie z twierdzeniem 11.4 mamy kongruencję $4\cdot(4x-5) \equiv 0 \pmod{17}$, którą możemy zapisać w postaci $16x \equiv 20 \pmod{17}$. Ponadto, $16 \equiv -1 \pmod{17}$ i $20 \equiv 3 \pmod{17}$, więc jest to równoważne kongruencji $-x \equiv 3 \pmod{17}$, ale $\mathrm{NWD}(-1, 17) = 1$, więc po pomnożeniu obu stron tej kongruencji przez (-1) uzyskujemy rozwiązanie: $x \equiv -3 \pmod{17}$, czyli $x \equiv 14 \pmod{17}$. Rozwiązaniem kongruencji $12x \equiv 15 \pmod{17}$ jest zatem klasa $14 + 17\mathbb{Z} = \{14 + 17k : k \in \mathbb{Z}\}$.

Definicja 11.6. Niech $m_1, m_2, \ldots, m_s$ będą liczbami naturalnymi i niech $f_1, f_2, \ldots, f_s$ będą wielomianami o współczynnikach całkowitych. Mówimy, że liczba całkowita a spełnia układ kongruencji:

$$\begin{cases} f_1(x) & \equiv 0 & \pmod{m_1} \\ f_2(x) & \equiv 0 & \pmod{m_2} \\ \vdots & \vdots & \vdots \\ f_s(x) & \equiv 0 & \pmod{m_s} \end{cases}, \tag{11.3}$$

jeśli $f_i(a) \equiv 0 \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, s$.

Uwaga 11.7. Przy oznaczeniach definicji 11.6 załóżmy, że $a, b \in \mathbb{Z}$ są takie, że $a \equiv b \pmod{\text{NWW}(m_1, m_2, \ldots, m_s)}$ i a spełnia układ kongruencji (11.3). Wtedy $f_i(a) \equiv 0 \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, m$, ale $m_i | \text{NWW}(m_1, m_2, \ldots, m_s)$, więc $a \equiv b \pmod{m_i}$, skąd na mocy twierdzenia 10.5 (vi), $f(b_i) \equiv 0 \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, m$. Wobec tego liczba b też spełnia układ kongruencji (11.3). Z tego powodu przez **rozwiązanie układu kongruencji** (11.3) będziemy rozumieli klasę abstrakcji przystawania modulo $\text{NWW}(m_1, m_2, \ldots, m_s)$, której każdy element spełnia ten układ kongruencji. Termin rozwiązać układ kongruencji oznacza zatem: wyznaczyć wszystkie jej rozwiązania w postaci klas modulo $\text{NWW}(m_1, m_2, \ldots, m_s)$.

Twierdzenie 11.8. *Niech $m_1, m_2, \ldots, m_s$ będą liczbami naturalnymi i niech f będzie wielomianem o współczynnikach całkowitych. Dla dowolnej liczby całkowitej a równoważne są warunki:*

(i) a spełnia układ kongruencji $\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \vdots \qquad \vdots \qquad\qquad \vdots \\ f(x) \equiv 0 \pmod{m_s} \end{cases}$,

(ii) a spełnia kongruencję $f(x) \equiv 0 \pmod{\text{NWW}(m_1, m_2, \ldots, m_s)}$.

Dowód. $(i) \Rightarrow (ii)$. Z założenia $f(a) \equiv 0 \pmod{m_i}$, skąd $m_i \mid f(a)$ dla każdego $i = 1, 2, \ldots, s$. Zatem z twierdzenia 8.36 mamy, że, $\text{NWW}(m_1, m_2, \ldots, m_s) \mid f(a)$, czyli

$$f(a) \equiv 0 \pmod{\text{NWW}(m_1, m_2, \ldots, m_s)}.$$

$(ii) \Rightarrow (i)$. Z założenia $f(a) \equiv 0 \pmod{\text{NWW}(m_1, m_2, \ldots, m_s)}$. Ponadto dla $i = 1, 2, \ldots, s$ mamy, że $m_i \mid \text{NWW}(m_1, m_2, \ldots, m_s)$, więc $f(a) \equiv 0 \pmod{m_i}$. □

Uwaga 11.9. Jak wiemy każda liczba naturalna $m > 1$ może być zapisana w postaci $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ dla pewnych różnych liczb pierwszych $p_1, p_2, \ldots, p_s$ i dla pewnych liczb naturalnych $\alpha_1, \alpha_2, \ldots, \alpha_s$. Ponieważ każde dwie spośród liczb $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ są względnie pierwsze, więc na mocy twierdzenia 11.8 dla każdego wielomianu f o współczynnikach całkowitych kongruencja $f(x) \equiv 0 \pmod{m}$ ma taki sam

zbiór rozwiązań jak układ kongruencji:

$$\begin{cases} f(x) & \equiv 0 & (\mathrm{mod}\ p_1^{\alpha_1}) \\ f(x) & \equiv 0 & (\mathrm{mod}\ p_2^{\alpha_2}) \\ \vdots & \vdots & \vdots \\ f(x) & \equiv 0 & (\mathrm{mod}\ p_s^{\alpha_s}) \end{cases}.$$

Ponadto, z twierdzenia chińskiego o resztach wynika, że jeżeli $f(a_i) \equiv \equiv 0 \pmod{p_i^{\alpha_i}}$ dla każdego $i = 1, 2, \ldots, s$, to istnieje dokładnie jedno modulo m całkowite r takie, że $r \equiv a_i \pmod{p_i^{\alpha_i}}$, skąd $f(r) \equiv 0 \pmod{p_i^{\alpha_i}}$ dla $i = 1, 2, \ldots, s$, czyli $r + m\mathbb{Z}$ jest rozwiązaniem kongruencji $f(x) \equiv 0 \pmod{m}$. Na odwrót, jeśli $a + m\mathbb{Z}$ jest rozwiązaniem kongruencji $f(x) \equiv 0 \pmod{m}$, to $f(a) \equiv 0 \pmod{m}$, więc z twierdzenia 11.8, $f_i(a) \equiv 0 \pmod{p_i^{\alpha_i}}$ dla każdego $i = 1, 2, \ldots, s$.

Wynika stąd prosty algorytm rozwiązywania kongruencji $f(x) \equiv 0 \pmod{m}$. Mianowicie, najpierw rozkładamy m na czynniki pierwsze: $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, a następnie dla $i = 1, 2, \ldots, s$ rozwiązujemy kongruencję $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$. Jeśli pewna z tych kongruencji nie posiada rozwiązania, to kongruencja $f(x) \equiv 0 \pmod{m}$ też nie posiada rozwiązania. W przeciwnym przypadku znajdujemy wszystkie rozwiązania kongruencji $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ dla $i = 1, 2, \ldots, s$ i następnie dla każdego ciągu $(a_1, a_2, \ldots, a_s)$ liczb całkowitych takich, że $f(a_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ konstruujemy za pomocą twierdzenia chińskiego o resztach liczbę całkowitą r taką, że $r \equiv a_i \pmod{p_i^{\alpha_i}}$ dla $i = 1, 2, \ldots, s$. Wtedy $r + m\mathbb{Z}$ jest rozwiązaniem kongruencji $f(x) \equiv \equiv 0 \pmod{m}$ i wszystkie rozwiązania tej kongruencji można uzyskać w ten sposób. W szczególności, jeśli M_i jest liczba rozwiązań kongruencji $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ dla $i = 1, 2, \ldots, s$, to kongruencja $f(x) \equiv 0 \pmod{m}$ posiada dokładnie $M_1 \cdot M_2 \cdot \ldots \cdot M_s$ rozwiązań.

W ten sposób problem rozwiązywania kongruencji, a także układów kongruencji sprowadza się do problemu rozwiązywania kongruencji modulo p^α dla $p \in \mathbb{P}$ i $\alpha \in \mathbb{N}$.

Przykład 11.10. Zilustrujemy prezentowaną wyżej teorię na przykładzie wyznaczenia wszystkich rozwiązań kongruencji:

$$2x^2 + 3x + 5 \equiv 0 \pmod{95}. \tag{11.4}$$

Rozkładamy 95 na czynniki pierwsze: $95 = 5 \cdot 19$. Następnie rozwiązujemy kongruencję:

$$2x^2 + 3x + 5 \equiv 0 \pmod 5. \tag{11.5}$$

Jest ona równoważna kongruencji $-3x^2 + 3x \equiv 0 \pmod 5$, czyli po skróceniu przez -3, kongruencji $x(x-1) \equiv 0 \pmod 5$, która posiada dokładnie dwa rozwiązania: $x \equiv 0 \pmod 5$ i $x \equiv 1 \pmod 5$, gdyż $5 \in \mathbb{P}$.

Teraz rozwiązujemy kongruencję:

$$2x^2 + 3x + 5 \equiv 0 \pmod{19}. \tag{11.6}$$

Ponieważ $3 \equiv -16 \pmod{19}$ i $5 \equiv -14 \pmod{19}$, więc $2x^2 - 16x - 14 \pmod{19}$ i po skróceniu przez 2 uzyskujemy kongruencję równoważną $x^2 - 8x - 7 \equiv 0 \pmod{19}$, którą można zapisać w postaci $(x-4)^2 - +16 - 7 \equiv 0 \pmod{19}$. Ponadto $1 - 16 - 7 = -23 \equiv -4 \pmod{19}$, więc mamy, że $(x-4)^2 - 4 \equiv 0 \pmod{19}$, a zatem $(x-4-2) \cdot (x - +4+2) \equiv 0 \pmod{19}$. Ponieważ $19 \in \mathbb{P}$, więc wszystkimi rozwiązaniami kongruencji (11.6) są $x \equiv 6 \pmod{19}$ i $x \equiv 2 \pmod{19}$.

Stąd na mocy uwagi 11.9 kongruencja (11.4) posiada dokładnie $2 \cdot 2 = 4$ rozwiązania. Wyznaczymy je w oparciu o twierdzenie chińskie o resztach.

Jeśli $x \equiv 0 \pmod 5$ i $x \equiv 2 \pmod{19}$, to $x = 2 + 19k$ dla $k \in \mathbb{Z}$ i dla $k = 2$ mamy, że $x = 40 \equiv 0 \pmod 5$, skąd $x \equiv 40 \pmod{95}$.

Jeśli $x \equiv 0 \pmod 5$ i $x \equiv 6 \pmod{19}$, to $x = 6 + 19k$ dla $k \in \mathbb{Z}$ i dla $k = 1$ mamy, że $x = 25 \equiv 0 \pmod 5$, skąd $x \equiv 25 \pmod{95}$.

Jeśli $x \equiv 1 \pmod 5$ i $x \equiv 2 \pmod{19}$, to $x = 2 + 19k$ dla $k \in \mathbb{Z}$ i dla $k = 1$ mamy, że $x = 21 \equiv 1 \pmod 5$, skąd $x \equiv 21 \pmod{95}$.

Jeśli $x \equiv 1 \pmod 5$ i $x \equiv 6 \pmod{19}$, to $x = 6 + 19k$ dla $k \in \mathbb{Z}$ i dla $k = 0$ mamy, że $x = 6 \equiv 1 \pmod 5$, skąd $x \equiv 6 \pmod{95}$.

Ostatecznie mamy, że $x \equiv 6, 21, 25, 40 \pmod{95}$.

Stwierdzenie 11.11. *Niech $m_1, m_2, \ldots, m_s$ będą liczbami naturalnymi i niech $a_1, a_2, \ldots, a_s$ będą liczbami całkowitymi. Układ kongruen-*

cji:

$$\begin{cases} x & \equiv a_1 & (\mathrm{mod}\ m_1) \\ x & \equiv a_2 & (\mathrm{mod}\ m_2) \\ \vdots & \vdots & \vdots \\ x & \equiv a_s & (\mathrm{mod}\ m_s) \end{cases}, \tag{11.7}$$

albo nie posiada rozwiązania albo posiada dokładnie jedno rozwiązanie.

Dowód. Oznaczmy $m = \mathrm{NWW}(m_1, \ldots, m_s)$. Załóżmy, że ten układ kongruencji posiada rozwiązanie $a + m\mathbb{Z}$. Niech $b + m\mathbb{Z}$ będzie rozwiązaniem układu (11.7). Wtedy dla każdego $i = 1, 2, \ldots, s$ mamy, że $a \equiv a_i \pmod{m_i}$ i $b \equiv a_i \pmod{m_i}$, skąd $a \equiv b \pmod{m_i}$. Wobec tego z twierdzenia 10.5, $a \equiv b \pmod{m}$, skąd $b + m\mathbb{Z} = a + m\mathbb{Z}$. □

Stwierdzenie 11.12. *Niech $p \in \mathbb{P}$, niech $a_1, a_2, \ldots, a_s \in \mathbb{Z}$ i niech $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_s$ będą liczbami naturalnymi. Układ kongruencji*

$$\begin{cases} x & \equiv a_1 & (\mathrm{mod}\ p^{\alpha_1}) \\ x & \equiv a_2 & (\mathrm{mod}\ p^{\alpha_2}) \\ \vdots & \vdots & \vdots \\ x & \equiv a_s & (\mathrm{mod}\ p^{\alpha_s}) \end{cases}, \tag{11.8}$$

posiada rozwiązanie wtedy i tylko wtedy, gdy $a_s \equiv a_i \pmod{p^{\alpha_i}}$ dla każdego $i = 1, 2, \ldots, s-1$. Jeśli ten warunek jest spełniony, to ten układ posiada dokładnie jedno rozwiązanie: $x \equiv a_s \pmod{p^{\alpha_s}}$.

Dowód. Z naszych założeń wynika, że $\mathrm{NWW}(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_s}) = p^{\alpha_s}$. Oznaczmy: $m = p^{\alpha_s}$. Załóżmy, że układ (11.8) posiada rozwiązanie $a + m\mathbb{Z}$. Wtedy $a \equiv a_i \pmod{p^{\alpha_i}}$ dla każdego $i = 1, 2, \ldots, s$. W szczególności $a \equiv a_s \pmod{m}$, więc $a + m\mathbb{Z} = a_s + m\mathbb{Z}$. Ponadto ponieważ $\alpha_s \geqslant \alpha_i$ dla $i = 1, 2, \ldots, s-1$, więc $a \equiv a_s \pmod{p^{\alpha_i}}$, skąd $a_s \equiv a_i \pmod{p^{\alpha_i}}$ dla każdego $i = 1, 2, \ldots, s$.

Na odwrót, niech $a_s \equiv a_i \pmod{p^{\alpha_i}}$ dla każdego $i = 1, 2, \ldots, s-1$. Wtedy oczywiście $a_s + m\mathbb{Z}$ jest rozwiązaniem układu (11.8). □

Twierdzenie 11.13. *Niech $s \geqslant 2$ i $m_1, m_2, \ldots, m_s$ będą liczbami naturalnymi oraz niech $a_1, a_2, \ldots, a_s$ będą liczbami całkowitymi. Układ*

kongruencji (11.7) *posiada rozwiązanie wtedy i tylko wtedy, gdy dla dowolnych różnych liczb* $i, j \in \{1, \ldots, s\}$ *spełniony jest warunek:*

$$\mathrm{NWD}(m_i, m_j) \mid a_i - a_j. \tag{11.9}$$

Dowód. Przypuśćmy, że istnieje $x \in \mathbb{Z}$ takie, że $x \equiv a_i \pmod{m_i}$ dla każdego $i = 1, \ldots, s$. Weźmy dowolne różne liczby $i, j \in \{1, \ldots, s\}$ i niech $d = \mathrm{NWD}(m_i, m_j)$. Ponieważ $d \mid m_i$ i $d \mid m_j$, więc $x \equiv a_i \pmod{d}$ oraz $x \equiv a_j \pmod{d}$, skąd $a_i \equiv a_j \pmod{d}$, czyli $d \mid a_i - a_j$.

Na odwrót, przypuśćmy, że dla dowolnych różnych liczb $i, j \in \in \{1, \ldots, s\}$ spełniony jest warunek (11.9). Wtedy istnieją różne liczby pierwsze $p_1, \ldots, p_n$ takie, że dla każdego $i = 1, \ldots, s$ istnieją nieujemne liczby całkowite $\alpha_{i1}, \ldots, \alpha_{in}$ takie, że $m_i = p_1^{\alpha_{i1}} \cdot \ldots \cdot p_n^{\alpha_{in}}$. Weźmy dowolne $k = 1, \ldots, n$ oraz dowolne różne liczby $i, j \in \{1, \ldots, s\}$. Wtedy z (11.9) na mocy twierdzenia 9.30 mamy, że $p_k^{min\{\alpha_{ik}, \alpha_{jk}\}} \mid a_i - a_j$. Wobec tego ze stwierdzenia 11.12 istnieje $x_k \in \mathbb{Z}$ takie, że $x_k \equiv a_i \pmod{p_k^{\alpha_{ik}}}$ dla każdego $i = 1, \ldots, s$. Niech $\beta_k = \max\{\alpha_{1k}, \ldots, \alpha_{sk}\}$ oraz $M = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$. Na mocy twierdzenia chińskiego o resztach istnieje $x \in \mathbb{Z}$ takie, że $x \equiv x_k \pmod{M}$ dla każdego $k = 1, \ldots, n$. Dalej, na mocy twierdzenia 9.32 mamy, że $M = \mathrm{NWW}(m_1, \ldots, m_s)$. Stąd $x \equiv x_k \pmod{m_i}$ dla każdego $i = 1, \ldots, s$ i dla każdego $k = 1, \ldots, n$. Ponadto $x_k \equiv a_i \pmod{p_k^{\alpha_{ik}}}$ oraz $p_k^{\alpha_{ik}} \mid m_i$, więc $x \equiv a_i \pmod{p_k^{\alpha_{ik}}}$ dla każdego $k = 1, \ldots, n$, skąd $x \equiv a_i \pmod{m_i}$ dla każdego $i = 1, \ldots, s$. Oznacza to, że układ kongruencji (11.7) posiada rozwiązanie. □

Przykład 11.14. Zastosujemy twierdzenie 11.13 do zbadania, czy ma rozwiązanie następujący układ kongruencji:

$$\begin{cases} x \equiv 1 \pmod{1111} \\ x \equiv 22 \pmod{22222} \\ x \equiv 444 \pmod{444444} \end{cases}.$$

Z cechy podzielności przez 11 wynika, że $11 \mid 1111$ oraz $11 \mid 444444$. Zatem $11 \mid \mathrm{NWD}(1111, 444444)$. Jeśli nasz układ ma rozwiązanie, to na mocy twierdzenia 11.13 będziemy mieli, że $11 \mid 444 - 1$, czyli $11 \mid 443$. Tymczasem $3 - 4 + 4 = 3$, więc $[443]_{11} = 3 \neq 0$, a zatem mamy sprzeczność. Wobec tego dany układ kongruencji nie posiada rozwiązania.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Ćwiczenie 11.15. Rozwiązać następujący układ kongruencji:

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 11 \pmod{14} \\ x \equiv 7 \pmod{30} \end{cases}.$$

Przykład 11.16. Rozwiążemy następujący układ kongruencji:

$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{15} \end{cases}.$$

Ponieważ $6 = 2 \cdot 3$, $8 = 2^3$ i $15 = 3 \cdot 5$, więc $\mathrm{NWW}(6, 8, 15) = 2^3 \cdot \cdot 3 \cdot 5 = 120$. Ponadto na mocy uwagi 11.9 nasz układ jest równoważny układowi:

$$\begin{cases} x \equiv 5 \pmod{2} \\ x \equiv 5 \pmod{3} \\ x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}.$$

Na mocy stwierdzenia 11.12 ten ostatni układ jest równoważny układowi:

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}.$$

Z kolei ten układ można na mocy uwagi 11.9 zapisać w postaci:

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{15} \end{cases}.$$

Zgodnie z metodą podaną w dowodzie twierdzenia chińskiego o resztach rozwiązanie tego układu $r + 120\mathbb{Z}$ znajdziemy ze wzoru:

$$r = 15x_1 \cdot 3 + 8x_2 \cdot 2,$$

gdzie $15x_1 \equiv 1 \pmod{8}$ oraz $8x_2 \equiv 1 \pmod{15}$. Stąd mamy, że $-x_1 \equiv \equiv 1 \pmod{8}$, czyli $x_1 \equiv -1 \pmod{8}$ i można obrać $x_1 = -1$ oraz

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$16x_2 \equiv 2 \pmod{15}$, czyli $x_2 \equiv 2 \pmod{15}$ i wystarczy przyjąć $x_2 = 2$. Stąd $r = 15 \cdot (-1) \cdot 3 + 8 \cdot 2 \cdot 2 = -13$, ale $-13 \equiv 107 \pmod{120}$, więc rozwiązaniem naszego układu jest klasa $107 + 120\mathbb{Z}$, czyli $x \equiv 107 \pmod{120}$.

Przykład 11.17. Rozwiążemy następujący układ kongruencji:

$$\begin{cases} x \equiv 31 \pmod{63} \\ x \equiv 58 \pmod{99} \\ x \equiv 47 \pmod{55} \end{cases}.$$

Ponieważ $63 = 3^2 \cdot 7$, $99 = 3^2 \cdot 11$ i $55 = 5 \cdot 11$, więc $\mathrm{NWW}(63, 99, 55) = 3^2 \cdot 5 \cdot 7 \cdot 11 = 3465$. Ponadto na mocy uwagi 11.9 nasz układ jest równoważny układowi:

$$\begin{cases} x \equiv 31 \pmod{9} \\ x \equiv 31 \pmod{7} \\ x \equiv 58 \pmod{9} \\ x \equiv 58 \pmod{11} \\ x \equiv 47 \pmod{5} \\ x \equiv 47 \pmod{11} \end{cases}.$$

Na mocy stwierdzenia 11.12 ten ostatni układ jest równoważny układowi:

$$\begin{cases} x \equiv 4 \pmod{9} \\ x \equiv 3 \pmod{7} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{11} \end{cases}.$$

Zgodnie z metodą podaną w dowodzie twierdzenia chińskiego o resztach rozwiązanie tego układu $r + 3465\mathbb{Z}$ znajdziemy ze wzoru:

$$r = 7 \cdot 5 \cdot 11 \cdot x_1 \cdot 4 + 9 \cdot 5 \cdot 11 \cdot x_2 \cdot 3 + 9 \cdot 7 \cdot 11 \cdot x_3 \cdot 2 + 9 \cdot 7 \cdot 5 \cdot x_4 \cdot 3,$$

gdzie $7 \cdot 5 \cdot 11 \cdot x_1 \equiv 1 \pmod{9}$, $9 \cdot 5 \cdot 11 \cdot x_2 \equiv 1 \pmod{7}$, $9 \cdot 7 \cdot 11 \cdot x_3 \equiv 1 \pmod{5}$ i $9 \cdot 7 \cdot 5 \cdot x_4 \equiv 1 \pmod{11}$. Proste obliczenia pozwalają na aby wykazać, ze można obrać następujące wartości: $x_1 = 4$, $x_2 = 3$, $x_3 = 2$ i $x_4 = -3$, co daje nam $r = 10552 \equiv 157 \pmod{3465}$. Wobec tego ostatecznie $x \equiv 157 \pmod{3465}$.

11.2 Kongruencje liniowe

Ogólna postać kongruencji liniowej:

$$ax \equiv b \pmod{m}, \tag{11.10}$$

gdzie $a, b \in \mathbb{Z}$, $a \neq 0$ i $m \in \mathbb{N}$.

Twierdzenie 11.18. *Kongruencja liniowa* (11.10) *posiada rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(a, m) \mid b$. *Jeżeli ten warunek jest spełniony, to kongruencja* (11.10) *ma dokładnie* $\mathrm{NWD}(a, m)$ *rozwiązań. Dokładniej, jeżeli* $ax_0 \equiv b \pmod{m}$ *dla pewnego* $x_0 \in \mathbb{Z}$, *to wszystkimi rozwiązaniami kongruencji* (11.10) *są klasy:*

$$x_0 + m\mathbb{Z}, (x_0 + m_1) + m\mathbb{Z}, (x_0 + 2m_1) + m\mathbb{Z}, \ldots, (x_0 + (d-1)m_1) + m\mathbb{Z},$$

gdzie $d = \mathrm{NWD}(a, m)$ *i* $m_1 = \frac{m}{d}$.

Dowód. Przypuśćmy, że kongruencja (11.10) ma rozwiązanie $r + m\mathbb{Z}$. Wtedy $ar \equiv b \pmod{m}$, więc $m \mid ar - b$, czyli $ar - b = km$ dla pewnego $k \in \mathbb{Z}$. Dalej, $d \mid a$ i $d \mid m$, więc stąd $d \mid b$.

Na odwrót. Załóżmy, że $d \mid b$. Wtedy $a = da_1$, $b = db_1$ i $m = dm_1$ dla pewnych liczb całkowitych a_1 i b_1 oraz dla pewnego $m_1 \in \mathbb{N}$, przy czym na mocy twierdzenia 8.32, $\mathrm{NWD}(a_1, m_1) = 1$. Kongruencja (11.10) ma zatem postać $da_1x \equiv db_1 \pmod{dm_1}$, więc na mocy twierdzenia 11.4 (ii), liczba całkowita spełnia ją wtedy i tylko wtedy, gdy ta liczba spełnia kongruencję $a_1x \equiv b_1 \pmod{m_1}$. Z lematu 10.8 ta ostatnia kongruencja posiada dokładnie jedno rozwiązanie $x_0 + m_1\mathbb{Z}$ i stąd na mocy stwierdzenia 11.1 kongruencja (11.10) posiada dokładnie d rozwiązań, przy czym są to klasy: $x_0 + m\mathbb{Z}, (x_0 + m_1) + m\mathbb{Z}, (x_0 + 2m_1) + m\mathbb{Z}, \ldots, (x_0 + (d-1)m_1) + m\mathbb{Z}$. □

Ćwiczenie 11.19. Wiedząc, że $69 \cdot 29 \equiv 192 \pmod{201}$ wyznacz wszystkie rozwiązania kongruencji $69x \equiv 192 \pmod{201}$.

Przykład 11.20. Rozwiążemy kongruencję liniową:

$$88x \equiv 324 \pmod{404}.$$

Z algorytm Euklidesa mamy, że $\mathrm{NWD}(88, 404) = \mathrm{NWD}(36, 88) = \mathrm{NWD}(36, 16) = \mathrm{NWD}(16, 4) = 4$ i $324 : 4 = 81$. Zatem na mocy twierdzenia 11.18 ta kongruencja posiada dokładnie 4 rozwiązania. Możemy dokonać w niej skrócenia przez 4 i uzyskamy kongruencję

$$22x \equiv 81 \pmod{101}.$$

Zapiszmy kolejne dzielenia z resztą w algorytmie Euklidesa obliczania $\mathrm{NWD}(22, 101)$:

$$\begin{aligned} 101 &= 5 \cdot 22 - 9 \\ 22 &= 2 \cdot 9 + 4 \\ 9 &= 2 \cdot 4 + 1 \end{aligned} \quad . \tag{11.11}$$

Teraz kolejno przedstawiamy reszty w postaci $22x + 101y$: $9 = 22 \cdot 5 + 101 \cdot (-1)$, $4 = 22 \cdot 1 + 9 \cdot (-2) = 22 \cdot 1 + [22 \cdot 5 + 101 \cdot (-1)] \cdot (-2) = 22 \cdot (-9) + 101 \cdot 2$, $1 = 9 \cdot 1 + 4 \cdot (-2) = 22 \cdot 5 + 101 \cdot (-1) + [22 \cdot (-9) + 101 \cdot 2] \cdot (-2) = 22 \cdot 23 + 101 \cdot (-5)$. Wobec tego $22 \cdot 23 \equiv 1 \pmod{101}$. Ponadto $81 \equiv -20 \pmod{101}$, więc $22 \cdot (23 \cdot (-20)) \equiv 81 \pmod{101}$, czyli $22 \cdot 45 \equiv 81 \pmod{101}$.

Ten sam wynik możemy uzyskać inaczej wykorzystując to, że kongruencja $22x \equiv 81 \pmod{101}$ posiada dokładnie jedno rozwiązanie. Ponieważ $81 \equiv -20 \pmod{101}$, więc $22x \equiv -20 \pmod{101}$ i po skróceniu przez 2, $11x \equiv -10 \pmod{101}$. Teraz po pomnożeniu przez 10 i uwzględnieniu tego, że $110 \equiv 9 \pmod{101}$ i $-100 \equiv 1 \pmod{101}$ otrzymujemy, że $9x \equiv 1 \pmod{101}$. Dalej, $11x \equiv -10 \pmod{101}$, więc po odjęciu stronami dostajemy, że $2x \equiv -11 \pmod{101}$, czyli $2x \equiv 90 \pmod{101}$, skąd $x \equiv 45 \pmod{101}$.

Teraz z twierdzenia 11.18 mamy, że $x \equiv 45, 45+101, 45+2\cdot 101, 45+3 \cdot 101 \pmod{404}$, czyli $x \equiv 45, 146, 247, 348 \pmod{404}$. Zatem wszystkimi rozwiązaniami naszej kongruencji są klasy:
$45 + 404\mathbb{Z}, 146 + 404\mathbb{Z}, 247 + 404\mathbb{Z}, 348 + 404\mathbb{Z}$.

Ćwiczenie 11.21. Udowodnij, że wszystkimi rozwiązaniami kongruencji $276x \equiv 188 \pmod{952}$ są $x \equiv 149, 387, 625, 863 \pmod{952}$.

Przykład 11.22. Dla dowolnych $a_1, a_2, a_3 \in \mathbb{Z}$ wyznaczymy wszystkie liczby całkowite x takie, że $x \equiv a_1 \pmod 4$ i $x \equiv a_2 \pmod 5$

i $x \equiv a_3 \pmod 7$. Ponieważ liczby 4, 5 i 7 są parami względnie pierwsze i $4 \cdot 5 \cdot 7 = 140$, więc dowodu twierdzenia chińskiego o resztach uzyskujemy, że $x \equiv r \pmod{140}$, gdzie $r = 35x_1a_1 + 28x_2a_2 + 20x_3a_3$ oraz $35x_1 \equiv 1 \pmod 4$ i $28x_2 \equiv 1 \pmod 5$ i $20x_3 \equiv 1 \pmod 7$. Wobec tego $-x_1 \equiv 1 \pmod 4$, $-2x_2 \equiv -4 \pmod 5$ i $-x_3 \equiv 1 \pmod 7$, czyli $x_1 \equiv -1 \pmod 4$, $x_2 \equiv 2 \pmod 5$ i $x_3 \equiv -1 \pmod 7$. Możemy zatem przyjąć $x_1 = x_3 = -1$ i $x_2 = 2$. Wtedy $r = -35a_1 + 56a_2 - 20a_3$ i $x = 140k + r$ dla $k \in \mathbb{Z}$.

Ćwiczenie 11.23. Niech $a_1, a_2 \in \mathbb{Z}$. Wyznaczyć wszystkie liczby całkowite x takie, że $x \equiv a_1 \pmod{13}$ i $x \equiv a_2 \pmod{17}$.

Rozdział 12

Kongruencje kwadratowe

12.1 Zagadnienia wstępne

Kongruencją kwadratową nazywamy każdą kongruencję postaci:

$$ax^2 + bx + c \equiv 0 \pmod{m}, \tag{12.1}$$

gdzie $a, b, c \in \mathbb{Z}$, $a \neq 0$ oraz $m \in \mathbb{N}$ i $m > 1$. Z twierdzenia o jednoznaczności rozkładu mamy, że $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ dla pewnych różnych liczb pierwszych $p_1, \ldots, p_s$ i dla pewnych $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$. Zatem na mocy uwagi 11.9 kongruencja (12.1) jest równoważna następującemu układowi kongruencji:

$$\begin{cases} ax^2 + bx + c \equiv 0 \pmod{p_1^{\alpha_1}} \\ ax^2 + bx + c \equiv 0 \pmod{p_2^{\alpha_2}} \\ \qquad\qquad \vdots \qquad\qquad \vdots \\ ax^2 + bx + c \equiv 0 \pmod{p_s^{\alpha_s}} \end{cases}.$$

Daje to redukcję problemu rozwiązywania kongruencji (12.1) do przypadku, gdy $m = p^k$, gdzie $p \in \mathbb{P}$ oraz $k \in \mathbb{N}$.

Ustalmy liczby całkowite a, b, c takie, że $a \neq 0$ oraz liczbę pierwszą p i liczbę naturalną k. Zajmiemy się teraz kongruencją postaci:

$$ax^2 + bx + c \equiv 0 \pmod{p^k}. \tag{12.2}$$

Pochodną funkcji kwadratowej $f(x) = ax^2+bx+c$ nazywamy funkcję $f'(x) = 2ax + b$. Zauważmy, że dla każdego $x_0 \in \mathbb{Z}$ zachodzi wzór:

$$f(x) = f(x_0) + f'(x_0) \cdot (x - x_0) + a(x - x_0)^2. \tag{12.3}$$

Rzeczywiście, $f(x)-f(x_0) = a(x^2-x_0^2)+b(x-x_0) = (x-x_0)\cdot[a(x-x_0)+ +b]$ oraz $f'(x_0)\cdot(x-x_0)+a(x-x_0)^2 = (x-x_0)\cdot[(2ax_0+b)+a(x-x_0)] = = (x - x_0) \cdot [a(x - x_0) + b]$.

Zauważmy, że jeżeli $x_1 + p^{k+1}\mathbb{Z}$ jest rozwiązaniem kongruencji $f(x) \equiv 0 \pmod{p^{k+1}}$, to $x_1 + p^{k+1}\mathbb{Z}$ jest też rozwiązaniem kongruencji $f(x) \equiv 0 \pmod{p^k}$. Dodatkowo, jeśli $x_0, x_1 \in \mathbb{Z}$ są takie, że $x_1 \equiv x_0 \pmod{p^k}$ i $f(x_0) \equiv 0 \pmod{p^k}$, to ze wzoru (12.3) i tego, że $2k \geqslant k+1$ wynika, że

$$f(x_1) \equiv 0 \pmod{p^{k+1}} \iff f(x_0)+(x_1-x_0)f'(x_0) \equiv 0 \pmod{p^{k+1}}.$$

W ten sposób udowodniliśmy następujący:

Lemat 12.1. *Niech $f(x)$ będzie funkcją kwadratową o współczynnikach całkowitych, niech $p \in \mathbb{P}$, $k \in \mathbb{N}$ oraz niech $x_1 \in \mathbb{Z}$. Wówczas $x_1 + p^{k+1}\mathbb{Z}$ jest rozwiązaniem kongruencji $f(x) \equiv 0 \pmod{p^{k+1}}$ wtedy i tylko wtedy, gdy istnieje $x_0 \in \mathbb{Z}$ takie, że $x_1 \equiv x_0 \pmod{p^k}$, $x_0 + p^k\mathbb{Z}$ jest rozwiązaniem kongruencji $f(x) \equiv 0 \pmod{p^k}$ oraz $f(x_0) + (x_1 - x_0)f'(x_0) \equiv 0 \pmod{p^{k+1}}$.*

Wprowadzamy oznaczenia:

$$U_k = \{u \in \mathbb{Z}_{p^k} : f(u) \equiv 0 \pmod{p^k} \text{ i } p \nmid f'(u)\},$$

$$V_k = \{v \in \mathbb{Z}_{p^k} : f(v) \equiv 0 \pmod{p^k} \text{ oraz } p \mid f'(v) \text{ i } p^{k+1} \mid f(v)\},$$

$$W_k = \{v \in \mathbb{Z}_{p^k} : f(v) \equiv 0 \pmod{p^k} \text{ oraz } p \mid f'(v) \text{ i } p^{k+1} \nmid f(v)\}.$$

Następujące twierdzenie sprowadza w sposób rekurencyjny problem rozwiązywania kongruencji kwadratowych $f(x) \equiv 0 \pmod{p^n}$ dla $n \in \mathbb{N}$ do przypadku, gdy $n = 1$, to znaczy do problemu rozwiązywania kongruencji $f(x) \equiv 0 \pmod{p}$. Mianowicie, z twierdzenia 11.18 zastosowanego dla $m = p^{k+1}$ oraz $a = f'(u)$, gdzie $u \in U_k$ oraz z lematu 12.1 i ze stwierdzenia 11.1 dostajemy:

Twierdzenie 12.2. *Niech $f(x)$ będzie funkcją kwadratową o współczynnikach całkowitych oraz niech $p \in \mathbb{P}$ i $k \in \mathbb{N}$. Kongruencja $f(x) \equiv 0 \pmod{p^{k+1}}$ ma rozwiązanie wtedy i tylko wtedy, gdy zbiór $U_k \cup V_k$ jest niepusty. Ponadto dla każdego $u \in U_k$ istnieje dokładnie jedno $u_1 \in \mathbb{Z}_{p^{k+1}}$ takie, że $u_1 \equiv u \pmod{p^k}$ i $f(u_1) \equiv 0 \pmod{p^{k+1}}$, przy czym $f(u) + (u_1 - u)f'(u) \equiv 0 \pmod{p^{k+1}}$. Natomiast dla każdego $v \in V_k$ istnieje dokładnie p elementów $v_1 \in \mathbb{Z}_{p^{k+1}}$ takich, że $v_1 \equiv v \pmod{p^k}$ oraz $f(v_1) \equiv 0 \pmod{p^{k+1}}$ i są nimi: $v, v + p^k, \ldots, v + (p-1)p^k \in \mathbb{Z}_{p^{k+1}}$. W szczególności, liczba rozwiązań tej kongruencji jest równa $|U_k| + p|V_k|$ oraz $|U_k| = |U_1|$.*

Przykład 12.3. Zilustrujemy twierdzenie 12.2 rozwiązując kongruencję $x^2 + 8x + 7 \equiv 0 \pmod{3^3}$. W tym celu rozwiążemy najpierw kongruencję $x^2 + 8x + 7 \equiv 0 \pmod{3}$. Zauważmy, że jest ona równoważna kongruencji $x^2 + 2x + 1 \equiv (x+1)^2 \equiv 0 \pmod{3}$, skąd $x \equiv 2 \pmod{3}$. Ponadto $f'(x) = 2x + 8$, więc $3 \mid f'(2)$ oraz $f(2) = 27 \equiv 0 \pmod{3^2}$. Stąd $U_1 = \emptyset$, $V_1 = \{2\}$. Na mocy twierdzenia 12.2, wszystkimi rozwiązaniami kongruencji $x^2 + 8x + 7 \equiv 0 \pmod{3^2}$ są $x \equiv 2, 5, 8 \pmod{3^2}$. Ponieważ $3 \mid f'(2)$, $3 \mid f'(5)$, $3 \mid f'(8)$ oraz $f(2) \equiv 0 \pmod{3^3}$, $f(5) \equiv 18 \pmod{3^3}$, $f(8) \equiv 0 \pmod{3^3}$, więc $U_2 = \emptyset$, $V_2 = \{2, 8\}$. Zatem, ponownie z twierdzenia 12.2, wszystkimi rozwiązaniami kongruencji $x^2 + 8x + 7 \equiv 0 \pmod{3^3}$ są klasy: $2 + 3^3\mathbb{Z}$, $11 + 3^3\mathbb{Z}$, $20 + 3^3\mathbb{Z}$, $8 + 3^3\mathbb{Z}$, $17 + 3^3\mathbb{Z}$, $26 + 3^3\mathbb{Z}$.

Ćwiczenie 12.4. Rozwiąż kongruencję $x^2 + 6x + 14 \equiv 0 \pmod{125}$.

Wykorzystując standardowe rozumowanie indukcyjne oparte na twierdzeniu 12.2 uzyskujemy następujące wnioski:

Wniosek 12.5. *Niech $f(x)$ będzie funkcją kwadratową o współczynnikach całkowitych i niech $p \in \mathbb{P}$. Jeśli nie istnieje liczba całkowita u taka, że $p \mid f(u)$ i $p \mid f'(u)$, to dla każdego $k \in \mathbb{N}$ liczba rozwiązań kongruencji $f(x) \equiv 0 \pmod{p^k}$ jest równa liczbie rozwiązań kongruencji $f(x) \equiv 0 \pmod{p}$.*

Wniosek 12.6. *Niech $f(x)$ będzie funkcją kwadratową o współczynnikach całkowitych i niech $p \in \mathbb{P}$. Wówczas $|U_k| = |U_1|$ dla dowolnego*

$k \in \mathbb{N}$. Ponadto każde $u_k \in U_k$ może być wyznaczone z zależności rekurencyjnej: $f(u_{k-1}) + (u_k - u_{k-1})f'(u_1) \equiv 0 \pmod{p^k}$ dla dokładnie jednego $u_1 \in U_1$.

Pokażemy, że rozwiązując kongruencję (12.2) można ograniczyć się do przypadku, gdy $p \nmid a$. Rzeczywiście, jeżeli $p \mid a$, to $a = p^r a_1$ dla pewnych $r \in \mathbb{N}$, $a_1 \in \mathbb{Z}$, $p \nmid a_1$. Z twierdzenia 11.4 (ii) kongruencja (12.2) jest równoważna kongruencji $p^{2r}a_1x^2 + p^r bx + p^r c \equiv 0 \pmod{p^{k+r}}$, która z kolei jest równoważna układowi kongruencji:

$$\begin{cases} a_1y^2 + by + p^r c \equiv 0 & \pmod{p^{k+r}} \\ p^r x \equiv y & \pmod{p^{k+r}} \end{cases}.$$

Wobec tego problem rozwiązywania kongruencji kwadratowych sprowadza się do do problemu rozwiązywania kongruencji postaci

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{12.4}$$

w których p jest liczbą pierwszą oraz a, b i c są liczbami całkowitych, przy czym $p \nmid a$.

Przypadek $p = 2$ jest trywialny, gdyż wówczas kongruencja (12.4) przybiera postać: $x^2 + bx + c \equiv 0 \pmod 2$. Jeśli b jest nieparzyste, to nasza kongruencja redukuje się do postaci: $x^2 + x + c \equiv 0 \pmod 2$, więc dla nieparzystego c nie posiada ona rozwiązania, zaś dla parzystego c posiada dwa rozwiązania: $x \equiv 0 \pmod 2$ i $x \equiv 1 \pmod 2$. W przypadku, gdy b jest parzyste nasza kongruencja przybiera postać $x^2 + c \equiv 0 \pmod 2$ i dla parzystego c posiada ona dokładnie jedno rozwiązanie $x \equiv 0 \pmod 2$, zaś dla nieparzystego c też posiada dokładnie jedno rozwiązanie: $x \equiv 1 \pmod 2$. Podsumowując, kongruencja $x^2 + bx + c \equiv 0 \pmod 2$ nie posiada rozwiązania wtedy i tylko wtedy, gdy liczby b i c są nieparzyste.

Dalej będziemy zatem rozpatrywali tylko nieparzyste liczby pierwsze p. Wówczas $p \nmid 4a$, więc $\mathrm{NWD}(4a, p) = 1$ i na mocy twierdzenia 11.4 (iii) zbiór rozwiązań kongruencji (12.4) jest równy zbiorowi rozwiązań kongruencji $4a^2x + 4abx + 4ac \equiv 0 \pmod p$, ale $4a^2x + 4abx + 4ac = (2ax + b)^2 - (b^2 - 4ac)$, więc zbiór rozwiązań kongruencji (12.4) jest

równy zbiorowi rozwiązań kongruencji

$$(2ax + b)^2 \equiv \Delta \pmod{p}, \tag{12.5}$$

gdzie $\Delta = b^2 - 4ac$ nazywamy **wyróżnikiem kongruencji** (12.4).

Jeśli teraz $p \mid \Delta$, to dla $x \in \mathbb{Z}$: $(2ax + b)^2 \equiv \Delta \pmod{p}$ wtedy i tylko wtedy, gdy $p|(2ax + b)^2$, czyli z pierwszości p, wtedy i tylko wtedy, gdy $2ax + b \equiv 0 \pmod{p}$. Ta ostatnia kongruencja na mocy twierdzenia 11.18 posiada dokładnie jedno rozwiązanie.

Dalej, jeśli nie istnieje $y \in \mathbb{Z}$ takie, że $y^2 \equiv \Delta \pmod{p}$, to kongruencja (12.5) nie posiada rozwiązania, a więc też kongruencja (12.4) nie posiada wtedy rozwiązania.

Rozważmy teraz ostatni przypadek, gdy $p \nmid \Delta$ i istnieje $y_0 \in \mathbb{Z}$ takie, że $y_0^2 \equiv \Delta \pmod{p}$. Pokażemy, że wówczas zachodzi następujące

Stwierdzenie 12.7. *Jeżeli liczba całkowita Δ nie jest podzielna przez nieparzystą liczbę pierwszą p i $y_0^2 \equiv \Delta \pmod{p}$ dla pewnej liczby całkowitej y_0, to kongruencja $y^2 \equiv \Delta \pmod{p}$ posiada dokładnie dwa rozwiązania: $y_0 + p\mathbb{Z}p$ i $-y_0 + p\mathbb{Z}$.*

Dowód. Z naszych założeń wynika, że $p \nmid y_0$ oraz $(-y_0)^2 = y_0^2 \equiv \Delta \pmod{p}$. Zatem $y_0 + p\mathbb{Z}p$ i $-y_0 + p\mathbb{Z}$ są rozwiązaniami kongruencji $y^2 \equiv \equiv \Delta \pmod{p}$. Gdyby te rozwiązania były równe, to $y_0 \equiv -y_0 \pmod{p}$, skąd $p \mid 2y_0$. Ponadto p jest nieparzystą liczbą pierwszą i $p \nmid y_0$, więc prowadzi to do sprzeczności. Wobec tego $y_0 + p\mathbb{Z}p \neq -y_0 + p\mathbb{Z}p$.

Weźmy dowolne $y_1 \in \mathbb{Z}$ takie, że $y_1^2 \equiv \Delta \pmod{p}$. Wtedy $y_1^2 \equiv \equiv y_0^2 \pmod{p}$. Zatem $p \mid y_1^2 - y_0^2$, ale $y_1^2 - y_0^2 = (y_1 - y_0)(y_1 + y_0)$, więc z pierwszości p, $p \mid y_1 - y_0$ lub $p \mid y_1 + y_0$, skąd $y_1 \equiv y_0 \pmod{p}$ lub $y_1 \equiv -y_0 \pmod{p}$. Zatem $y_1 + p\mathbb{Z} = y_0 + p\mathbb{Z}$ lub $y_1 + p\mathbb{Z} = -y_0 + p\mathbb{Z}$, co kończy dowód. □

Z przeprowadzonego dowodu wynika, że w przypadku, gdy $p \nmid \Delta$ i istnieje $y_0 \in \mathbb{Z}$ takie, że $y_0^2 \equiv \Delta \pmod{p}$ rozwiązywanie kongruencji (12.4) sprowadza się do rozwiązania dwóch kongruencji liniowych:

$$2ax + b \equiv y_0 \pmod{p} \quad \text{oraz} \quad 2ax + b \equiv -y_0 \pmod{p}. \tag{12.6}$$

Każda z tych kongruencji na mocy twierdzenia 11.18 posiada dokładnie jedno rozwiązanie, przy czym te rozwiązania są różne, bo jak pokazaliśmy, $y_0 \not\equiv -y_0 \pmod{p}$. Wobec tego w tym przypadku kongruencja (12.4) posiada dokładnie dwa rozwiązania.

W ten sposób udowodniliśmy następujące

Twierdzenie 12.8. *Niech p będzie nieparzystą liczbą pierwszą i niech $a, b, c \in \mathbb{Z}$, gdzie $p \nmid a$. Niech $\Delta = b^2 - 4ac$. Wówczas:*

(i) jeśli $p|\Delta$, to kongruencja (12.4) *posiada dokładnie jedno rozwiązanie, które jest rozwiązaniem kongruencji $2ax + b \equiv 0 \pmod{p}$,*

(ii) jeśli kongruencja $x^2 \equiv \Delta \pmod{p}$ nie posiada rozwiązania, to kongruencja (12.4) *też nie posiada rozwiązania,*

(iii) jeśli $p \nmid \Delta$ i $y_0^2 \equiv \Delta \pmod{p}$ dla pewnego $y_0 \in \mathbb{Z}$, to kongruencja (12.4) *posiada dokładnie dwa rozwiązania $x_1 + p\mathbb{Z}$ i $x_2 + p\mathbb{Z}$, gdzie $2ax_1 + b \equiv y_0 \pmod{p}$ i $2ax_2 + b \equiv -y_0 \pmod{p}$.*

12.2 Reszty i niereszty kwadratowe

Podsumowując rozważania poprzedniego paragrafu widzimy, że problem rozwiązywania kongruencji (12.4) sprowadziliśmy do problemu rozwiązywania kongruencji postaci:

$$x^2 \equiv a \pmod{p}, \tag{12.7}$$

gdzie p jest liczbą pierwszą nieparzystą, zaś a jest liczbą całkowitą niepodzielną przez p. Jeżeli kongruencja (12.7) ma rozwiązanie, to mówimy, że a **jest resztą kwadratową modulo** p i piszemy $(\frac{a}{p}) = 1$. W przeciwnym przypadku mówimy, że a **jest niereszt ą kwadratową modulo** p i piszemy $(\frac{a}{p}) = -1$. By zdefiniowana w ten sposób funkcja była określona dla wszystkich całkowitych a, przyjmujemy w przypadku $p \mid a$ umowę, że $(\frac{a}{p}) = 0$. Tak zdefiniowaną funkcję

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\}$$

nazywa się **symbolem Legendre'a** dla modułu p.

Przykład 12.9. Niech a będzie liczbą całkowitą niepodzielną przez nieparzystą liczbę pierwszą p. Wtedy $p \nmid a^2$ oraz $x \equiv a \pmod{p}$ jest rozwiązaniem kongruencji $x^2 \equiv a^2 \pmod{p}$. Wobec tego wprost z definicji symbolu Legendre'a mamy wzór:

$$\left(\frac{a^2}{p}\right) = 1. \tag{12.8}$$

Uwaga 12.10. Jeżeli $a, b, c \in \mathbb{Z}$ i $c^2 \equiv a \pmod{p}$ oraz $b \equiv a \pmod{p}$, to $c^2 \equiv b \pmod{p}$. Wobec tego: jeśli a jest resztą kwadratową modulo p, to każda liczba z klasy $a + p\mathbb{Z}$ też jest resztą kwadratową modulo p. W szczególności, $(\frac{a}{p}) = (\frac{b}{p})$, jeśli $a \equiv b \pmod{p}$.

Lemat 12.11. *Zbiór* $\{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ *ma dokładnie* p *elementów i wszystkie jego elementy dają parami różne reszty z dzielenia przez nieparzystą liczbę pierwszą* p.

Dowód. Oczywiście $|\{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}| = 1 + 2 \cdot \frac{p-1}{2} = 1 + (p-1) = p$. Jeśli $x, y \in \{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$, to $|x| \leqslant \frac{p-1}{2}$ i $|y| \leqslant \frac{p-1}{2}$, skąd $|x - y| \leqslant |x| + |y| \leqslant 2 \cdot \frac{p-1}{2} = p - 1$. Jeśli $[x]_p = [y]_p$, to $p | x - y$, skąd $p \mid |x - y|$, więc ponieważ $|x - y| < p$, to $|x - y| = 0$, czyli $x = y$. □

Twierdzenie 12.12. *Niech* p *będzie nieparzystą liczbą pierwszą. Wówczas zbiór* $\frac{p-1}{2}$ *elementowy:*

$$\{[1^2]_p, [2^2]_p, \ldots, [(p-1)/2)^2]_p\} \tag{12.9}$$

składa się z różnych reszt kwadratowych modulo p *i każda reszta kwadratowa modulo* p *przystaje modulo* p *do dokładnie jednej liczby z tego zbioru. Ponadto zbiór* $\frac{p-1}{2}$ *elementowy:*

$$\{1, 2, \ldots, p-1\} \setminus \{[1^2]_p, [2^2]_p, \ldots, [(p-1)/2)^2]_p\} \tag{12.10}$$

składa się z różnych niereszt kwadratowych modulo p *i każda niereszta kwadratowa modulo* p *przystaje do dokładnie jednej liczby z tego zbioru. W szczególności liczba elementów zbioru* $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$*, które są resztami kwadratowymi modulo* p *jest równa liczbie elementów zbioru* $\mathbb{Z}_p$*, które są niereszatami kwadratowymi modulo* p *i wynosi* $\frac{p-1}{2}$.

Dowód. Niech a będzie resztą kwadratową modulo p. Wtedy $p \nmid a$ i $a \equiv c^2 \pmod{p}$ dla pewnego $c \in \mathbb{Z}$. Stąd $p \nmid c$ i na mocy lematu 12.11, $c \equiv \pm j \pmod{p}$ dla pewnego $j \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Stąd $a \equiv j^2 \pmod{p}$, czyli $a \equiv [j^2]_p \pmod{p}$. Dalej, dla $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$ mamy, że $p \nmid i^2$ i $i^2 \equiv [i^2]_p \pmod{p}$, więc $p \nmid [i^2]_p$ i $[i^2]_p \neq 0$. Stąd $[i^2]_p$ jest resztą kwadratową modulo p dla każdego $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Niech $x, y \in \{1, 2, \ldots, \frac{p-1}{2}\}$ będą takie, że $[x^2]_p = [y^2]_p$. Wtedy $p \mid x^2 - y^2$, ale $x^2 - y^2 = (x - y)(x + y)$, więc $p \mid x - y$, skąd $x = [x]_p = [y]_p = y$ lub $p \mid x + y$. Jednakże $0 < x + y \leqslant 2 \cdot \frac{p-1}{2} = p - 1 < p$, więc $p \nmid x + y$. Zatem zbiór (12.9) ma dokładnie $\frac{p-1}{2}$ elementów i pierwsza część naszego twierdzenia jest udowodniona.

Wobec tego zbiór (12.10) ma dokładnie $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ elementów, z których ani jeden nie jest podzielny przez p. Zatem każdy z elementów zbioru (12.10) jest nieresztą kwadratową modulo p. Jeśli liczba całkowita a jest nieresztą kwadratową modulo p, to $p \nmid a$ i $[a]_p \in \mathbb{Z}_p$ oraz $[a]_p$ nie należy do zbioru (12.9). Stąd $[a]_p \neq 0$ i $[a]_p$ należy do zbioru (12.10) oraz $a \equiv [a]_p \pmod{p}$. Dowód twierdzenia został więc zakończony. □

Przykład 12.13. (a). Na mocy twierdzenia 12.12 liczba $1^2 = 1$ jest jedynym elementem zbioru $\mathbb{Z}_3$, który jest resztą kwadratową modulo 3, zaś liczba 2 jest jedynym elementem zbioru $\mathbb{Z}_3$, który jest nieresztą kwadratową modulo 3. Wobec tego dla dowolnej liczby całkowitej a niepodzielnej przez 3 mamy wzór:

$$\left(\frac{a}{3}\right) = \begin{cases} 1, & \text{jeśli } a \equiv 1 \pmod{3} \\ -1, & \text{jeśli } a \equiv 2 \pmod{3} \end{cases}.$$

(b). Podobnie, na mocy twierdzenia 12.12 wszystkimi elementami zbioru $\mathbb{Z}_5$, które są resztami kwadratowymi modulo 5, są jedynie $[1^2]_5 = 1$ i $[2^2]_5 = 4$, zaś 2 i 3 są wszystkimi elementami zbioru $\mathbb{Z}_5$, które są nieresztami kwadratowymi modulo 5. Wobec tego dla dowolnej liczby całkowitej a niepodzielnej przez 5 mamy wzór:

$$\left(\frac{a}{5}\right) = \begin{cases} 1, & \text{jeśli } a \equiv 1, 4 \pmod{5} \\ -1, & \text{jeśli } a \equiv 2, 3 \pmod{5} \end{cases}.$$

(c). Dla $p = 7$, $\frac{p-1}{2} = 3$, więc na mocy twierdzenia 12.12 wszystkimi elementami zbioru $\mathbb{Z}_7$, które są resztami kwadratowymi modulo 7, są jedynie $[1^2]_7 = 1$, $[2^2]_7 = 4$ i $[3^2]_7 = 2$, zaś 3, 5 i 6 są wszystkimi elementami zbioru $\mathbb{Z}_7$, które są niereszta mi kwadratowymi modulo 7. Wobec tego dla dowolnej liczby całkowitej a niepodzielnej przez 7 mamy wzór:

$$\left(\frac{a}{7}\right) = \begin{cases} 1, & \text{jeśli } a \equiv 1, 2, 4 \pmod 7 \\ -1, & \text{jeśli } a \equiv 3, 5, 6 \pmod 7 \end{cases}.$$

Twierdzenie 12.14. (kryterium Eulera). *Niech p będzie nieparzystą liczbą pierwszą i niech $a \in \mathbb{Z}$. Wówczas:*

(i) a jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $a^{\frac{p-1}{2}} \equiv 1 \pmod p$,

(ii) a jest niereszta ą kwadratową modulo p wtedy i tylko wtedy, gdy $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Dowód. (i). Załóżmy, że a jest resztą kwadratową modulo p. Wtedy $p \nmid a$ i $a \equiv c^2 \pmod p$ dla pewnego $c \in \mathbb{Z}$. Stąd $p \nmid c$, więc z małego twierdzenia Fermata, $c^{p-1} \equiv 1 \pmod p$, ale p jest nieparzyste, więc $\frac{p-1}{2} \in \mathbb{N}$ i po podniesieniu obu stron kongruencji $a \equiv c^2 \pmod p$ do potęgi $\frac{p-1}{2}$ uzyskujemy, że $a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1 \pmod p$, czyli $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Na odwrót, niech $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Wtedy $p \nmid a$ i $a + p\mathbb{Z}$ jest rozwiązaniem kongruencji $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$. Z pierwszej części dowodu i z twierdzenia 12.12 klasy $j^2 + p\mathbb{Z}$ dla $j = 1, 2, \ldots, \frac{p-1}{2}$ są różnymi rozwiązaniami tej kongruencji. Gdyby a nie było resztą kwadratową modulo p, to ta kongruencja miałaby co najmniej $1 + \frac{p-1}{2}$ rozwiązań, co przeczy twierdzeniu Lagrange'a o liczbie pierwiastków kongruencji. Zatem a musi być resztą kwadratową modulo p.

(ii). Przypuśćmy, że $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Wtedy $p \nmid a$. Ponieważ $p > 2$, więc $1 \not\equiv -1 \pmod p$. Wobec tego $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. Stąd i na mocy (i), a jest niereszta ą kwadratową modulo p.

Na odwrót, załóżmy, że a jest niereszta ą kwadratową modulo p. Wtedy $p \nmid a$ i na mocy (i), $p \nmid a^{\frac{p-1}{2}} - 1$. Z małego twierdzenia Fermata, $a^{p-1} \equiv 1 \pmod p$, czyli $p | (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, ale $p \nmid a^{\frac{p-1}{2}} - 1$, więc $p | a^{\frac{p-1}{2}} + 1$, skąd $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. □

Z kryterium Eulera otrzymujemy natychmiast następujący

Wniosek 12.15. *Dla dowolnej nieparzystej liczby pierwszej p i dla dowolnej liczby całkowitej a zachodzi wzór:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Wniosek 12.16. *Dla nieparzystej liczby pierwszej p liczba -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $p \equiv 1 \pmod 4$. Wobec tego zachodzi wzór:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{jeśli } p \equiv 1 \pmod 4 \\ -1, & \text{jeśli } p \equiv 3 \pmod 4 \end{cases}.$$

Dowód. Ponieważ $p \nmid -1$, więc na mocy twierdzenia 12.14 liczba -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Dodatkowo $p > 2$ oraz $(-1)^{\frac{p-1}{2}} = \pm 1$, więc -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $(-1)^{\frac{p-1}{2}} = 1$, a to zachodzi wtedy i tylko wtedy, gdy liczba $\frac{p-1}{2}$ jest parzysta, czyli gdy $p \equiv 1 \pmod 4$. □

Wniosek 12.17. *Niech $a_1, a_2, \ldots, a_n$ będą liczbami całkowitymi niepodzielnymi przez nieparzystą liczbę pierwszą p. Wówczas:*

$$\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right).$$

Dowód. Z własności liczb pierwszych mamy, że $p \nmid a_1 \cdot a_2 \cdot \ldots \cdot a_n$. Ponadto $(\frac{a_i}{p}) \equiv a_i^{\frac{p-1}{2}} \pmod p$ dla każdego $i = 1, 2, \ldots, n$ na mocy kryterium Eulera. Stąd po pomnożeniu stronami tych kongruencji uzyskamy, że

$$\left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right) \equiv (a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{\frac{p-1}{2}} \pmod{p}.$$

Dodatkowo

$$(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{\frac{p-1}{2}} \equiv \left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) \pmod{p}$$

na mocy kryterium Eulera, więc z przechodniości kongruencji otrzymujemy, że

$$\left(\frac{a_1}{p}\right)\cdot\left(\frac{a_2}{p}\right)\cdot\ldots\cdot\left(\frac{a_n}{p}\right)\equiv\left(\frac{a_1\cdot a_2\cdot\ldots\cdot a_n}{p}\right)\pmod p.$$

Uwzględniając to, że liczby występujące w obu stronach ostatniej zależności są równe ±1 i $-1\not\equiv 1 \pmod p$, bo $p>2$, uzyskujemy żądany wzór. □

12.3 Prawo wzajemności reszt kwadratowych

Przypomnijmy, że dla rzeczywistej liczby x symbol $\lfloor x\rfloor$ oznacza największą liczbę całkowitą nie większą od x.

Lemat 12.18. *Niech c będzie liczbą całkowitą niepodzielną przez nieparzystą liczbę pierwszą p. Wówczas istnieje dokładnie jedna liczba $r\in\{1,2,\ldots,\frac{p-1}{2}\}$ taka, że $c\equiv(-1)^{\lfloor\frac{2c}{p}\rfloor}r \pmod p$. Ponadto liczba $\lfloor\frac{2c}{p}\rfloor$ jest nieparzysta wtedy i tylko wtedy, gdy $[c]_p>\frac{p-1}{2}$.*

Dowód. Z twierdzenia o dzieleniu z resztą $c=kp+[c]_m$ dla pewnego $k\in\mathbb{Z}$, ale $p\nmid c$, więc $[c]_p\neq 0$. Jeżeli $[c]_p\in\{1,2,\ldots,\frac{p-1}{2}\}$, to $0<2[c]_p\leqslant p-1<p$, więc $2k<\frac{2c}{p}=2k+\frac{2[c]_p}{p}<2k+1$, skąd $\lfloor\frac{2c}{p}\rfloor=2k$, ale $c\equiv[c]_p \pmod p$, więc stąd $c\equiv(-1)^{\lfloor\frac{2c}{p}\rfloor}r \pmod p$ dla $r=[a]_p$. Niech zatem $[c]_p>\frac{p-1}{2}$. Wtedy $[c]_p\geqslant\frac{p-1}{2}+1=\frac{p+1}{2}>\frac{p}{2}$, więc $p<2[c]_p\leqslant 2(p-1)<2p$. Stąd $2k+1\leqslant 2k+\frac{2[c]_p}{p}=\frac{2c}{p}<2k+2$, czyli $\lfloor\frac{2c}{p}\rfloor=2k+1$. Zatem $(-1)^{\lfloor\frac{2c}{p}\rfloor}(p-[c]_p)=[c]_p-p\equiv c \pmod p$ oraz $p-[c]_p\in\{1,2,\ldots,\frac{p-1}{2}\}$, bo $0<p-[c]_p\leqslant p-\frac{p+1}{2}=\frac{p-1}{2}$. Wobec tego w tym przypadku wystarczy obrać $r=p-[c]_p$.

Jeżeli $r,s\in\{1,2,\ldots,\frac{p-1}{2}\}$, $c\equiv(-1)^{\lfloor\frac{2c}{p}\rfloor}r \pmod p$ i $c\equiv(-1)^{\lfloor\frac{2c}{p}\rfloor}s \pmod p$, to $(-1)^{\lfloor\frac{2c}{p}\rfloor}r\equiv(-1)^{\lfloor\frac{2c}{p}\rfloor}s \pmod p$, skąd $r\equiv s \pmod p$, czyli $s=[s]_p=[r]_p=r$. □

Twierdzenie 12.19. (kryterium Gaussa). *Niech $p > 2$ będzie liczbą pierwszą, która nie dzieli liczby całkowitej a. Wówczas równoważne są warunki:*

(i) a jest resztą kwadratową modulo p,

(ii) liczba $\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2ai)/p \rfloor$ jest parzysta,

(iii) liczba wszystkich $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$ takich, że $[ai]_p > \frac{p-1}{2}$ jest parzysta.

Dowód. Ponieważ $p \in \mathbb{P}$, $p \nmid a$ oraz $p \nmid i$, więc $p \nmid ai$ dla każdego $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Stąd na mocy lematu 12.18 dla każdego $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$ istnieje dokładnie jedno $r_i \in \{1, 2, \ldots, \frac{p-1}{2}\}$ takie, że

$$ai \equiv (-1)^{\lfloor (2ai)/p \rfloor} r_i \pmod{p}. \tag{12.11}$$

Ponadto z lematu 12.18 wynika, że funkcja $i \mapsto r_i$ jest różnowartościowa. Wobec tego

$$\{r_1, r_2, \ldots, r_{(p-1)/2}\} = \{1, 2, \ldots, (p-1)/2\}. \tag{12.12}$$

Zatem wymnażając stronami kongruencje (12.11) dla $i = 1, 2, \ldots, \frac{p-1}{2}$ i uwzględniając (12.12) uzyskujemy, że

$$a^{\frac{p-1}{2}} \cdot A \equiv (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2ai)/p \rfloor} \cdot A \pmod{p}$$

dla $A = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$, ale p jest liczbą pierwszą, więc $p \nmid A$, czyli $\mathrm{NWD}(A, p) = 1$ i w otrzymanej kongruencji możemy skrócić A uzyskując wzór:

$$a^{\frac{p-1}{2}} \equiv (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2ai)/p \rfloor} \pmod{p}. \tag{12.13}$$

$(i) \Rightarrow (ii)$. Z Kryterium Eulera $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, więc na mocy (12.13) i tego, że $p > 2$, liczba $\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2ai)/p \rfloor$ jest

parzysta. $(ii) \Rightarrow (iii)$. Wynika od razu z lematu 12.18. $(iii) \Rightarrow (i)$. Ponieważ suma parzystej liczby liczb nieparzystych jest liczbą parzystą, więc na mocy lematu 12.18 liczba $\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2ai)/p \rfloor$ jest parzysta. Zatem z (12.13), $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ i na mocy Kryterium Eulera a jest resztą kwadratową modulo p. □

Przykład 12.20. Za pomocą Kryterium Gaussa zbadamy, dla jakich liczb pierwszych $p > 2$ liczba 2 jest resztą kwadratową modulo p. Najpierw zauważamy, że dla $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$ liczba $\frac{2 \cdot 2i}{p} \leqslant \frac{4 \cdot \frac{p-1}{2}}{p} = \frac{2p-2}{p} = 2 - \frac{2}{p} < 2$ oraz $\frac{2 \cdot 2i}{p} > 0$. Zatem $\lfloor (4i)/p \rfloor \in \{0, 1\}$. Pozostaje zatem obliczyć liczbę tych $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$, dla których $\lfloor (4i)/p \rfloor = 1$, czyli takich, że $1 \leqslant \frac{4i}{p}$, to znaczy $\frac{p}{4} \leqslant i \leqslant \frac{p-1}{2}$. Jednakże $4 \nmid p$, więc $i = \lfloor p/4 \rfloor + 1, \ldots, \frac{p-1}{2}$. Zatem liczba takich i jest równa $\frac{p-1}{2} - \lfloor p/4 \rfloor$. Wobec tego $\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2 \cdot 2i)/p \rfloor = \frac{p-1}{2} - \lfloor p/4 \rfloor$ i na mocy Kryterium Gaussa 2 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $\frac{p-1}{2} - \lfloor p/4 \rfloor$ jest liczbą parzystą. Ponadto $p \equiv 1, 3, 5, 7 \pmod{8}$, więc w pierwszym przypadku $p = 8k + 1$ dla pewnego $k \in \mathbb{N}$, skąd $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k - \lfloor 2k + \frac{1}{4} \rfloor = 4k - 2k = 2k$. W drugim przypadku, $p = 8k + 3$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k + 1 - \lfloor 2k + \frac{3}{4} \rfloor = 4k + 1 - 2k = 2k + 1$. W trzecim przypadku, $p = 8k + 5$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k + 2 - \lfloor 2k + 1 + \frac{1}{4} \rfloor = 4k + 2 - (2k + 1) = 2k + 1$. W ostatnim przypadku, $p = 8k + 7$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k + 3 - \lfloor 2k + 1 + \frac{3}{4} \rfloor = 4k + 3 - (2k + 1) = 2k + 2$. Wobec tego ostatecznie: 2 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $p \equiv 1 \pmod{8}$ lub $p \equiv 7 \pmod{8}$. Zauważmy jeszcze, że jeżeli $p \equiv 1 \pmod{8}$ lub $p \equiv 7 \pmod{8}$, to $p = 8k \pm 1$ dla pewnego $k \in \mathbb{N}$, więc $\frac{p^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 - 2k$, skąd $(-1)^{\frac{p^2-1}{8}} = 1$ oraz jeżeli $p \equiv 3 \pmod{8}$ lub $p \equiv 5 \pmod{8}$, to $p = 8k \pm 3$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p^2-1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 - 6k + 1$, skąd $(-1)^{\frac{p^2-1}{8}} = -1$.

Mamy zatem udowodniony wzór:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{jeśli } p \equiv 1,7 \pmod 8 \\ -1, & \text{jeśli } p \equiv 3,5 \pmod 8 \end{cases}. \tag{12.14}$$

Przykład 12.21. Dla dowolnej liczby pierwszej $p > 2$ znajdziemy wzór na $(\frac{-2}{p})$. Ponieważ $-2 = (-1) \cdot 2$, więc z wniosków 12.17 i 12.15 oraz ze wzoru (12.14) uzyskujemy od razu następujący wzór:

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}. \tag{12.15}$$

Oczywiście $p \equiv 1,3,5,7 \pmod 8$. Jeśli $p \equiv 1 \pmod 8$, to $p \equiv 1 \pmod 4$, więc ze wzoru (12.14) i z wniosku 12.15 mamy, że $(\frac{-2}{p}) = 1 \cdot 1 = 1$. Jeśli $p \equiv 3 \pmod 8$, to $p \equiv 3 \pmod 4$, więc ze wzoru (12.14) i z wniosku 12.15 mamy, że $(\frac{-2}{p}) = (-1) \cdot (-1) = 1$. Jeśli $p \equiv 5 \pmod 8$, to $p \equiv 1 \pmod 4$, więc ze wzoru (12.14) i z wniosku 12.15 mamy, że $(\frac{-2}{p}) = 1 \cdot (-1) = -1$. Jeśli $p \equiv 7 \pmod 8$, to $p \equiv 3 \pmod 4$, więc ze wzoru (12.14) i z wniosku 12.15 mamy, że $(\frac{-2}{p}) = (-1) \cdot 1 = -1$. Wobec tego udowodniliśmy wzór:

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{jeśli } p \equiv 1,3 \pmod 8 \\ -1, & \text{jeśli } p \equiv 5,7 \pmod 8 \end{cases}. \tag{12.16}$$

Lemat 12.22. *Niech p i q będą różnymi nieparzystymi liczbami pierwszymi. Oznaczmy przez A zbiór wszystkich par liczb naturalnych (x, y) takich, że $1 \leqslant x \leqslant \frac{p-1}{2}$ i $1 \leqslant y \leqslant \frac{q-1}{2}$ oraz $1 \leqslant py - qx \leqslant \frac{p-1}{2}$. Wówczas $(\frac{q}{p}) = (-1)^{|A|}$.*

Dowód. Niech X oznacza zbiór wszystkich $x \in \{1, 2, \ldots, \frac{p-1}{2}\}$ takich, że $[qx]_p > \frac{p-1}{2}$. Wtedy na mocy Kryterium Gaussa $(\frac{q}{p}) = (-1)^{|X|}$. Wystarczy zatem wykazać, że zbiory A i X są równoliczne.

Niech $x \in X$. Wtedy z lematu 12.18 istnieje $r \in \{1, 2, \ldots, \frac{p-1}{2}\}$ takie, że $qx \equiv -r \pmod p$. Zatem $qx + r = py$ dla pewnego $y \in \mathbb{Z}$, ale $qx + r > 0$, więc $y > 0$, czyli $y \geqslant 1$. Ponadto $x \leqslant \frac{p-1}{2}$ i $r \leqslant \frac{p-1}{2}$, więc $py \leqslant (q+1)\frac{p-1}{2}$, skąd $y \leqslant \frac{q+1}{2} \cdot \frac{p-1}{p} < \frac{q+1}{2}$. Zatem $y \leqslant \frac{q+1}{2} - 1 = \frac{q-1}{2}$. Ponadto $1 \leqslant r = py - qx \leqslant \frac{p-1}{2}$. Zatem $(x, y) \in A$. Jeżeli $y' \in$

$\in \{1, 2, \ldots, \frac{q-1}{2}\}$ i $1 \leqslant py' - qx \leqslant \frac{p-1}{2}$, to $|(py - qx) - (py' - qx)| \leqslant$ $\leqslant \frac{p-1}{2}$, czyli $p|y - y'| \leqslant \frac{p-1}{2}$, skąd $|y - y'| = 0$, czyli $y' = y$. Zatem dla każdego $x \in X$ istnieje dokładnie jedno y takie, że $(x, y) \in A$. Wobec tego funkcja $x \mapsto (x, y)$ odwzorowuje różnowartościowo zbiór X w zbiór A. Pozostaje zatem do wykazania, że ta funkcja jest „na". W tym celu weźmy dowolne $(x, y) \in A$. Wtedy $x \in \{1, 2, \ldots, \frac{p-1}{2}\}$, $y \in \{1, 2, \ldots, \frac{q-1}{2}\}$ i $1 \leqslant r \leqslant \frac{p-1}{2}$ dla $r = py - qx$. Stąd $qx = py - r =$ $= (y - 1)p + (p - r)$, więc ponieważ $p > p - r \geqslant p - \frac{p-1}{2} = \frac{p+1}{2} > \frac{p-1}{2}$, to $p - r = [qx]_p > \frac{p-1}{2}$. Zatem $x \in A$ i $x \mapsto (x, y)$. Kończy to dowód naszego lematu. □

Udowodnimy teraz fundamentalny rezultat w teorii reszt kwadratowych odkryty przez Eulera i udowodniony po raz pierwszy przez Gaussa (miał on wtedy zaledwie 19 lat!).

Twierdzenie 12.23. (prawo wzajemności reszt kwadratowych). *Dla dowolnych różnych nieparzystych liczb pierwszych p i q zachodzi wzór:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \tag{12.17}$$

Dowód. Oznaczmy przez A zbiór wszystkich par (x, y) liczb naturalnych takich, że $1 \leqslant x \leqslant \frac{p-1}{2}$ i $1 \leqslant y \leqslant \frac{q-1}{2}$ oraz $1 \leqslant py - qx \leqslant \frac{p-1}{2}$ i niech B będzie zbiorem par liczb naturalnych (x, y) takich, że $1 \leqslant x \leqslant$ $\leqslant \frac{p-1}{2}$ i $1 \leqslant y \leqslant \frac{q-1}{2}$ oraz $1 \leqslant qx - py \leqslant \frac{q-1}{2}$, czyli $-\frac{q-1}{2} \leqslant py - qx \leqslant -1$. Wtedy na mocy lematu 12.22, $\left(\frac{q}{p}\right) = (-1)^{|A|}$ i $\left(\frac{p}{q}\right) = (-1)^{|B|}$. Zatem

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{|A|+|B|}. \tag{12.18}$$

Dla $x \in \{1, 2, \ldots, \frac{p-1}{2}\}$ i $y \in \{1, 2, \ldots, \frac{q-1}{2}\}$ nie może zajść $qx - py = 0$, bo wtedy byłoby $p \mid qx$, a ponieważ $p, q \in \mathbb{P}$ i $p \neq q$, więc mielibyśmy, że $p \mid x$, co jest niemożliwe, bo $1 \leqslant x < p$. Wobec tego zbiór $U =$ $= \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\}$ jest sumą parami rozłącznych zbiorów A, B, C i D, gdzie $C = \{(x, y) \in U : py - qx < -\frac{q-1}{2}\}$ i $D = \{(x, y) \in U : \frac{p-1}{2} < py - qx\}$.

Zauważmy, że dla $(x,y) \in U$ mamy, że $(\frac{p+1}{2}-x, \frac{q+1}{2}-y) \in U$. Niech teraz $(x,y) \in C$. Wtedy $qx - py < -\frac{q+1}{2}$, więc $p(\frac{q+1}{2} - y) - q(\frac{p+1}{2} - +x) = \frac{pq+p}{2} - py - \frac{pq+q}{2} + qx = \frac{p-q}{2} - (py - qx) > \frac{p-q}{2} + \frac{q+1}{2} = \frac{p+1}{2}$, skąd $(\frac{p+1}{2} - x, \frac{q+1}{2} - y) \in D$. Wobec tego przekształcenie $(x,y) \mapsto \mapsto (\frac{p+1}{2}-x, \frac{q+1}{2}-y)$ jest różnowartościowym odwzorowaniem zbioru C w zbiór D. Weźmy dowolne $(u,v) \in D$. Wtedy $(\frac{p+1}{2} - u, \frac{q+1}{2} - v) \in U$ oraz $\frac{p-1}{2} < pv - qu$, więc $p(\frac{q+1}{2} - v) - q(\frac{p+1}{2} - u) = \frac{qp+p}{2} - pv - \frac{pq+q}{2} + qu = = \frac{p-q}{2} - (pv - qu) < \frac{p-q}{2} - \frac{p-1}{2} = -\frac{q-1}{2}$, skąd $(\frac{p+1}{2} - x, \frac{q+1}{2} - y) \in C$, przy czym $(\frac{p+1}{2} - x, \frac{q+1}{2} - y) \mapsto (u,v)$. Wobec tego tak zdefiniowane odwzorowanie jest bijekcją zbioru C na zbiór D i $|C| = |D|$. Dalej, $|U| = \frac{p-1}{2} \cdot \frac{q-1}{2}$ i $|U| = |A| + |B| + |C| + |D| = |A| + |B| + 2|C|$. Stąd $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (-1)^{|A|+|B|} = (\frac{p}{q}) \cdot (\frac{q}{p})$, na mocy (12.18). □

W praktyce wzór (12.17) wygodnie jest stosować w postaci następującej formuły:

$$\left(\frac{q}{p}\right) = \begin{cases} (\frac{p}{q}), & \text{jeśli } p \equiv 1 \pmod 4 \text{ lub } q \equiv 1 \pmod 4 \\ -(\frac{p}{q}), & \text{jeśli } p \equiv 3 \pmod 4 \text{ i } q \equiv 3 \pmod 4 \end{cases}. \tag{12.19}$$

Przykład 12.24. Dla liczb pierwszych $p > 3$ obliczymy $(\frac{3}{p})$. Oczywiście $p \equiv 1, 5, 7, 11 \pmod{12}$. Jeśli $p \equiv 1 \pmod{12}$, to $p \equiv 1 \pmod 4$, więc ze wzoru (12.19) mamy, że $(\frac{3}{p}) = (\frac{p}{3})$, a ponieważ $p \equiv 1 \pmod 3$, więc $(\frac{p}{3}) = (\frac{1}{3}) = 1$, czyli wtedy $(\frac{3}{p}) = 1$.

Jeśli $p \equiv 5 \pmod{12}$, to $p \equiv 1 \pmod 4$ i $p \equiv 2 \pmod 3$, więc $(\frac{3}{p}) = (\frac{p}{3}) = (\frac{2}{3}) = -1$, czyli wtedy $(\frac{3}{p}) = -1$.

Jeśli $p \equiv 7 \pmod{12}$, to $p \equiv 3 \pmod 4$ i $p \equiv 1 \pmod 3$, więc ze wzoru (12.19) mamy, że $(\frac{3}{p}) = -(\frac{p}{3}) = -(\frac{1}{3}) = -1$, czyli wtedy $(\frac{3}{p}) = -1$.

Jeśli $p \equiv 11 \pmod{12}$, to $p \equiv 3 \pmod 4$ i $p \equiv 2 \pmod 3$, więc ze wzoru (12.19) mamy, że $(\frac{3}{p}) = -(\frac{p}{3}) = -(\frac{2}{3}) = -(-1) = 1$, czyli wtedy $(\frac{3}{p}) = 1$.

Otrzymane rezultaty możemy zapisać zatem takim wzorem:

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{jeśli } p \equiv 1, 11 \pmod{12} \\ -1, & \text{jeśli } p \equiv 5, 7 \pmod{12} \end{cases}. \tag{12.20}$$

Ćwiczenie 12.25. Udowodnij, że dla nieparzystych liczb pierwszych $p \neq 5$ zachodzi wzór:

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{jeśli } p \equiv 1,4 \pmod 5 \\ -1, & \text{jeśli } p \equiv 2,3 \pmod 5 \end{cases}. \tag{12.21}$$

Przykład 12.26. Z rozwiązania zadania 22.29 wiemy, że $151 \in \mathbb{P}$. Obliczymy teraz $(\frac{91}{151})$. Ponieważ $91 = 7 \cdot 13$, więc z wniosku 12.17 uzyskujemy, że $(\frac{91}{151}) = (\frac{7}{151}) \cdot (\frac{13}{151})$.

Dalej, $7 \equiv 3 \pmod 4$, $13 \equiv 1 \pmod 4$ i $[151]_4 = 3$, więc ze wzoru (12.19) mamy, że $(\frac{7}{151}) = -(\frac{151}{7}) = -(\frac{4}{7}) = -1$, bo $[151]_7 = 4 = 2^2$ oraz $(\frac{13}{151}) = (\frac{151}{13}) = (\frac{8}{13})$, ale $8 = 2 \cdot 4$ i $(\frac{4}{13}) = 1$, więc z wniosku 12.17 mamy, że $(\frac{13}{151}) = (\frac{2}{13})$. Ponadto $13 \equiv 5 \pmod 8$, więc $(\frac{2}{13}) = -1$ ze wzoru (12.14).

Wobec tego $(\frac{91}{151}) = (-1) \cdot (-1) = 1$. Zatem istnieje $k \in \mathbb{Z}$ takie, że $k^2 \equiv 91 \pmod{151}$ oraz na mocy stwierdzenia 12.7 kongruencja $x^2 \equiv 91 \pmod{151}$ ma dokładnie dwa rozwiązania: $x \equiv k \pmod{151}$ i $x \equiv -k \pmod{151}$.

Ćwiczenie 12.27. Oblicz $(\frac{69}{307})$. Ile rozwiązań posiada kongruencja $x^2 \equiv 69 \pmod{307}$?

12.4 Symbol Jacobiego

Niech $m > 1$ będzie nieparzystą liczbą naturalną i niech a będzie liczbą całkowitą. Istnieją wówczas nieparzyste liczby pierwsze (niekoniecznie różne) $p_1, p_2, \ldots, p_s$ takie, że $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Iloczyn symboli Legendre'a $(\frac{a}{p_1}) \cdot \ldots \cdot (\frac{a}{p_s})$ oznaczać będziemy przez $(\frac{a}{m})$. Zatem

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_s}\right). \tag{12.22}$$

Ponadto, tak zdefiniowaną liczbę $(\frac{a}{m})$ nazywamy **symbolem Jacobiego**. Z tego określenia mamy od razu, że jeżeli $m \in \mathbb{P}$, to symbol Jacobiego $(\frac{a}{m})$ pokrywa się z symbolem Legenrdre'a $(\frac{a}{p})$, gdzie $p = m$.

Ćwiczenie 12.28. Udowodnij, że dla dowolnej liczby nieparzystej $m > 1$ i dla dowolnego $a \in \mathbb{Z}$:

$$\left(\frac{a}{m}\right) \neq 0 \iff \mathrm{NWD}(a, m) = 1.$$

Przykład 12.29. Zauważmy, że kongruencja $x^2 \equiv a \pmod{15}$ nie posiada rozwiązania, gdyż inaczej kongruencja $x^2 \equiv 2 \pmod 3$ miałaby rozwiązanie, a to jak wiemy nie jest prawdą. Natomiast symbol Jacobiego $(\frac{2}{15}) = (\frac{2}{3}) \cdot (\frac{2}{5}) = (-1) \cdot (-1) = 1$. Wobec tego równość $(\frac{a}{m}) = 1$ na ogół nie implikuje tego, że kongruencja $x^2 \equiv a \pmod m$ ma rozwiązanie.

Stwierdzenie 12.30. *Niech $m > 1$ będzie nieparzystą liczbą naturalną względnie pierwszą z liczbą całkowitą a taką, że $(\frac{a}{m}) = -1$. Wówczas kongruencja $x^2 \equiv a \pmod m$ nie posiada rozwiązania.*

Dowód. Oczywiście $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ dla pewnych $p_1, \ldots, p_s \in \mathbb{P} \setminus \{2\}$. Ponieważ $(\frac{a}{m}) = -1$, więc ze wzoru (12.22) wynika, że $(\frac{a}{p_i}) = -1$ dla pewnego $i = 1, \ldots, s$. Zatem kongruencja $x^2 \equiv a \pmod{p_i}$ nie posiada rozwiązania. Ponadto $p_i \mid m$, więc kongruencja $x^2 \equiv a \pmod m$ też nie ma rozwiązania. □

Stwierdzenie 12.31. *Niech $m > 1$ będzie nieparzystą liczbą naturalną względnie pierwszą z liczbą całkowitą a i niech $b \in \mathbb{Z}$ oraz $b \equiv a \pmod m$. Wtedy $\mathrm{NWD}(b, m) = 1$ oraz $(\frac{b}{m}) = (\frac{a}{m})$.*

Dowód. Niech $d = \mathrm{NWD}(b, m)$. Wtedy $d \mid b$ i $d \mid m$, ale $m \mid b - a$, więc $d \mid b - a$, skąd $d \mid a$. Wobec tego $d \mid a$ i $d \mid m$, a ponieważ $\mathrm{NWD}(a, m) = 1$, więc $d = 1$, czyli $\mathrm{NWD}(b, m) = 1$.

Dalej, $m = p_1 \cdot \ldots \cdot p_s$ dla pewnych nieparzystych liczb pierwszych $p_1, \ldots, p_s$ i $(\frac{b}{p_i}) = (\frac{a}{p_i})$ dla $i = 1, \ldots, s$ na mocy uwagi 12.10. Zatem $(\frac{b}{m}) = (\frac{b}{p_1}) \cdot \ldots \cdot (\frac{b}{p_s}) = (\frac{a}{p_1}) \cdot \ldots \cdot (\frac{a}{p_s}) = (\frac{a}{m})$. □

Stwierdzenie 12.32. *Niech $m > 1$ będzie nieparzystą liczbą naturalną względnie pierwszą z liczbą całkowitą a. Wtedy $\mathrm{NWD}(a^2, m) = 1$ oraz $(\frac{a^2}{m}) = 1$.*

Dowód. Ponieważ $\mathrm{NWD}(a,m)=1$, więc $\mathrm{NWD}(a^2,m)=1$ na mocy stwierdzenia 8.49. Ponadto $m=p_1\cdot\ldots\cdot p_s$ dla pewnych nieparzystych liczb pierwszych $p_1,\ldots,p_s$ i $(\frac{a^2}{p_i})=1$ dla $i=1,\ldots,s$ na mocy wzoru(12.8). Stąd i ze wzoru (12.22) mamy, że $(\frac{a}{m})=1^s=1$. □

Stwierdzenie 12.33. *Niech $m>1$ będzie nieparzystą liczbą naturalną względnie pierwszą z liczbami całkowitymi $a_1,\ldots,a_k$. Wtedy* $\mathrm{NWD}(a_1\cdot\ldots\cdot a_k,m)=1$ *oraz* $(\frac{a_1\cdot\ldots\cdot a_k}{m})=(\frac{a_1}{m})\cdot\ldots\cdot(\frac{a_k}{m})$.

Dowód. Pierwsza część tezy wynika ze stwierdzenia 8.49. Ponadto $m=p_1\cdot\ldots\cdot p_s$ dla pewnych nieparzystych liczb pierwszych $p_1,\ldots,p_s$ i $(\frac{a_1\cdot\ldots\cdot a_k}{p_i})=(\frac{a_1}{p_i})\cdot\ldots\cdot(\frac{a_k}{p_i})$ dla $i=1,\ldots,s$ na mocy wniosku 12.17. Stąd i ze wzoru (12.22) mamy, że $(\frac{a_1\cdot\ldots\cdot a_k}{m})=(\frac{a_1\cdot\ldots\cdot a_k}{p_1})\cdot\ldots\cdot(\frac{a_1\cdot\ldots\cdot a_k}{p_s})=$ $=(\frac{a_1}{p_1})\cdot\ldots\cdot(\frac{a_k}{p_1})\cdot\ldots\cdot(\frac{a_1}{p_s})\cdot\ldots\cdot(\frac{a_k}{p_s})=[(\frac{a_1}{p_1})\cdot\ldots\cdot(\frac{a_k}{p_1})]\cdot\ldots\cdot[(\frac{a_1}{p_s})\cdot\ldots\cdot(\frac{a_k}{p_s})]=$ $=(\frac{a_1}{m})\cdot\ldots\cdot(\frac{a_k}{m})$. □

Lemat 12.34. *Dla dowolnej liczby naturalnej s i dla dowolnych nieparzystych liczb całkowitych $n_1,\ldots,n_s$ zachodzi wzór:*

$$(n_1-1)+(n_2-1)+\ldots+(n_s-1)\equiv n_1\cdot n_2\cdot\ldots\cdot n_s-1 \pmod 4. \quad (12.23)$$

Dowód. Zastosujemy indukcję ze względu na $s\in\mathbb{N}$. Dla $s=1$ teza jest oczywista. Niech n_1 i n_2 będą nieparzystymi liczbami całkowitymi. Wtedy $(n_1n_2-1)-[(n_1-1)+(n_2-1)]=(n_1-1)(n_2-1)$, skąd $4\mid(n_1n_2-1)-[(n_1-1)+(n_2-1)]$, a to oznacza, że wzór (12.23) zachodzi dla $s=2$.

Przypuśćmy, że wzór (12.23) zachodzi dla pewnej liczby naturalnej $s\geqslant 2$ i niech $n_1,\ldots,n_s,n_{s+1}$ będą dowolnymi nieparzystymi liczbami całkowitymi. Wówczas

$$(n_1-1)+(n_2-1)+\ldots+(n_s-1)\equiv n_1\cdot n_2\cdot\ldots\cdot n_s-1 \pmod 4 \quad (12.24)$$

na mocy założenia indukcyjnego, a ponieważ liczba $n_1\cdot\ldots\cdot n_s$ jest nieparzysta, więc z kroku dla $s=2$ mamy, że

$$(n_1\cdot n_2\cdot\ldots\cdot n_s-1)+(n_{s+1}-1)\equiv n_1\cdot\ldots\cdot n_s\cdot n_{s+1}-1 \pmod 4.$$

Stąd i z (12.24) wynika, że wzór (12.23) zachodzi dla liczby $s+1$.

Wobec tego na mocy zasady indukcji dowodzony wzór zachodzi dla każdego $s\in\mathbb{N}$. □

Twierdzenie 12.35. *Dla dowolnej nieparzystej liczby naturalnej $m > 1$ zachodzi wzór:*

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1, & \text{jeśli } m \equiv 1 \pmod 4 \\ -1, & \text{jeśli } m \equiv 3 \pmod 4 \end{cases}. \tag{12.25}$$

Dowód. Oczywiście $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ dla pewnych $p_1, \ldots, p_s \in \mathbb{P} \setminus \{2\}$. Ponadto $(\frac{-1}{p_i}) = (-1)^{\frac{p_i-1}{2}}$ dla każdego $i = 1, \ldots, s$ na mocy wniosku 12.16, więc ze wzoru (12.22) otrzymujemy, że

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{(p_1-1)+\ldots+(p_s-1)}{2}}.$$

Dalej, $(p_1 - 1) + \ldots + (p_s - 1) = (p_1 \cdot \ldots \cdot p_s) - 1 + 4k = m - 1 + 4k$ dla pewnego $k \in \mathbb{Z}$ na mocy lematu 12.34, więc $\frac{(p_1-1)+\ldots+(p_s-1)}{2} = \frac{m-1}{2} + 2k$ i wobec tego $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$. Ponadto liczba m jest nieparzysta, więc $m \equiv 1 \pmod 4$ lub $m \equiv 3 \pmod 4$. W pierwszym przypadku liczba $\frac{m-1}{2}$ jest parzysta, czyli $(-1)^{\frac{m-1}{2}} = 1$, zaś w drugim przypadku liczba $\frac{m-1}{2}$ jest nieparzysta, czyli $(-1)^{\frac{m-1}{2}} = -1$. □

Lemat 12.36. *Dla dowolnej liczby naturalnej s i dla dowolnych nieparzystych liczb całkowitych $n_1, \ldots, n_s$ zachodzi wzór:*

$$(n_1^2 - 1) + (n_2^2 - 1) + \ldots + (n_s^2 - 1) \equiv (n_1 \cdot n_2 \cdot \ldots \cdot n_s)^2 - 1 \pmod{16}. \tag{12.26}$$

Dowód. Zastosujemy indukcję ze względu na $s \in \mathbb{N}$. Dla $s = 1$ teza jest oczywista. Niech n_1 i n_2 będą nieparzystymi liczbami całkowitymi. Wtedy $[(n_1 n_2)^2 - 1] - [(n_1^2 - 1) + (n_2^2 - 1)] = (n_1^2 - 1)(n_2^2 - 1)$. Ponadto, jeśli liczba całkowita a jest nieparzysta, to $a \equiv 1, 3 \pmod 4$, skąd $a^2 \equiv 1 \pmod 4$, czyli $4 \mid a^2 - 1$. Wobec tego $16 \mid (n_1^2 - 1)(n_2^2 - 1)$, skąd $(n_1^2 - 1) + (n_2^2 - 1) \equiv (n_1 n_2)^2 - 1 \pmod{16}$, a to oznacza, że wzór (12.26) zachodzi dla $s = 2$.

Przypuśćmy, że wzór (12.26) zachodzi dla pewnej liczby naturalnej $s \geqslant 2$ i niech $n_1, \ldots, n_s, n_{s+1}$ będą dowolnymi nieparzystymi liczbami całkowitymi. Wówczas

$$(n_1^2 - 1) + (n_2^2 - 1) + \ldots + (n_s^2 - 1) \equiv (n_1 \cdot n_2 \cdot \ldots \cdot n_s)^2 - 1 \pmod{16} \tag{12.27}$$

na mocy założenia indukcyjnego, a ponieważ liczba $n_1 \cdot \ldots \cdot n_s$ jest nieparzysta, więc z kroku dla $s = 2$ mamy, że

$$[(n_1 \cdot n_2 \cdot \ldots \cdot n_s)^2 - 1] + (n_{s+1}^2 - 1) \equiv (n_1 \cdot \ldots \cdot n_s \cdot n_{s+1})^2 - 1 \pmod{16}.$$

Stąd i z (12.27) wynika, że wzór (12.26) zachodzi dla liczby $s + 1$.

Wobec tego na mocy zasady indukcji dowodzony wzór zachodzi dla każdego $s \in \mathbb{N}$. □

Twierdzenie 12.37. *Dla dowolnej nieparzystej liczby naturalnej $m > 1$ zachodzi wzór:*

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1, & \text{jeśli } m \equiv 1, 7 \pmod 8 \\ -1, & \text{jeśli } m \equiv 3, 5 \pmod 8 \end{cases}. \tag{12.28}$$

Dowód. Oczywiście $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ dla pewnych $p_1, \ldots, p_s \in \mathbb{P} \setminus \{2\}$. Ponadto $(\frac{2}{p_i}) = (-1)^{\frac{p_i^2-1}{8}}$ dla każdego $i = 1, \ldots, s$ na mocy wzoru (12.14), więc ze wzoru (12.22) otrzymujemy, że

$$\left(\frac{2}{m}\right) = (-1)^{\frac{(p_1^2-1)+\ldots+(p_s^2-1)}{8}}.$$

Dalej, $(p_1^2-1)+\ldots+(p_s^2-1) = (p_1 \cdot \ldots \cdot p_s)^2 - 1 + 16k = m^2 - 1 + 16k$ dla pewnego $k \in \mathbb{Z}$ na mocy lematu 12.36, więc $\frac{(p_1^2-1)+\ldots+(p_s^2-1)}{8} = \frac{m^2-1}{8} + 2k$ i wobec tego $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

Uzasadnienie drugiej części wzoru (12.28) jest bardzo podobne do podanego w przykładzie 12.20, więc je pominiemy. □

Stwierdzenie 12.38. *Niech $m > 1$ będzie nieparzystą liczbą naturalną niepodzielną przez nieparzystą liczbę pierwszą q. Wówczas zachodzi wzór:*

$$\left(\frac{q}{m}\right) \cdot \left(\frac{m}{q}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{m-1}{2}}. \tag{12.29}$$

Dowód. Z założenia wynika, że $m = p_1 \cdot \ldots \cdot p_s$ dla pewnych nieparzystych liczb pierwszych $p_1, \ldots, p_s$ różnych od q. Ze wzoru (12.22) mamy, że

$$\left(\frac{q}{m}\right) = \left(\frac{q}{p_1}\right) \cdot \ldots \cdot \left(\frac{q}{p_s}\right).$$

Dodatkowo, na mocy stwierdzenia 12.33:

$$\left(\frac{m}{q}\right) = \left(\frac{p_1}{q}\right) \cdot \ldots \cdot \left(\frac{p_s}{q}\right).$$

Zatem $\left(\frac{q}{m}\right) \cdot \left(\frac{m}{q}\right)$ jest iloczynem s liczb postaci $\left(\frac{q}{p_i}\right) \cdot \left(\frac{p_i}{q}\right)$ dla $i = 1, \ldots, s$. Na mocy prawa wzajemności reszt kwadratowych $\left(\frac{q}{p_i}\right) \cdot \left(\frac{p_i}{q}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{p_i-1}{2}}$ dla $i = 1, \ldots, s$, więc

$$\left(\frac{q}{m}\right) \cdot \left(\frac{m}{q}\right) = (-1)^{\frac{q-1}{2} \cdot (\frac{p_1-1}{2} + \ldots + \frac{p_s-1}{2})}.$$

Dalej, $(p_1 - 1) + \ldots + (p_s - 1) = (p_1 \cdot \ldots \cdot p_s) - 1 + 4k = m - 1 + 4k$ dla pewnego $k \in \mathbb{Z}$ na mocy lematu 12.34, więc $\frac{p_1-1}{2} + \ldots + \frac{p_s-1}{2} = \frac{m-1}{2} + 2k$, a zatem $(-1)^{\frac{q-1}{2} \cdot (\frac{p_1-1}{2} + \ldots + \frac{p_s-1}{2})} = (-1)^{\frac{q-1}{2} \cdot \frac{m-1}{2}}$, co kończy nasz dowód. □

Następne twierdzenie nazywane jest **prawem wzajemności dla symboli Jacobiego**.

Twierdzenie 12.39. *Niech $m > 1$ i $n > 1$ będą względnie pierwszymi i nieparzystymi liczbami naturalnymi. Wówczas zachodzi wzór:*

$$\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}. \tag{12.30}$$

Dowód. Z założenia wynika, że $n = q_1 \cdot \ldots \cdot q_s$ dla pewnych nieparzystych liczb pierwszych $q_1, \ldots, q_s$, które nie są dzielnikami liczby m. Ze wzoru (12.22) mamy, że

$$\left(\frac{m}{n}\right) = \left(\frac{m}{q_1}\right) \cdot \ldots \cdot \left(\frac{m}{q_s}\right).$$

Dodatkowo, na mocy stwierdzenia 12.33:

$$\left(\frac{n}{m}\right) = \left(\frac{q_1}{m}\right) \cdot \ldots \cdot \left(\frac{q_s}{m}\right).$$

Zatem $\left(\frac{q}{m}\right) \cdot \left(\frac{m}{q}\right)$ jest iloczynem s liczb postaci $\left(\frac{m}{q_i}\right) \cdot \left(\frac{q_i}{m}\right)$ dla $i = 1, \ldots, s$. Na mocy stwierdzenia 12.38 mamy, że $\left(\frac{m}{q_i}\right) \cdot \left(\frac{q_i}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{q_i-1}{2}}$ dla $i = 1, \ldots, s$, więc

$$\left(\frac{q}{m}\right) \cdot \left(\frac{m}{q}\right) = (-1)^{\frac{m-1}{2} \cdot \left(\frac{q_1-1}{2} + \ldots + \frac{q_s-1}{2}\right)}.$$

Dalej, $(q_1 - 1) + \ldots + (q_s - 1) = (q_1 \cdot \ldots \cdot q_s) - 1 + 4k = n - 1 + 4k$ dla pewnego $k \in \mathbb{Z}$ na mocy lematu 12.34, więc $\frac{q_1-1}{2} + \ldots + \frac{q_s-1}{2} = \frac{n-1}{2} + 2k$, a zatem $(-1)^{\frac{m-1}{2} \cdot \left(\frac{q_1-1}{2} + \ldots + \frac{q_s-1}{2}\right)} = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$, co kończy nasz dowód. □

Dzięki wyprowadzonym przez nas własnościom symbolu Jacobiego można w wielu przypadkach znacząco uprościć obliczanie symbolu Legenre'a. Pokażemy to w następującym przykładzie.

Przykład 12.40. Sprawdzimy, czy ma rozwiązanie kongruencja:

$$x^2 \equiv 506 \pmod{1103}.$$

Korzystając z algorytmu Euklidesa wyliczamy, że $\mathrm{NWD}(506, 1103) = \mathrm{NWD}(506, 91) = \mathrm{NWD}(91, 51) = \mathrm{NWD}(51, 11) = \mathrm{NWD}(11, 4) = 1$. Teraz obliczamy symbol Jacobiego $(\frac{506}{1103})$. Ponieważ $1103 \equiv 3 \pmod 8$ oraz $506 = 2 \cdot 253$, więc ze stwierdzenia 12.33 i ze wzoru (12.28) uzyskujemy, że $(\frac{506}{1103}) = (\frac{253}{1103})$. Dalej, $253 \equiv 1 \pmod 4$, więc ze wzoru (12.30) jest $(\frac{253}{1103}) = (\frac{1103}{253})$, ale $1103 \equiv 91 \pmod{253}$, więc $(\frac{1103}{253}) = (\frac{91}{253}) = (\frac{253}{91})$ na mocy stwierdzenia 12.31 i twierdzenia 12.39. Dalej, $253 \equiv -20 \pmod{91}$, skąd $(\frac{253}{91}) = (\frac{-20}{91})$ na mocy stwierdzenia 12.31. Ponieważ $-20 = (-1) \cdot 2^2 \cdot 5$, więc ze stwierdzeń 12.33 i 12.32 mamy, że $(\frac{-20}{91}) = (\frac{-1}{91}) \cdot (\frac{5}{91})$. Dalej, $91 \equiv 3 \pmod 4$, więc $(\frac{-1}{91}) = -1$ ze stwierdzenia 12.35 oraz $5 \equiv 1 \pmod 4$, więc $(\frac{5}{91}) = (\frac{91}{5}) = (\frac{1}{5}) = 1$ na mocy twierdzenia 12.39 i stwierdzenia 12.33. Ostatecznie uzyskujemy, że $(\frac{506}{1103}) = -1$, a zatem na mocy stwierdzenia 12.30 nasza kongruencja nie posiada rozwiązania.

Zauważmy jeszcze to, że dzięki własnościom symbolu Jacobiego nie musieliśmy sprawdzać, czy 1103 jest liczbą pierwszą, co dla dużych liczb jest bardzo pracochłonne.

Przykład 12.41. Wykorzystując symbol Jacobiego pokażemy, że $2^m - 1 \nmid 3^n - 1$ dla dowolnych liczb naturalnych m, n takich, że $m \geqslant 2$ i $2 \nmid n$. Przypuśćmy, że takie, m oraz n istnieją. Wtedy $3^n \equiv 1 \pmod{2^m - 1}$, więc $1 = (\frac{1}{2^m-1}) = (\frac{3^n}{2^m-1}) = (\frac{3}{2^m-1})^n$. Zatem z nieparzystości n, $(\frac{3}{2^m-1}) = 1$. Z drugiej strony, z twierdzenia 12.39:

$$\left(\frac{3}{2^m-1}\right) \cdot \left(\frac{2^m-1}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{2^m-2}{2}} = (-1)^{2^{m-1}-1} = -1,$$

ponieważ $m \geqslant 2$. Wobec tego $(\frac{2^m-1}{3}) = -1$ i $3 \nmid 2^m - 1$ oraz $2^m - 1 \equiv 2 \pmod 3$, bo każda niereszta kwadratowa modulo 3 przystaje do 2 modulo 3 na mocy przykładu 12.13. Stąd $2^m \equiv 0 \pmod 3$, co prowadzi do sprzeczności.

Ćwiczenie 12.42. Czy kongruencja $x^2 \equiv -903 \pmod{2111}$ ma rozwiązanie?

Ćwiczenie 12.43. Obliczyć symbol Jacobiego $\left(\frac{150}{7063}\right)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 13

Sumy kwadratów liczb całkowitych

Już Diofantos zajmował się problemem przedstawiania liczb naturalnych w postaci sumy kwadratów. Rozkwit badań w tym temacie nastąpił dzięki tłumaczeniu tekstów Diofantosa przez Claude'a Gasparda Bacheta na język łaciński, które zostało sporządzone w 1621 roku. Wywarło to duży wpływ na Fermata, który dzięki metodzie „zejścia" potrafił udowodnić, że każda liczba pierwsza postaci $4k + 1$ jest sumą kwadratów dwóch liczb naturalnych, lecz nie opublikował swego dowodu. Duży wkład w tę tematykę wniósł Euler, który w 1749 udowodnił twierdzenie Fermata o dwóch kwadratach i uzyskał jeszcze wiele innych ciekawych wyników, które zostaną przedstawione poniżej.

13.1 Sumy dwóch kwadratów

Lemat 13.1. *Załóżmy, że liczba naturalna m jest sumą kwadratów dwóch liczb całkowitych i $p \equiv 3 \pmod 4$ jest dzielnikiem pierwszym liczby m. Wówczas $\alpha_p(m)$ jest liczbą parzystą.*

Dowód. Z założenia $m = x^2 + y^2$ dla pewnych $x, y \in \mathbb{Z}$. Najpierw przez indukcję względem $k \in \mathbb{N}_0$ przy dowolnych $x, y \in \mathbb{Z}$ udowodnimy, że jeśli $p^{2k+1} \mid x^2 + y^2$, to $p^{k+1} \mid x$ i $p^{k+1} \mid y$. Dla $k = 0$ teza wynika od

razu z przykładu 10.39. Niech teraz teza zachodzi dla pewnego $k \in \mathbb{N}_0$ i załóżmy, że $p^{2k+3} \mid x^2+y^2$. Z przykładu 10.39 wynika, że $x = pa$ i $y = pb$ dla pewnych $a, b \in \mathbb{Z}$. Zatem $p^{2k+3} \mid p^2(a^2+b^2)$, skąd $p^{2k+1} \mid a^2+b^2$ i z założenia indukcyjnego $a = p^{k+1}u$ oraz $b = p^{k+1}v$ dla pewnych $u, v \in \mathbb{Z}$. Wobec tego $x = p^{k+2}u$ i $y = p^{k+2}v$, czyli teza zachodzi dla liczby $k+1$ i na mocy zasady indukcji teza zachodzi dla dowolnego $k \in \mathbb{N}_0$.

Przypuśćmy teraz, że liczba $\alpha_p(m)$ jest nieparzysta. Wtedy $\alpha_p(m) = 2k+1$ dla pewnego $k \in \mathbb{N}_0$ i $p^{2k+1} \mid x^2+y^2$, więc z pierwszej części dowodu $x = p^{k+1}u$ i $y = p^{k+1}v$ dla pewnych $u, v \in \mathbb{Z}$. Zatem $m = p^{2k+2}(u^2+v^2)$, skąd $p^{\alpha_p(m)+1} \mid m$, co prowadzi do sprzeczności i kończy dowód. □

Lemat 13.2. *Jeżeli liczby naturalne $a_1, \ldots, a_n$ są sumami kwadratów dwóch liczb całkowitych, to $a_1 \cdot \ldots \cdot a_n$ też jest sumą kwadratów dwóch liczb całkowitych.*

Dowód. Z tożsamości $(a^2+b^2)\cdot(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$ wynika, że teza zachodzi dla $n = 2$. Przypuśćmy, że teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ i niech liczby naturalne $a_1, \ldots, a_n, a_{n+1}$ będą sumami kwadratów dwóch liczb całkowitych. Wtedy $a_{n+1} = c^2+d^2$ dla pewnych $c, d \in \mathbb{Z}$ i $a_1 \cdot \ldots \cdot a_n = a^2+b^2$ dla pewnych $a, b \in \mathbb{Z}$. Wobec tego $a_1 \cdot \ldots \cdot a_n \cdot a_{n+1} = (ac+bd)^2+(ad-bc)^2$, czyli teza zachodzi dla liczby $n+1$, co na mocy zasady indukcji kończy dowód. □

Twierdzenie 13.3. *Liczba naturalna m jest sumą kwadratów dwóch liczb całkowitych wtedy i tylko wtedy, gdy liczba $\alpha_p(m)$ jest parzysta dla każdej liczby pierwszej $p \equiv 3 \pmod 4$.*

Dowód. Załóżmy, że $\alpha_p(m)$ jest parzyste dla każdej liczby pierwszej $p \equiv 3 \pmod 4$. Z twierdzenia o jednoznaczności rozkładu wynika, że istnieje niepusty i skończony podzbiór X zbioru $\mathbb{P}$ taki, że m jest iloczynem liczb postaci $p^{\alpha_p(m)}$ dla $p \in X$. Jeśli $\alpha_p(m) = 0$, to $p^{\alpha_p(m)} = 1 = 0^2+1^2$. Niech dalej $\alpha_p(m) > 0$. Jeśli $p = 2$, to $p = 1^2+1^2$ i z lematu 13.2 mamy, że $p^{\alpha_p(m)} = x^2+y^2$ dla pewnych $x, y \in \mathbb{Z}$. Jeśli $p \equiv 1 \pmod 4$, to $p = a^2+b^2$ dla pewnych $a, b \in \mathbb{N}$ na mocy twierdzenia Fermata o dwóch kwadratach, więc $p^{\alpha_p(m)} = x^2+y^2$ dla pewnych

$x, y \in \mathbb{Z}$ na mocy lematu 13.2. Jeśli $p \equiv 3 \pmod 4$, to $\alpha_p(m) = 2s$ dla pewnego $s \in \mathbb{N}$, więc $p^{\alpha_p(m)} = 0^2 + (p^k)^2$. W ten sposób pokazaliśmy, że dla każdego $p \in X$ liczba $p^{\alpha_p(m)}$ jest sumą kwadratów dwóch liczb całkowitych. Zatem z lematu 13.2 liczba m też jest sumą kwadratów dwóch liczb całkowitych.

Implikacja odwrotna wynika od razu z lematu 13.1. □

Przykład 13.4. Pokażemy, że dla każdego $k \in \mathbb{N}_0$ liczba $m = 9k + 3$ nie jest sumą kwadratów dwóch liczb całkowitych. W tym celu wystarczy zauważyć, że $3 \mid m$ i $3^2 \nmid m$, skąd $\alpha_3(m) = 1$ jest liczbą nieparzystą, czyli teza wynika z twierdzenia 13.3.

Zauważmy jeszcze, że nie istnieją $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ takie, że każdy wyraz ciągu $(an + b)$ jest sumą kwadratów dwóch liczb całkowitych. Rzeczywiście, z ćwiczenia 10.41 istnieje liczba pierwsza $p > a$ taka, że $p \equiv 3 \pmod 4$, więc $p \nmid a$, skąd $ak \equiv -b \pmod p$ dla pewnego $k \in \mathbb{Z}$. Ponadto $m = k + na \in \mathbb{N}$ dla pewnego $n \in \mathbb{N}$, skąd wynika, że $p \mid am + b$ i $p \mid a(m + p) + b$. Jeśli $am + b$ i $a(m + p) + b$ są sumami kwadratów dwóch liczb całkowitych, to na mocy twierdzenia 13.3 te liczby są podzielne przez p^2. Zatem ich różnica, czyli liczba ap też jest podzielna przez p^2, co prowadzi do sprzeczności, gdyż $p > a > 0$.

Przykład 13.5. Pokażemy, że dla nieskończenie wielu liczb naturalnych n każda z liczb n, $n + 1$ i $n + 2$ jest sumą kwadratów dwóch liczb całkowitych. Rzeczywiście, łatwo zauważyć, że dla dowolnego $s \in \mathbb{N}$ oraz dla $n = 4(s^2 + s)^2$ mamy, że $n = (2s^2 + 2s)^2 + 0^2$, $n + 1 = (2s^2 + 2s)^2 + 1^2$ i $n + 2 = (2s^2 + 2s - 1)^2 + (2s + 1)^2$.

Zauważmy jeszcze, że dla każdej liczby naturalnej n pewna z liczb n, $n + 1$, $n + 2$ i $n + 3$ przystaje do 3 modulo 4 i zgodnie z zadaniem 22.73 nie jest ona sumą kwadratów dwóch liczb całkowitych.

Teraz opiszemy liczby naturalne, które są sumami kwadratów dwóch względnie pierwszych liczb całkowitych.

Stwierdzenie 13.6. *Niech p będzie liczbą pierwszą taką, że $p \equiv 1 \pmod 4$. Jeżeli $a, b, c, d \in \mathbb{N}$ i $p = a^2 + b^2 = c^2 + d^2$ oraz $a \geqslant b$ i $c \geqslant d$, to $a = c$ i $b = d$.*

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dowód. Zauważmy, że $p^2 = (a^2+b^2)\cdot(c^2+d^2) = (ac-bd)^2+(ad+bc)^2 = (ac+bd)^2+(ad-bc)^2$ oraz $(ac-bd)\cdot(ac+bd) = a^2c^2-b^2d^2 = a^2(p-d^2)-(p-a^2)d^2 = p(a^2-d^2)$, skąd $p \mid ac-bd$ lub $p \mid ac+bd$. Jeśli $p \mid ac-bd$, to ponieważ $p^2 = (ac-bd)^2+(ad+bc)^2$, więc p dzieli $ad+bc$, skąd $ad+bc \geqslant p$ i w konsekwencji tego $ac-bd = 0$. Zatem $ac = bd$. Z pierwszości p wynika, że $\mathrm{NWD}(a,b) = \mathrm{NWD}(c,d) = 1$, więc z zasadniczego twierdzenia arytmetyki $a \mid d$ i $d \mid a$, czyli $a = d$, skąd $b = c$, co przeczy temu, że $a > b$ i $c > d$. Wobec tego $p \mid ac+bd$ i z równości $p^2 = (ac+bd)^2+(ad-bc)^2$ dostajemy, że $ad-bc = 0$, skąd $ad = bc$ i znowu z zasadniczego twierdzenia arytmetyki otrzymujemy, że $a = c$ i $b = d$. □

Stwierdzenie 13.7. *Niech p będzie liczbą pierwszą taką, że $p \equiv 1 \mod 4$. Wówczas dla dowolnego $n \in \mathbb{N}$ istnieją względnie pierwsze liczby naturalne x i y takie, że $p^n = x^2+y^2$.*

Dowód. Na mocy twierdzenia Fermata o dwóch kwadratach $p = a^2+b^2$ dla pewnych $a, b \in \mathbb{N}$. Stąd i z pierwszości liczby p wynika, że $\mathrm{NWD}(a,b) = 1$, czyli teza zachodzi dla $n = 1$.

Załóżmy, że dla pewnej liczby naturalnej n istnieją względnie pierwsze liczby naturalne c i d takie, że $p^n = c^2+d^2$. Wtedy $p^{n+1} = (a^2+b^2)\cdot(c^2+d^2) = (ac-bd)^2+(ad+bc)^2 = (ac+bd)^2+(ad-bc)^2$. Przypuśćmy, że $p \mid ac-bd$ i $p \mid ac+bd$. Wtedy p dzieli sumę tych liczb, czyli $p \mid 2ac$, skąd $p \mid a$ lub $p \mid c$. Ponadto $p = a^2+b^2$ i $p^n = c^2+d^2$, więc $p \mid b$ lub $p \mid d$, co przeczy temu, że $\mathrm{NWD}(a,b) = \mathrm{NWD}(c,d) = 1$. Wobec tego $p \nmid ac-bd$ lub $p \nmid ac+bd$. Pokażemy, że w pierwszym przypadku liczby $ac-bd$ i $ac+bd$ są względnie pierwsze. Gdyby tak nie było, to te liczby miałyby wspólny dzielnik pierwszy q, który dzieli liczbę p^{n+1}, a więc $q = p$, skąd $p \mid ac-bd$, wbrew założeniu. Natomiast w drugim przypadku pokazujemy analogicznie, że liczby $ac+bd$ i $ad-bc$ są względnie pierwsze. Dodatkowo w pierwszym przypadku $ac-bd \neq 0$, skąd $|ac-bd| \in \mathbb{N}$ oraz w drugim $ad-bc \neq 0$, skąd $|ad-bc| \in \mathbb{N}$. Oznacza to, że teza zachodzi dla liczby $n+1$.

Zatem na mocy zasady indukcji stwierdzenie zachodzi dla każdego $n \in \mathbb{N}$. □

Lemat 13.8. *Jeżeli względnie pierwsze liczby naturalne n i m są sumami kwadratów dwóch względnie pierwszych liczb całkowitych, to $m \cdot n$ też jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych.*

Dowód. Z założenia wynika, że $m = a^2 + b^2$ i $n = c^2 + d^2$ dla pewnych $a, b, c, d \in \mathbb{N}$ takich, że $\mathrm{NWD}(a, b) = \mathrm{NWD}(c, d) = 1$. Zauważmy, że $m \cdot n = (a^2 + b^2) \cdot (c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

Jeśli liczby $ac - bd$ i $ad + bc$ nie są względnie pierwsze, to posiadają wspólny dzielnik pierwszy p, który dzieli liczbę $m \cdot n$. Stąd $p \mid m$ lub $p \mid n$. Niech $p \mid m$. Wtedy $p \mid a^2 + b^2$, $p \mid ac - bd$ i $p \mid ad + bc$, skąd $bd^2 \equiv acd \pmod{p}$ i $acd \equiv -bc^2 \pmod{p}$. Zatem $bd^2 \equiv -bc^2 \pmod{p}$, ale $p \nmid b$, gdyż $p \mid a^2 + b^2$ i $\mathrm{NWD}(a, b) = 1$, więc $d^2 \equiv -c^2 \pmod{p}$. Stąd $p \mid c^2 + d^2$, czyli $p \mid n$ i mamy sprzeczność z tym, że $\mathrm{NWD}(m, n) = 1$. Wobec tego $p \mid n$. Stąd $d^2 \equiv -c^2 \pmod{p}$, $a^2 c \equiv abd \pmod{p}$ i $abd \equiv -b^2 c \pmod{p}$. Zatem $a^2 c \equiv -b^2 c \pmod{p}$, a ponieważ $p \mid c^2 + d^2$ i $\mathrm{NWD}(c, d) = 1$, więc $p \nmid c$ i stąd $a^2 \equiv -b^2 \pmod{p}$, czyli $p \mid m$, co przeczy temu, że $\mathrm{NWD}(m, n) = 1$.

Zatem liczby $ac - bd$ i $ad + bc$ są względnie pierwsze, co kończy dowód lematu. □

Z lematu 13.8 i ze stwierdzenia 8.49 przez prostą indukcję uzyskujemy następujące

Stwierdzenie 13.9. *Niech $a_1, \ldots, a_n$ będą parami względnie pierwszymi liczbami naturalnymi. Jeżeli każda z tych liczb jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych, to ich iloczyn $a_1 \cdot \ldots \cdot a_n$ też jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych.*

Twierdzenie 13.10. (Eulera). *Liczba naturalna m jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych wtedy i tylko wtedy, gdy m nie posiada dzielnika pierwszego postaci $4k+3$ oraz $4 \nmid m$.*

Dowód. $\Leftarrow$. Dla $m = 1$ mamy $m = 0^2 + 1^2$, a dla $m = 2$ jest $m = 1^2 + 1^2$. Niech dalej $m > 2$. Wtedy z twierdzenia o jednoznaczności rozkładu $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ albo $m = 2 \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ dla pewnych liczb naturalnych

$s, \alpha_1, \ldots, \alpha_s$ i dla pewnych różnych liczb pierwszych $p_1, \ldots, p_s$ postaci $4k+1$. Zatem na mocy stwierdzenia 13.7 i lematu 13.9 liczba m jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych.

$\Rightarrow$. Niech $m \in \mathbb{N}$ i $m = a^2 + b^2$, gdzie $a, b \in \mathbb{Z}$ i $\mathrm{NWD}(a,b) = 1$. Przypuśćmy, że istnieje liczba pierwsza $p \equiv 3 \pmod 4$ taka, że $p \mid m$. Wtedy $p \mid a$ i $p \mid b$ na mocy przykładu 10.39, co prowadzi do sprzeczności. Jeśli $4 \mid m$, to liczba $a^2 + b^2$ jest parzysta, więc liczby a i b są tej samej parzystości, a ponieważ są one względnie pierwsze, więc $2 \nmid a$ i $2 \nmid b$. Zatem z zadania 22.13 mamy, że $a^2 + b^2 \equiv 1 + 1 = 2 \pmod 4$, co przeczy temu, że $4 \mid a^2 + b^2$. Wobec tego $4 \nmid m$. □

Następne dwa stwierdzenia opisują liczby naturalne, które są sumami kwadratów dwóch liczb naturalnych.

Wniosek 13.11. *Dla $m \in \mathbb{N}$ liczba m^2 jest sumą kwadratów dwóch liczb naturalnych wtedy i tylko wtedy, gdy m posiada dzielnik pierwszy $p \equiv 1 \pmod 4$.*

Dowód. Niech $m^2 = a^2 + b^2$ dla pewnych $a, b \in \mathbb{N}$. Niech $d = \mathrm{NWD}(a,b)$. Wtedy $d^2 \mid m^2$, więc $m = d \cdot n$ dla pewnego $n \in \mathbb{N}$. Ponadto $a = dx$ i $b = dy$ dla pewnych względnie pierwszych $x, y \in \mathbb{N}$ oraz $n^2 = x^2 + y^2$. Stąd $n > 1$, bo $x^2 + y^2 \geqslant 2$. Z twierdzenia 13.10 wynika, że $4 \nmid n^2$, czyli $2 \nmid n$ oraz n^2 nie posiada dzielnika pierwszego postaci $4k+3$. Ponadto $n > 1$, więc liczba n musi posiadać dzielnik pierwszy $p \equiv 1 \pmod 4$.

Na odwrót, niech liczba pierwsza $p \equiv 1 \pmod 4$ będzie dzielnikiem liczby m. Wtedy $m = pn$ dla pewnego $n \in \mathbb{N}$ i ze stwierdzenia 13.7 wynika, że $p^2 = a^2 + b^2$ dla pewnych $a, b \in \mathbb{N}$. Stąd $m^2 = (an)^2 + (bn)^2$, co kończy dowód. □

Wniosek 13.12. *Załóżmy, że liczba naturalna n nie jest kwadratem liczby naturalnej. Wówczas liczba n jest sumą kwadratów dwóch liczb naturalnych wtedy i tylko wtedy, gdy liczba $\alpha_p(n)$ jest parzysta dla każdej liczby pierwszej $p \equiv 3 \pmod 4$.*

Dowód. $\Leftarrow$. Na mocy twierdzenia 13.3 mamy, że $n = x^2 + y^2$ dla pewnych $x, y \in \mathbb{Z}$. Stąd $n = |x|^2 + |y|^2$, a ponieważ $n \neq k^2$ dla $k \in \mathbb{N}$,

więc $|x|, |y| \in \mathbb{N}$. Implikacja odwrotna wynika od razu z twierdzenia 13.3. □

Przykład 13.13. Uzasadnimy, że liczba naturalna n jest sumą kwadratów dwóch względnie pierwszych liczb naturalnych wtedy i tylko wtedy, gdy $n > 1$, $4 \nmid n$ oraz n nie posiada dzielnika pierwszego postaci $4k + 3$. Jeśli $n = a^2 + b^2$, gdzie $a, b \in \mathbb{N}$ i $\mathrm{NWD}(a, b) = 1$, to $n \geqslant 1^2 + 1^2 = 2$ i na mocy twierdzenia 13.10 liczba n nie posiada dzielnika pierwszego postaci $4k + 3$ i $4 \nmid n$. Na odwrót, niech $n > 1$, $4 \nmid n$ i n nie posiada dzielnika pierwszego postaci $4k+3$. Wtedy z twierdzenia 13.10 istnieją względnie pierwsze nieujemne liczby całkowite a i b takie, że $a^2+b^2 = n$. Jeśli $a = 0$, to $1 = \mathrm{NWD}(a, b) = b$, skąd $n = 1$, co prowadzi do sprzeczności. Podobnie pokazujemy, że $b \neq 0$. Wobec tego $a, b \in \mathbb{N}$.

Ćwiczenie 13.14. Znajdź dwie różne pary (a, b) liczb naturalnych takich, że $365 = a^2 + b^2$.

Opisanie wszystkich liczb naturalnych, które są sumami kwadratów trzech liczb całkowitych jest o wiele bardziej skomplikowane niż w przypadku liczb będących sumami kwadratów dwóch liczb całkowitych. Problem ten rozwiązał Gauss udowadniając, że liczba naturalna a jest sumą kwadratów trzech liczb całkowitych wtedy i tylko wtedy, gdy $a \neq 4^h(8k+7)$ dla dowolnych $h, k \in \mathbb{N}_0$. Współczesny dowód tego twierdzenia można znaleźć na przykład w [28]. Trudności polegają między innymi na tym, że iloczyn liczb naturalnych będących sumami kwadratów trzech liczb całkowitych nie musi być sumą kwadratów trzech liczb całkowitych, co widać na przykładzie liczb $3 = 1^2 + 1^2 + 1^2$ oraz $5 = 0^2 + 1^2 + 2^2$, gdyż $3 \cdot 5 = 8 \cdot 1 + 7$, a z twierdzenia Gaussa wiemy, że liczba $8k + 7$ dla każdego $k \in \mathbb{N}_0$ nie jest sumą kwadratów trzech liczb całkowitych. Dowód jednej z implikacji w twierdzeniu Gaussa jest bardzo prosty. Teraz go przedstawimy.

Stwierdzenie 13.15. *Dla dowolnych nieujemnych liczb całkowitych h i k liczba $4^h(8k + 7)$ nie jest sumą kwadratów trzech liczb całkowitych.*

Dowód. Przypuśćmy, że istnieje $k \in \mathbb{N}_0$ takie, że $8k+7 = a^2+b^2+c^2$ dla pewnych $a, b, c \in \mathbb{Z}$. Wtedy, albo wszystkie liczby a, b, c są nieparzyste,

albo dwie z nich są parzyste, a trzecia jest nieparzysta. W pierwszym przypadku z zadania 22.13 uzyskujemy, że $8k+7 = a^2+b^2+c^2 \equiv \equiv 3 \pmod 8$, co prowadzi do sprzeczności, a w drugim przypadku na mocy zadania 22.13 jest $8k+7 = a^2+b^2+c^2 \equiv 0+0+1 \equiv 1 \pmod 4$, co też prowadzi do sprzeczności. W ten sposób wykazaliśmy nasze stwierdzenie dla $h = 0$.

Załóżmy, że $4^h(8k+7) = x^2+y^2+z^2$ dla pewnych $h \in \mathbb{N}$, $k \in \mathbb{N}_0$ oraz $x, y, z \in \mathbb{Z}$. Na mocy zasady minimum możemy bez zmniejszania ogólności zakładać, że liczba h jest najmniejsza z możliwych. Ponieważ $4 \mid x^2+y^2+z^2$, więc albo wszystkie liczby x, y i z są parzyste albo dwie z nich są nieparzyste, a trzecia z nich jest parzysta. Jednak w tym drugim przypadku na mocy zadania 22.13 jest $x^2+y^2+z^2 \equiv 0+1+1 \equiv 2 \pmod 4$, co prowadzi do sprzeczności, więc $x = 2a$, $y = 2b$ i $z = 2c$ dla pewnych $a, b, c \in \mathbb{Z}$. Stąd $4^{h-1}(8k+7) = a^2+b^2+c^2$ i z minimalności h mamy, że $h-1 \notin \mathbb{N}$, czyli $h-1 = 0$ oraz $8k+7 = a^2+b^2+c^2$, co jak pokazaliśmy wcześniej, jest niemożliwe. □

Przykład 13.16. Udowodnimy, że dla każdego $n \in \mathbb{N}$ liczba $2^{2n+1} = (2^n)^2+(2^n)^2$ nie jest sumą kwadratów trzech liczb naturalnych. Przypuśćmy, że tak nie jest. Wtedy na mocy zasady minimum istnieje najmniejsza liczba naturalna m taka, że $2^{2m+1} = a^2+b^2+c^2$ dla pewnych $a, b, c \in \mathbb{N}$. Ponieważ liczba $a^2+b^2+c^2$ jest parzysta, więc albo wszystkie liczby a, b, c są parzyste, albo dwie z nich są nieparzyste i trzecia jest parzysta. W drugim przypadku $a^2+b^2+c^2 \equiv 0+1+1 \equiv 2 \pmod 4$, co przeczy temu, że $4 \mid a^2+b^2+c^2$, gdyż $a^2+b^2+c^2 = 2^{2m+1}$. Stąd $a = 2x$, $b = 2y$ i $c = 2z$ dla pewnych $x, y, z \in \mathbb{N}$ oraz $2^{2(m-1)+1} = x^2+y^2+z^2$. Zatem z minimalności liczby m wynika stąd, że $m-1 \notin \mathbb{N}$, czyli $m = 1$ i $2 = x^2+y^2+z^2 \geqslant 3$, co prowadzi do sprzeczności.

Ćwiczenie 13.17. Niech $n \in \mathbb{N}$. Udowodnij, że jeżeli $4n$ jest sumą kwadratów dwóch (trzech) liczb naturalnych, to n też jest sumą kwadratów dwóch (trzech) liczb naturalnych.

Ćwiczenie 13.18. Niech $n \in \mathbb{N}$. Udowodnij, że liczba 4^n nie jest sumą kwadratów ani dwóch ani trzech liczb naturalnych.

Ćwiczenie 13.19. Przedstaw liczbę 3146 w postaci sumy kwadratów dwóch liczb naturalnych.

13.2 Sumy czterech kwadratów

Już Diofantos w swoim dziele *Arithmetica* opisywał przypadki, w których liczbę naturalną można rozpisać na sumę czterech kwadratów. Claude Gaspard Bachet (tłumacz dzieł Diofantosa na łacinę) w 1621 roku wypowiedział hipotezę, że każda liczba naturalna jest sumą kwadratów czterech liczb całkowitych i sprawdził jej prawdziwość dla bardzo wielu liczb. Stąd też czasem tę hipotezę nazywa się twierdzeniem Bacheta. Fermat na marginesie książki Diofantosa napisał, że umie udowodnić tę hipotezę metodą zejścia, ale tego nie opublikował. Następny krok zrobił Euler, który za pomocą odkrytej przez siebie tożsamości (patrz wzór (13.1) pokazał, że każda dodatnia liczba wymierna jest sumą kwadratów czterech liczb wymiernych. Dopiero w roku 1770 Joseph Louis Lagrange dowiódł prawdziwości hipotezy Bacheta i od tej pory nazywamy ją **twierdzeniem Lagrange'a o czterech kwadratach**.

Twierdzenie 13.20. *Każda liczba naturalna jest sumą kwadratów czterech liczb całkowitych.*

Dowód tego pięknego twierdzenia Lagrange oparł na następującej tożsamości odkrytej przez Eulera:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2, \quad (13.1)$$

gdzie

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \quad z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \quad (13.2)$$

$$z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4, \quad z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2. \quad (13.3)$$

Pozostaje tajemnicą, w jaki sposób Euler odkrył te wzory, nazywane **tożsamością Eulera**. Współcześnie wiemy, że można je wyprowadzić

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

za pomocą własności tak zwanych kwaternionów Hamiltona. Sprawdzenie poprawności tych wzorów opiera się na wzorze $(a+b+c+d)^2 = a^2+b^2+c^2+d^2+2ab+2ac+2ad+2bc+2bd+2cd$ i na obserwacji, że wszystkie podwojone iloczyny występujące w prawej stronie wzoru (13.1) się skrócą, a pozostaną jedynie wyrażenia postaci $x_i^2 y_j^2$ dla wszystkich $i, j \in \{1,2,3,4\}$, których suma jest równa lewej stronie tego wzoru. Sprawdzenie szczegółów zostawiamy Czytelnikowi (proponujemy rozłożyć poziomo kartkę A4 i zastosować podane przez nas wskazówki).

Z tożsamości Eulera wynika przez prostą indukcję, że jeżeli liczby naturalne $a_1, \ldots, a_n$ są sumami kwadratów czterech liczb całkowitych, to ich iloczyn też jest sumą kwadratów czterech liczb całkowitych. Ponadto $1 = 0^2+0^2+0^2+1^2$ i $2 = 0^2+0^2+1^2+1^2$, więc na mocy twierdzenia o jednoznaczności rozkładu twierdzenie Lagrange'a będzie udowodnione, jeżeli pokażemy, że każda nieparzysta liczba pierwsza jest sumą kwadratów czterech liczb całkowitych. Potrzebujemy do tego dwóch lematów.

Lemat 13.21. *Niech $n \in \mathbb{N}$ będzie takie, że $2n = x^2+y^2+z^2+t^2$ dla pewnych $x, y, z, t \in \mathbb{Z}$. Wtedy n też jest sumą kwadratów czterech liczb całkowitych.*

Dowód. Ponieważ liczba $x^2+y^2+z^2+t^2$ jest parzysta, więc albo każda z liczb x, y, z, t jest parzysta, albo dokładnie dwie z nich są parzyste, albo wszystkie te liczby są nieparzyste. Zatem bez zmniejszania ogólności możemy zakładać, że liczby x i y są tej samej parzystości oraz liczby z i t też są tej samej parzystości. Stąd liczby $\frac{x+y}{2}$, $\frac{x-y}{2}$, $\frac{z+t}{2}$ i $\frac{z-t}{2}$ są całkowite oraz $\frac{x^2+y^2}{2} = (\frac{x+y}{2})^2 + (\frac{x-y}{2})^2$ i $\frac{z^2+t^2}{2} = (\frac{z+t}{2})^2 + (\frac{z-t}{2})^2$, więc $n = (\frac{x+y}{2})^2 + (\frac{x-y}{2})^2 + (\frac{z+t}{2})^2 + (\frac{z-t}{2})^2$, co kończy dowód. □

Lemat 13.22. *Dla każdej nieparzystej liczby pierwszej p istnieje liczba naturalna $m < \frac{p}{2}$ oraz istnieją liczby całkowite x i y takie, że $mp = x^2+y^2+1$.*

Dowód. Rozważmy liczby $0^2, 1^2, \ldots, (\frac{p-1}{p})^2$. Weźmy $i, j = 0, 1, \ldots, \frac{p-1}{2}$ takie, że $p \mid i^2-j^2$. Ponieważ $i^2-j^2 = (i-j)\cdot(i+j)$, więc z pierwszości p

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

mamy, że $p \mid i-j$ lub $p \mid i+j$. W pierwszym przypadku $i = [i]_p = [j]_p = j$, a w drugim, $i+j=0$, gdyż $0 \leqslant i+j < \frac{p}{2}+\frac{p}{2} = p$, więc $i=j=0$. Wobec tego każde dwie spośród liczb $0^2, 1^2, \ldots, (\frac{p-1}{p})^2$ dają różne reszty z dzielenia przez p. Wynika stąd, że liczby $1+0^2, 1+1^2, \ldots, 1+(\frac{p-1}{2})^2$ też dają różne reszty z dzielenia przez p oraz liczby $-0^2, -1^2, \ldots, -(\frac{p-1}{2})^2$ też dają różne reszty z dzielenia przez p. Mamy zatem dwa $1+\frac{p-1}{2} = \frac{p+1}{2}$ - elementowe podzbiory $A = \{[-0^2]_p, [-1^2]_p, \ldots, [-(\frac{p-1}{2})^2]_p\}$ oraz $B = \{[1+0^2]_p, [1+1^2]_p, \ldots, [1+(\frac{p-1}{2})^2]_p\}$ zbioru p - elementowego $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Jeśli $A \cap B = \emptyset$, to $|A \cup B| = |A| + |B| = p+1 > p$, co prowadzi do sprzeczności. Wobec tego istnieje $a \in A \cap B$, skąd istnieją $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$ takie, że $a = [-x^2]_p = [1+y^2]_p$. Zatem $1+y^2 \equiv -x^2 \pmod{p}$, skąd $p \mid x^2+y^2+1$. Zatem $x^2+y^2+1 = mp$ dla pewnego $m \in \mathbb{N}$, przy czym $0 \leqslant x, y \leqslant \frac{p-1}{2}$, więc $mp \leqslant 2 \cdot (\frac{p-1}{2})^2 + 1 = \frac{p^2-2p+3}{2} < \frac{p^2}{2}$, gdyż $p \geqslant 3$, skąd $m < \frac{p}{2}$. □

Teraz udowodnimy następujące stwierdzenie i w ten sposób zakończymy dowód twierdzenia Lagrange'a o czterech kwadratach.

Stwierdzenie 13.23. *Każda nieparzysta liczba pierwsza p jest sumą kwadratów czterech liczb całkowitych.*

Dowód. Na mocy lematu 13.22 i zasady minimum istnieje najmniejsza liczba naturalna $m < \frac{p}{2}$ taka, że $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ dla pewnych $x_1, x_2, x_3, x_4 \in \mathbb{Z}$. Z lematu 13.21 uzyskujemy, że liczba m jest nieparzysta. Przypuśćmy, że $m > 1$. Weźmy dowolne $r \in \mathbb{Z}_m$. Wtedy $r \in \{0, 1, \ldots, \frac{m-1}{2}\}$ lub $r = \frac{m-1}{2} + i$ dla pewnego $i = 1, \ldots, \frac{m-1}{2}$. W drugim przypadku $r \equiv r - m \pmod{m}$ oraz $-\frac{m-1}{2} \leqslant r - m < 0$. Wynika stąd, że dla dowolnego $k \in \mathbb{Z}$ istnieje liczba całkowita r taka, że $k \equiv r \pmod{m}$ oraz $|r| < \frac{m}{2}$. Wobec tego istnieją $y_1, y_2, y_3, y_4 \in \mathbb{Z}$ takie, że $|y_i| < \frac{m}{2}$ oraz $x_i \equiv y_i \pmod{m}$ dla $i = 1, 2, 3, 4$. Stąd $mp = x_1^2+x_2^2+x_3^2+x_4^2 \equiv y_1^2+y_2^2+y_3^2+y_4^2 \pmod{m}$, więc $y_1^2+y_2^2+y_3^2+y_4^2 = sm$ dla pewnego $s \in \mathbb{N}_0$, przy czym $y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4 \cdot \frac{m^2}{4}$, więc $s < m$.

Przypuśćmy, że $s = 0$. Wtedy $y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0$, skąd $y_1 = y_2 = y_3 = y_4 = 0$ i wobec tego $m^2 \mid x_1^2+x_2^2+x_3^2+x_4^2$, czyli $m^2 \mid mp$, a więc $m \mid p$. Ponadto $1 < m < p$ i $p \in \mathbb{P}$, więc prowadzi to do sprzeczności. Zatem $s \in \mathbb{N}$.

Dalej, z tożsamości Eulera mamy, że $sm^2p = (x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$, gdzie z_1, z_2, z_3, z_4 dane są wzorami (13.2)-(13.3). Dodatkowo $x_i \equiv y_i \pmod{m}$ dla $i = 1, 2, 3, 4$, więc $z_1 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}$, $z_2 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod{m}$, $z_3 \equiv x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4 \equiv 0 \pmod{m}$ oraz $z_4 \equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 \equiv 0 \pmod{m}$. Wobec tego $z_i = ma_i$, gdzie $a_i \in \mathbb{Z}$ dla $i = 1, 2, 3, 4$. Stąd $sm^2p = m^2(a_1^2 + a_2^2 + a_3^2 + a_4^2)$, czyli $sp = a_1^2 + a_2^2 + a_3^2 + a_4^2$, przy czym $s \in \mathbb{N}$ i $s < m$, co przeczy minimalności liczby m.

W konsekwencji tych rozważań mamy, że $m = 1$ i p jest sumą kwadratów czterech liczb całkowitych. □

Przykład 13.24. Udowodnimy, że dla każdego $n \in \mathbb{N}$ liczba 2^{2n+1} nie jest sumą kwadratów czterech liczb naturalnych. Przypuśćmy, że tak nie jest. Wtedy na mocy zasady minimum istnieje najmniejsza liczba naturalna m taka, że $2^{2m+1} = a^2 + b^2 + c^2 = d^2$ dla pewnych $a, b, c, d \in \mathbb{N}$. Ponieważ liczba $a^2 + b^2 + c^2 + d^2$ jest parzysta, więc albo wszystkie liczby a, b, c, d są parzyste, albo dwie z nich są nieparzyste i dwie są parzyste. W drugim przypadku $a^2 + b^2 + c^2 + d^2 \equiv 0 + 0 + 1 + 1 \equiv 2 \pmod{4}$, co przeczy temu, że $4 \mid a^2 + b^2 + c^2 + d^2$, gdyż $a^2 + b^2 + c^2 + d^2 = 2^{2m+1}$. Stąd $a = 2x$, $b = 2y$, $c = 2z$ i $d = 2t$ dla pewnych $x, y, z, t \in \mathbb{N}$ oraz $2^{2(m-1)+1} = x^2 + y^2 + z^2 + t^2$. Zatem z minimalności liczby m wynika stąd, że $m - 1 \notin \mathbb{N}$, czyli $m = 1$ i $2 = x^2 + y^2 + z^2 + t^2 \geqslant 4$, co prowadzi do sprzeczności.

Ćwiczenie 13.25. Przedstaw liczbę 2022 w postaci sumy kwadratów czterech liczb całkowitych. Czy ta liczba jest sumą kwadratów dwóch (trzech) liczb całkowitych?

Ćwiczenie 13.26. Przedstaw liczbę

$$(2022^2 + 2023^2 + 2024^2) \cdot (2025^2 + 2026^2 + 2027^2)$$

w postaci sumy kwadratów czterech liczb całkowitych. Czy ta liczba jest sumą kwadratów dwóch (trzech) liczb całkowitych?

Ćwiczenie 13.27. Udowodnij, że żadna z liczb 9, 11, 14 i 17 nie jest sumą kwadratów czterech liczb naturalnych.

13.3 Problem Waringa

Twierdzenie Lagrange'a o czterech kwadratach zainspirowało brytyjskiego matematyka Edwarda Waringa do wypowiedzenia już w 1770 roku wielu hipotez związanych z przedstawianiem liczb naturalnych w postaci sum n-tych potęg nieujemnych liczb całkowitych. Waring postulował (bez podania dowodów) między innymi, że każda liczba naturalna jest sumą sześcianów pewnych dziewięciu nieujemnych liczb całkowitych oraz każda liczba naturalna jest sumą bikwadratów (czyli czwartych potęg) pewnych dziewiętnastu nieujemnych liczb całkowitych. W języku współczesnym **hipotezę Waringa** formułuje się następująco: dla dowolnej liczby naturalnej $n \geqslant 2$ istnieje liczba naturalna k_n taka, że każda liczba naturalna jest sumą co najwyżej k_n, n-tych potęg pewnych liczb naturalnych. Najmniejszą z takich liczb k_n oznacza się tradycyjnie przez $g(n)$ i nazywa **stałą Waringa** dla wykładnika n. Z twierdzenia Lagrange'a o czterech kwadratach i tego, że 7 nie jest sumą kwadratów trzech liczb całkowitych wynika, że $g(2) = 4$. Problem czwartych potęg został zaatakowany w połowie XIX wieku przez Liouville'a, który uzyskał nierówność $g(4) \leqslant 53$. Pierwszy wynik dotyczący sześcianów pochodzi od E. Mailleta (1878): $g(3) \leqslant 21$. Tenże autor otrzymał w roku 1896 oszacowanie $g(5) \leqslant 192$. Istnienie liczby $g(8)$ udowodnił znów Maillet w roku 1907, $g(10)$ oszacował I. Schur (1909) i wreszcie $g(7)$ Wieferich (1909). W tym samym roku ukazała się fundamentalna praca D. Hilberta, zawierająca pełny dowód istnienia liczby $g(n)$ dla dowolnego n. Dowód Hilberta opierał się na obliczaniu skomplikowanych całek wielowymiarowych i był mało przejrzysty. W późniejszym okresie wielu matematyków wniosło istotne uproszczenia do tego dowodu. Tak zmodyfikowany dowód Hilberta twierdzenia, które dziś zwie się **twierdzeniem Waringa-Hilberta** przedstawiono w monografii [27]. Natomiast pierwszy elementarny dowód tego twierdzenia (chociaż nadal bardzo skomplikowany) odkrył radziecki matematyk Yurij Vladimirovich Linnik.

Przykład 13.28. Udowodnimy, że $g(n) \geqslant 2^n + \lfloor \frac{3^n}{2^n} \rfloor - 2$ dla każdej liczby naturalnej $n \geqslant 2$. Niech $N = 2^n \cdot \lfloor \frac{3^n}{2^n} \rfloor - 1$. Ponieważ $2^n \nmid 3^n$, więc $k = \lfloor \frac{3^n}{2^n} \rfloor \in \mathbb{N} < \frac{3^n}{2^n}$, skąd $N < 3^n$. Niech $s \in \mathbb{N}$ i niech $N =$

$= a_1^n + a_2^n + \ldots + a_s^n$ dla pewnych $a_1, a_2, \ldots, a_s \in \mathbb{N}_0$. Wtedy $a_i < 3$, więc $a_i \in \{0, 1, 2\}$ dla każdego $i = 1, 2, \ldots, s$. Dla $t \in \{0, 1, 2\}$ oznaczmy przez k_t liczbę wszystkich $i \in \{1, 2, \ldots, s\}$ takich, że $a_i = t$. Wtedy $k_0, k_1, k_2 \in \mathbb{N}_0$, $k_0 + k_1 + k_2 = s$ oraz $k_1 + k_2 \cdot 2^n = N$. Stąd $k_2 \cdot 2^n \leqslant N = 2^n \cdot k - 1$, czyli $k_2 \leqslant k - 1$. Jeśli $k_2 = k - 1$, to $k_1 = N - 2^n \cdot (k-1) = 2^n - 1$, skąd $s \geqslant k_1 + k_2 = 2^n + k - 2 = 2^n + \lfloor \frac{3^n}{2^n} \rfloor - 2$. Jeśli zaś $k_2 < k - 1$, to $k_1 \geqslant N - 2^n \cdot (k-2) = 2^n + 2^n - 1 > 2^n + k - 2$, bo $k = \lfloor \frac{3^n}{2^n} \rfloor < \frac{3^n}{2^n} < \frac{4^n}{2^n} = 2^n$, czyli wtedy $s \geqslant k_1 > 2^n + \lfloor \frac{3^n}{2^n} \rfloor - 2$. Oznacza to, że liczba N jest sumą $2^n + \lfloor \frac{3^n}{2^n} \rfloor - 2$ n tych potęg pewnych nieujemnych liczb całkowitych, ale N nie jest sumą mniej niż $2^n + \lfloor \frac{3^n}{2^n} \rfloor - 2$, n - tych potęg pewnych nieujemnych liczb całkowitych. Wobec tego $g(n) \geqslant 2^n + \lfloor \frac{3^n}{2^n} \rfloor - 2$.

Ćwiczenie 13.29. Udowodnij, że liczba 79 nie jest sumą osiemnastu czwartych potęg pewnych nieujemnych liczb całkowitych.

Ćwiczenie 13.30. Wykazać, że liczby 23 i 239 nie są sumami sześcianów ośmiu nieujemnych liczb całkowitych.

Ćwiczenie 13.31. Wyznacz liczbę naturalną, która nie jest sumą trzydziestu sześciu piątych potęg nieujemnych liczb całkowitych.

Przedstawimy teraz dowód Liouville'a nierówności $g(4) \leqslant 53$ oparty na twierdzeniu 13.20 Lagrange'a o czterech kwadratach.

Lemat 13.32. (Tożsamość Liouville'a). *Dla dowolnych zmiennych x_1, x_2, x_3, x_4 prawdziwa jest równość:*

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = {} & \tfrac{1}{6}\left[(x_1 - x_2)^4 + (x_1 + x_2)^4\right] + \\ + {} & \tfrac{1}{6}\left[(x_1 - x_3)^4 + (x_1 + x_3)^4\right] + \\ + {} & \tfrac{1}{6}\left[(x_1 - x_4)^4 + (x_1 + x_4)^4\right] + \\ + {} & \tfrac{1}{6}\left[(x_2 - x_3)^4 + (x_2 + x_3)^4\right] + \\ + {} & \tfrac{1}{6}\left[(x_2 - x_4)^4 + (x_2 + x_4)^4\right] + \\ + {} & \tfrac{1}{6}\left[(x_3 - x_4)^4 + (x_3 + x_4)^4\right].\end{aligned} \tag{13.4}$$

Dowód. Dla dowolnych zmiennych x, y zachodzi $(x-y)^4 + (x+y)^4 = x^4 - 4x^3y + 6x^2y^2 - 4xy^3 + y^4 + x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 =$

$= 2x^4 + 12x^2y^2 + 2y^4$, zatem prawa strona tożsamości Liouville'a przybiera postać
$\frac{1}{3}x_1^4+2x_1^2x_2^2+\frac{1}{3}x_2^4+\frac{1}{3}x_1^4+2x_1^2x_3^2+\frac{1}{3}x_3^4+\frac{1}{3}x_1^4+2x_1^2x_4^2+\frac{1}{3}x_4^4+\frac{1}{3}x_2^4+2x_2^2x_3^2+$
$+\frac{1}{3}x_3^4+\frac{1}{3}x_2^4+2x_2^2x_4^2+\frac{1}{3}x_4^4+\frac{1}{3}x_3^4+2x_3^2x_4^2+\frac{1}{3}x_4^4 = x_1^4+2x_1^2x_2^2+2x_1^2x_3^2+$
$+2x_1^2x_4^2+x_2^4+2x_2^2x_3^2+2x_2^2x_4^2+x_3^4+2x_3^2x_4^2+x_4^4 = \left(x_1^2+x_2^2+x_3^2+x_4^2\right)^2$. □

Twierdzenie 13.33. (Liouville'a). *Każda liczba naturalna jest sumą* 53 *bikwadratów liczb całkowitych.*

Dowód. Niech a będzie liczbą naturalną. Wtedy z twierdzenia 13.20 istnieją liczby całkowite x_1, x_2, x_3, x_4 takie, że $a = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Z Lematu 13.32 mamy

$$\begin{aligned} 6a^2 \;&= 6\left(x_1^2+x_2^2+x_3^2+x_4^2\right)^2 = \left[(x_1-x_2)^4+(x_1+x_2)^4\right]+ \\ &+\left[(x_1-x_3)^4+(x_1+x_3)^4\right]+\left[(x_1-x_4)^4+(x_1+x_4)^4\right]+ \\ &+\left[(x_2-x_3)^4+(x_2+x_3)^4\right]+\left[(x_2-x_3)^4+(x_2+x_3)^4\right]+ \\ &+\left[(x_2-x_3)^4+(x_2+x_3)^4\right], \end{aligned} \tag{13.5}$$

czyli liczba $6a^2$ jest sumą dwunastu bikwadratów liczb całkowitych nieujemnych. Z twierdzenia o dzieleniu z resztą każdą nieujemną liczbę całkowitą możemy zapisać w postaci $6q + r$, gdzie $q, r \in \mathbb{Z}$, $q \geqslant 0$ i $r \in \in \{0, 1, 2, 3, 4, 5\}$. Ponownie korzystając z twierdzenia 13.20 otrzymujemy $q = a_1^2 + a_2^2 + a_3^2 + a_4^2$ dla a_1, a_2, a_3, $a_4 \in \mathbb{Z}$, wobec tego każdy składnik sumy równania (13.5) jest sumą czterech bikwadratów, co daje nam łącznie 48 bikwadratów. Ponadto zachodzi również:

$$r = \begin{cases} 0^4+0^4+0^4+0^4+0^4 & \text{dla } r=0, \\ 1^4+0^4+0^4+0^4+0^4 & \text{dla } r=1, \\ 1^4+1^4+0^4+0^4+0^4 & \text{dla } r=2, \\ 1^4+1^4+1^4+0^4+0^4 & \text{dla } r=3, \\ 1^4+1^4+1^4+1^4+0^4 & \text{dla } r=4, \\ 1^4+1^4+1^4+1^4+1^4 & \text{dla } r=5. \end{cases} \tag{13.6}$$

Stąd każdą liczbę naturalną możemy zapisać jako sumę 53 bikwadratów pewnych nieujemnych liczb całkowitych. □

Następne ćwiczenie jest związane z zabawną historią z 1919 roku opowiedzianą przez G. H. Hardy'ego:

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

> „Pamiętam, jak raz chciałem go (S. Ramanujana) odwiedzić, gdy leżał chory w Putney. Jechałem taksówką z numerem 1729. Powiedziałem mu, że ten numer jest raczej nieciekawy i mam nadzieję, że to nie był zły omen. – Nie – odparł – to jest bardzo interesujące; to najmniejsza liczba naturalna posiadająca dwa istotnie różne rozkłady na sumę sześcianów dwóch liczb naturalnych."

Ćwiczenie 13.34. Udowodnij, że liczba 1729 jest najmniejszą liczbą naturalną posiadającą dwa istotnie różne rozkłady na sumy sześcianów dwóch liczb naturalnych.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 14

Systemy pozycyjne

14.1 Uwagi historyczne o systemach liczenia

Już w trzecim tysiącleciu p.n.e. używano w Egipcie hieroglifów do oznaczania liczebności. Innych cyfr używano w Babilonii, jeszcze innych w starożytnej Grecji i Rzymie. Umiejętność nazywania liczb znacznie wyprzedziła umiejętność ich zapisywania, z czasem jednak wprowadzono znaki, za pomocą których zapisywano liczby. Powstawały zasady tworzenia nowych liczb i tak powstały systemy liczbowe.

Systemem liczbowym nazywa się sposób zapisywania liczb oraz zbiór reguł umożliwiających wykonywanie działań na tych liczbach.

Dla każdego systemu liczbowego istnieje zbiór znaków, za pomocą których tworzy się liczby. Znaki te zwane cyframi można zestawiać ze sobą na różne sposoby otrzymując nieskończoną liczbę kombinacji.

Najbardziej prymitywny systemem liczbowy, to system, w którym występuje tylko jeden znak. W systemie tym kolejne liczby są tworzone przez proste powtarzanie tego znaku. Z bardziej złożonych systemów rozróżnia się pozycyjne i niepozycyjne systemy liczbowe. W **systemach liczbowych pozycyjnych** liczbę przedstawia się jako ciąg cyfr. Wartość jej jest zależna od położenia (pozycji) cyfry w liczbie. **Systemy niepozycyjne** posiadają osobne symbole kilku liczb, a na-

stępnie posiadają kolejne symbole dla ich wielokrotności. W systemach tych liczby tworzy się przez dodawanie kolejnych symboli.

System babiloński

Babilońskich znaków używano w Mezopotamii około 5000 lat temu; zachowały się do naszych czasów na glinianych tabliczkach. Wśród tych tabliczek znaleziono sporo takich, na których wypisana jest pewna wiedza matematyczna Babilonii. Babilończycy pisali pismem klinowym. Liter klinowych było dużo, ale znaków cyfrowych było niewiele. Babilończycy, którzy byli sławni ze swoich słynnych obserwacji astronomicznych i obliczeń, korzystali z pozycyjnego systemu sześćdziesiątkowego (systemu liczbowego o podstawie 60), który towarzyszy nam jeszcze dziś. Do dzisiaj dzielimy godziny na sześćdziesiąt minut, minuty na sześćdziesiąt sekund.

Chociaż sześćdziesiąt może wydawać się dużą liczbą jak na podstawę, to jednak są pewne tego korzyści. Sześćdziesiąt jest najmniejszą liczbą, która jest podzielna przez dwa, trzy, cztery, pięć i sześć. Można ją podzielić również przez dziesięć, dwanaście, piętnaście, dwadzieścia i trzydzieści.

Problem sprawia tylko brak cyfry na określonej pozycji. Babilończycy nie znali cyfry zero. Zamiast zera pozostawiali na danej pozycji puste miejsce. Problem pojawiał się wtedy, gdy obok siebie było kilka takich pustych miejsc. Jednak w rachunkach starożytności nie operowano olbrzymimi wartościami, więc puste miejsca obok siebie w zapisie babilońskim były raczej rzadkością. W późniejszym okresie zaczęto takie puste miejsca zaznaczać małą, pionową kreseczką umieszczoną u góry.

Rzymski system zapisywania liczb

Pierwotny rzymski system zapisywania liczb był prosty, ale dość niewygodny. Rzymianie zapisywali liczby za pomocą tylko pionowych kresek, na kształt systemu karbowego. Wprowadzono więc dla oznaczenia ważnych liczb dodatkowe znaki. W systemie rzymskim posługujemy się znakami: I, V, X, L, C, D, M, gdzie:
I = 1, V = 5, X = 10, L = 50, C = 100, D = 500, M = 1000.

Rzymski sposób zapisywania liczb jest sposobem addytywnym, czy-

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

li wartość danej liczby określa się na podstawie sumy wartości jej znaków cyfrowych. Wyjątki od tej zasady to liczby: 4, 9, 40, 90, 400 i 900, do opisu których używa się odejmowania. Podczas zapisywania liczb w systemie rzymskim należy dążyć zawsze do tego, aby używać jak najmniejszej liczby znaków, pamiętając przy tym o zasadach:

1. Obok siebie mogą stać co najwyżej trzy znaki spośród: I, X, C lub M.

2. Obok siebie nie mogą stać dwa znaki: V, L, D.

3. Nie może być dwóch znaków oznaczających liczby mniejsze bezpośrednio przed znakiem oznaczającym liczbę większą.

4. Znakami poprzedzającymi znak oznaczający większą liczbę mogą być tylko znaki: I, X, C.

Za pomocą dostępnych znaków można zapisać liczby od 1 do 3999, ponieważ nie istnieją znaki dla liczb większych od 1000. Rzymianie posiadali takie symbole dla liczb: 5000, 10000, ale wyszły one już z użycia. Zasada odejmowania wartości, na mocy której 4 i 9 zapisywało się jako IX i IV, stała się powszechna dopiero w czasach średniowiecznych. Rzymianie zaś stosowali ją rzadko.

Rzymski system ma jedną wadę, jest niewygodny w prowadzeniu nawet prostych działań arytmetycznych. Rzymianie jednak potrafili dość sprawnie wykonywać działania dodawania i odejmowania posługując się przy tym liczydłem.

Arabski system zapisywania liczb

Nasz system dziesiętny, którym posługujemy się na co dzień, jest znany jako system arabski lub indyjsko-arabski. System dziesiętny został zapoczątkowany w Indiach w V w. n.e., a rozpowszechnił się w krajach arabskich dzięki matematykowi al-Chwarizmi, który w połowie VIII wieku przetłumaczył na arabski indyjską książkę o matematyce.

Dziewięć pierwszych cyfr oznaczających wartości od 1 do 9 były przedstawiane jako umowne znaki. Hindusi jako pierwsi wpadli na pomysł pisania cyfr słowami: 1=adi, 2=dvi, 3=tri, 4=katur, 5=pańca, 6=sat, 7=sapta, 8=asta, 9=nova.

Podawali również oddzielne nazwy dla kolejnych potęg liczby 10, stworzyli zasadę pozycyjnego przedstawiania liczb oraz wynaleźli zero. Arabowie także wprowadzili sposób zapisu i czytania liczb,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

w którym podaje się cyfrę, a potem rząd, w jakim ona stoi, choć Arabowie czytali odwrotnie, zaczynając od jedności do wyższego rzędu.

Do rozwoju i popularyzacji systemu dziesiętnego w Europie przyczynił się włoski matematyk i podróżnik Leonardo Fibonacci. Zafascynowany systemem, w 1202 roku napisał książkę *Liber Abaci*, w której tłumaczył jak używać arabskich cyfr, jak dodawać, odejmować i wykonywać inne działania w systemie dziesiętnym.

14.2 Zapisywanie liczb naturalnych w systemach pozycyjnych

Niech $g > 1$ będzie dowolną, ustaloną liczbą naturalną, którą nazywamy **podstawą systemu**. Na liczbę g możemy patrzeć jak na „dziesiątkę" w znanym nam ze szkoły systemie dziesiątkowym. Liczby $0, 1, \ldots, g-1$ będziemy nazywali **cyframi** systemu pozycyjnego o podstawie g. Natomiast sam system o podstawie g będziemy krótko oznaczali przez S_g.

Przykład 14.1. W pozycyjnym systemie dwójkowym S_2 podstawą systemu jest liczba 2, zaś cyframi są: 0 i 1. W S_3 podstawą systemu jest liczba 3, a cyframi są: 0, 1 i 2. W systemie S_{11} podstawą systemu jest liczba 11, zaś kolejne cyfry można oznaczać następująco: 0, 1,2, 3, 4, 5, 6, 7, 8, 9, A. W systemie dwunastkowym potrzebujemy jeszcze jednej cyfry (dla liczby 11) i zazwyczaj oznaczamy ją przez B.

Dla dowolnego $s \in \mathbb{N}_0$ i dowolnych cyfr $c_0, \ldots, c_s \in \{0, 1, \ldots, g-1\}$ takich, że $c_s \neq 0$ wprowadzamy zapis:

$$(c_s c_{s-1} \ldots c_1 c_0)_g = c_0 + c_1 g + c_2 g^2 + \ldots + c_s g^s. \tag{14.1}$$

Przykład 14.2. $(1101)_2 = 1 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$, $(A0)_{11} = = 0 + A \cdot 11 = 10 \cdot 11 = 110$. Ponadto, $3^2 + 3^4 = 0 + 0 \cdot 3^1 + 1 \cdot 3^2 + 0 \cdot \cdot 3^3 + 1 \cdot 3^4 = (10100)_3$.

Definicja 14.3. Liczbę $(c_s c_{s-1} \ldots c_1 c_0)_g$ nazywamy **ogólną postacią liczby** $(s+1)$-cyfrowej w systemie pozycyjnym o podstawie g.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 14.4. *Niech $s \in \mathbb{N}_0$. Wówczas w systemie pozycyjnym o podstawie g dwie liczby $(s+1)$-cyfrowe są równe wtedy i tylko wtedy, gdy mają takie same cyfry na wszystkich odpowiednich pozycjach, to znaczy jeżeli $c_i, d_i \in \{0, 1, \ldots, g-1\}$ dla $i = 0, 1, \ldots, s$, $c_s, d_s \neq 0$, to:*

$$(c_s c_{s-1} \ldots c_1 c_0)_g = (d_s d_{s-1} \ldots d_1 d_0)_g \iff [c_i = d_i \; \forall_{i=0,1,\ldots,s}]. \quad (14.2)$$

Dowód. Implikacja $\Leftarrow$ jest oczywista. Dla dowodu implikacji $\Rightarrow$ zastosujemy indukcję względem $s \in \mathbb{N}_0$. Dla $s = 0$ teza jest oczywista. Załóżmy, że teza zachodzi dla pewnego $s \in \mathbb{N}_0$ i weźmy dowolne $c_i, d_i \in \{0, 1, \ldots, g-1\}$ dla $i = 0, 1, \ldots, s+1$ takie, że $(c_{s+1} c_s \ldots c_1 c_0)_g = (d_{s+1} d_s \ldots d_1 d_0)_g$. Wtedy ze wzoru (14.1) $c_0 + g[c_1 + c_2 g + \ldots + c_{s+1} g^s] = d_0 + g[d_1 + d_2 g + \ldots + d_{s+1} g^s]$, więc ponieważ $c_0, d_0 \in \{0, 1, \ldots, g-1\}$, więc z twierdzenia o dzieleniu z resztą (zastosowanego dla liczby g) otrzymujemy, że $c_0 = d_0$ oraz $g(c_{s+1} c_s \ldots c_1)_g = g(d_{s+1} d_s \ldots d_1)_g$, skąd po skróceniu przez g i zastosowaniu założenia indukcyjnego, $c_i = d_i$ dla $i = 1, 2, \ldots, s+1$. Wobec tego $c_i = d_i$ dla każdego $i = 0, 1, \ldots, s+1$. Zatem teza zachodzi także dla liczby $s+1$. □

Stwierdzenie 14.5. *Niech $s, r \in \mathbb{N}_0$. Wówczas w systemie pozycyjnym o podstawie g:*

(i) najmniejszą liczbą naturalną $(s+1)$-cyfrową jest $(1\underbrace{0 \ldots 0}_{s\ zer})_g = g^s$,

(ii) największą liczbą naturalną $(s+1)$-cyfrową jest liczba $(\underbrace{(g-1)(g-1)\ldots(g-1)}_{s+1,\ (g-1)-tek})_g = g^{s+1} - 1$,

(iii) istnieje dokładnie $(g-1)g^s$ wszystkich liczb $(s+1)$-cyfrowych,

(iv) jeżeli $s < r$, to każda liczba $(s+1)$-cyfrowa jest mniejsza od każdej liczby $(r+1)$-cyfrowej.

Dowód. Oczywiście dowolna liczba $(s+1)$-cyfrowa w S_g ma postać $(c_s c_{s-1} \ldots c_1 c_0)_g$, gdzie $c_0, c_1, \ldots, c_s \in \{0, 1, \ldots, g-1\}$ oraz $c_s \neq 0$. Stąd $(c_s c_{s-1} \ldots c_1 c_0)_g$ jest liczbą naturalną.

(i) Ponieważ $c_s \geqslant 1$ oraz $c_i \geqslant 0$ dla każdego $i = 0, 1, \ldots, s-1$, więc $c_s g^s \geqslant g^s$ oraz $c_0 + c_1 g + \ldots + c_{s-1} g^{s-1} \geqslant 0$. Wobec tego na mocy wzoru

(14.1), $(c_s c_{s-1} \dots c_1 c_0)_g \geqslant g^s = (1\underbrace{0 \dots 0}_{s\ zer})_g$. Stąd i ze stwierdzenia 14.4, $(1\underbrace{0 \dots 0}_{s\ zer})_g$ jest najmniejszą liczbą $(s+1)$-cyfrową.

(ii). Ponieważ $c_i \leqslant g-1$, więc $c_i g^i \leqslant (g-1)g^i$ dla każdego $i = 0, 1, \dots, s$. Zatem na mocy wzoru (14.1) otrzymujemy nierówność: $(c_s c_{s-1} \dots c_1 c_0)_g \leqslant [(g-1)+(g-1)g+(g-1)g^2+\dots+(g-1)g^s]$. Ponadto $(g-1)+(g-1)g+(g-1)g^2+\dots+(g-1)g^s = (g-1)(1+g+\dots+g^s) = g^{s+1}-1$, więc stąd i ze stwierdzenia 14.4, $(\underbrace{(g-1)(g-1)\dots(g-1)}_{s+1,\ (g-1)-tek})_g$ jest największą liczbą $(s+1)$-cyfrową.

(iii). Na mocy stwierdzenia 14.4 wszystkich liczb $(s+1)$-cyfrowych jest tyle samo, co wszystkich ciągów postaci $(c_s, c_{s-1}, \dots, c_1, c_0)$, gdzie $c_s \in \{1, 2, \dots, g-1\}$ oraz $c_i \in \{0, 1, \dots, g-1\}$. Element c_s można zatem wybrać na dokładnie $g-1$ sposobów, zaś każdy z pozostałych s elementów $c_{s-1}, \dots, c_1, c_0$ można wybrać na dokładnie g sposobów. Wobec tego taki ciąg, a zatem i liczbę postaci (14.1), można wybrać na dokładnie $(g-1)g^s$ sposobów.

(iv). Na mocy (ii) każda liczba $(s+1)$-cyfrowa a jest mniejsza od liczby g^{s+1} oraz każda liczba $(r+1)$-cyfrowa b jest większa lub równa od liczby g^r, ale $r > s$, więc $r \geqslant s+1$, skąd $g^r \geqslant g^{s+1}$ i wobec tego $b > a$. □

Stwierdzenie 14.6. *Niech $s \in \mathbb{N}_0$. Wówczas w systemie pozycyjnym o podstawie g z dwóch różnych liczb $(s+1)$-cyfrowych a i b większą jest ta liczba, która ma większą cyfrę na najdalszej pozycji, to znaczy dla $a = (c_s c_{s-1} \dots c_1 c_0)_g$, $b = (d_s d_{s-1} \dots d_1 d_0)_g$, jeśli $c_s < d_s$ lub istnieje liczba naturalna $t < s$ taka, że $c_i = d_i$ dla każdego $i = s, s-1, \dots, t$ oraz $c_{t-1} < d_{t-1}$, to $a < b$.*

Dowód. Załóżmy, że $c_s < d_s$. Wtedy $c_s + 1 \leqslant d_s$. Wobec tego $b \geqslant ((c_s+1)d_{s-1} \dots d_1 d_0)_g \geqslant (c_s+1)g^s$. Ponadto, $(c_s+1)g^s = c_s g^s + g^s$ i na mocy stwierdzenia 14.5 (ii), $(c_{s-1} \dots c_1 c_0)_g < g^s$, więc $a = c_s g^s + (c_{s-1} \dots c_1 c_0)_g < c_s g^s + g^s$, skąd $a < b$.

Niech teraz istnieje liczba naturalna $t < s$ taka, że $c_i = d_i$ dla każdego $i = s, s-1, \dots, t$ oraz $c_{t-1} < d_{t-1}$. Wtedy z pierwszej części

naszego dowodu, $(c_{t-1}\dots c_1c_0)_g < (d_{t-1}\dots d_1d_0)_g$. Stąd po dodaniu do obu stron liczby $c_sg^s + c_{s-1}g^{s-1} + \dots + c_tg^t$ uzyskamy, że $a < b$. □

Twierdzenie 14.7. *Dla dowolnej liczby naturalnej $g > 1$ każda liczba naturalna n może być zapisana w postaci* (14.1). *Ponadto, zapis liczby naturalnej n w tej postaci jest jednoznaczny, to znaczy zarówno s jak i cyfry $c_0, c_1, \dots, c_s \in \{0, 1, \dots, g-1\}$ takie, że $c_s \neq 0$, są wybrane na dokładnie jeden sposób.*

Dowód. Jednoznaczność zapisu liczby n w postaci (14.1) wynika od razu ze stwierdzeń 14.4 i 14.5. Pozostaje zatem wykazać istnienie takiego zapisu. Załóżmy, że pewnej liczby naturalnej nie można zapisać w postaci (14.1). Wówczas z zasady minimum istnieje najmniejsza liczba naturalna m, której nie można zapisać w postaci (14.1). Ponadto jeśli $n < g$, to $n \in \{1, 2, \dots, g-1\}$ i wystarczy przyjąć $s = 0$ oraz $c_0 = n$. Wobec tego $m \geqslant g$. Z twierdzenia o dzieleniu z resztą wynika, że istnieją liczby całkowite q i r takie, że $m = qg + r$ oraz $0 \leqslant r < g$, skąd $r \in \{0, 1, \dots, g-1\}$. Ponadto $m \geqslant g$, więc gdyby $q \leqslant 0$, to $qg \leqslant 0$ i $m \leqslant 0 + r < g$, co prowadzi do sprzeczności. Zatem $q > 0$, czyli $q \in \mathbb{N}$ oraz $q < m$, bo $m \geqslant qg > q$, gdyż $g > 1$. Z minimalności liczby m wynika więc, że istnieje $t \in \mathbb{N}_0$ oraz istnieją $d_0, d_1, \dots, d_t \in \{0, 1, \dots, g-1\}$ takie, że $d_t \neq 0$ oraz $q = (d_t \dots d_1d_0)_g$, ale $m = g \cdot q + r$, więc $m = (d_t \dots d_1d_0r)_g$, czyli m jest postaci (14.1). W takim razie przypuszczenie, że pewnej liczby naturalnej nie można zapisać w postaci (14.1) doprowadziło nas do sprzeczności. Zatem każdą liczbę naturalną n można zapisać w postaci (14.1). □

Zaważmy, że dla liczby naturalnej n ze wzoru (14.1), $[n]_g = c_0$, to znaczy **ostatnią cyfrą liczby n zapisanej w S_g jest reszta z dzielenia tej liczby przez g**. Dla $s \geqslant 1$, oznaczając przez n_1 niepełny iloraz z dzielenia n przez g uzyskamy, że $n_1 = c_sg^{s-1} + \dots + c_2g + c_1$, skąd $c_1 = [n_1]_g$. Kontynuując ten proces aż do niepełnego ilorazu $c_s < g$ uzyskujemy kolejne cyfry liczby n w systemie pozycyjnym o podstawie g, przy czym wyznaczamy cyfry od prawej strony do lewej. Daje to nam algorytm zapisywania dowolnej liczby naturalnej w S_g. Zilustrujemy ten algorytm na przykładach.

Przykład 14.8. Zapiszemy liczbę 34 w systemach S_2, S_5 i S_{12}. Obliczenia dla systemu S_2 są następujące: $34 = 17 \cdot 2 + 0$, więc $34 = (\ldots 0)_2$, $17 = 8 \cdot 2 + 1$, więc $34 = (\ldots 10)_2$, dalej, $8 = 4 \cdot 2 + 0$, więc $34 = (\ldots 010)_2$, $4 = 2 \cdot 2 + 0$, czyli $34 = (\ldots 0010)_2$, $2 = 1 \cdot 2 + 0$ i $1 < 2$, więc ostatecznie $34 = (100010)_2$. Możemy wykonać sprawdzenie: $(100010)_2 = 0 + 1 \cdot 2 + 0 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 = 2 + 32 = 34$.

Obliczenia dla systemu S_5: $34 = 6 \cdot 5 + 4$, więc $34 = (\ldots 4)_5$, $6 = 1 \cdot 5 + 1$ i $1 < 5$, więc ostatecznie $34 = (114)_5$. Sprawdzenie: $(114)_5 = 4 + 1 \cdot 5^1 + 1 \cdot 5^2 = 9 + 25 = 34$.

Obliczenia dla systemu S_{12}: $34 = 2 \cdot 12 + 10$ i $2 < 12$, więc od razu $34 = (2A)_{12}$. Sprawdzenie: $(2A)_{12} = A + 2 \cdot 12 = 10 + 24 = 34$.

Przykład 14.9. Zapiszemy liczbę $(AAB)_{12}$ w S_{11}. Zauważmy, że $(AAB)_{12} = B + A \cdot 12 + A \cdot 12^2 = 11 + 10 \cdot 12 + 10 \cdot 144 = 1571$. Dalej, $1571 = 142 \cdot 11 + 9$, więc $1571 = (\ldots 9)_{11}$, $142 = 12 \cdot 11 + 10$ i $10 = A$, więc $1571 = (\ldots A9)_{11}$, $12 = 1 \cdot 11 + 1$ i $1 < 11$, więc ostatecznie $1571 = (11A9)_{11}$ oraz $(AAB)_{12} = (11A9)_{11}$.

Przykład 14.10. Obliczymy ile cyfr zużyto do oznaczenia wszystkich stron encyklopedii posiadającej 2435 stron. Mamy 9 stron jednocyfrowych, $99 - 9 = 90$ stron dwucyfrowych, na które zużyto $2 \cdot 90 = 180$ cyfr, mamy też $999 - 99 = 900$ stron trzycyfrowych, na które zużyto $3 \cdot 900 = 2700$ cyfr i mamy $2435 - 999 = 1436$ stron czterocyfrowych, na które zużyto $4 \cdot 1436 = 5744$ cyfr. Zatem razem zużyto $9 + 180 + 2700 + 5744 = 8633$ cyfr.

Przykład 14.11. Wiedząc, że do oznaczenia stron encyklopedii zużyto 11921 cyfr, obliczymy ile stron ma ta encyklopedia. Mamy 9 stron jednocyfrowych, 90 stron dwucyfrowych, na które zużyto $2 \cdot 90 = 180$ cyfr. Mamy też 900 stron trzycyfrowych, na które zużyto razem $3 \cdot 900 = 2700$ cyfr. Stąd razem do oznaczenia 999 stron tej encyklopedii zużyto $9 + 18 + 2700 = 2889$ cyfr. Liczb czterocyfrowych jest dokładnie $9999 - 999 = 9000$ i $4 \cdot 9000 = 36000 > 11921$. Zatem liczba stron tej encyklopedii jest czterocyfrowa. Oznaczmy ją przez x. Wtedy do oznaczenia wszystkich stron czterocyfrowych zużyto razem $4 \cdot (x - 999)$ cyfr. Mamy więc równanie: $2889 + 4 \cdot (x - 999) = 11921$. Stąd $4 \cdot (x -$

$999) = 9032$, czyli $x - 999 = 2258$ i ostatecznie $x = 3257$. Zatem ta encyklopedia ma 3257 stron.

Przykład 14.12. Dla liczb naturalnych $x > 1$ zapiszemy liczbę $x^4 - 2$ w systemie S_x. Mamy, że $x^4 - 2 = (x-1) \cdot x^3 + x^3 - 2 = (x-1) \cdot x^3 + (x-1) \cdot x^2 + x^2 - 2$, więc $x^4 - 2 = (x-1) \cdot x^3 + (x-1) \cdot x^2 + (x-1) \cdot x + (x-2)$, czyli $x^4 - 2 = (x-1 \;\; x-1 \;\; x-1 \;\; x-2)_x$ w systemie S_x.

Przykład 14.13. Systemy dwójkowy i szesnastkowy zwany też systemem **heksadecymalnym** mają bardzo ważne zastosowania w informatyce. Typowe oznaczenia cyfr w systemie szesnastkowym to: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$, gdzie $A = (10)_{10}$, $B = (11)_{10}$, $C = (12)_{10}$, $D = (13)_{10}$, $E = (14)_{10}$ i $F = (15)_{10}$.

Okazuje się, że bardzo łatwo zamieniać liczbę zapisaną w jednym z tych systemów na liczbę zapisaną w drugim z nich. Wykorzystujemy to, że $(16)_{10} = 2^4$, czyli $(10)_{16} = (10000)_2$.

Przejście od systemu dwójkowego do systemu szesnastkowego. Najpierw zauważmy, że największą liczbą 4 - cyfrową w S_2 jest $(1111)_2 = 1 + 2 + 4 + 8 = (15)_{10} = (F)_{16}$, więc dla dowolnych $x, y, z, t \in \{0, 1\}$ liczba $(xyzt)_2 = t + z \cdot 2 + y \cdot 4 + x \cdot 8$ jest cyfrą w systemie S_{16}. Na przykład $(1011)_2 = 1 + 2 + 8 = B$, $(0111)_2 = 1 + 2 + 4 = 7$, $(0010)_2 = 2$, itd. Wykorzystując to, że $(16)_{10} = 2^4$, czyli $(10)_{16} = (10000)_2$, mamy zatem następującą metodę na zamianę liczby zapisanej w S_2 na liczbę zapisaną w S_{16}: najpierw dzielimy liczbę a zapisaną w S_2 na bloki czterocyfrowe poczynając od lewej strony, a następnie każdy blok zapisujemy w postaci cyfry w systemie S_{16} i w ten sposób uzyskujemy kolejne cyfry liczby a w systemie S_{16}. Na przykład dla $a = (1101011101)_2$ mamy zapis blokowy: $11|0101|1101$ oraz $(11)_2 = 1 + 2 = 3$, $(0101)_2 = 1 + 4 = 5$, $(1101)_2 = 1 + 4 + 8 = D$. Stąd $(1101011101)_2 = (35D)_{16}$. Natomiast dla $b = (1000000110100)_2$ mamy zapis blokowy: $1|0000|0011|0100$ oraz $(1)_2 = 1$, $(0000)_2 = 0$, $(0011)_2 = 1 + 2 = 3$, $(0100)_2 = 4$, więc $b = (1034)_{16}$.

Przejście od systemu szesnastkowego do systemu dwójkowego. Teraz postępujemy odwrotnie, mianowicie każdą cyfrę liczby za-

pisanej w S_{16} zapisujemy w postaci 4-bitowej w systemie S_2 i następnie zastępujemy każdą z tych cyfr otrzymaną liczbą z systemu S_2. Zatem kolejno $0 = (0000)_2$, $1 = (0001)_2$, $2 = (0010)_2$, $3 = 1+2 = (0011)_2$, $4 = (0100)_2$, $5 = (0101)_2$, $6 = 4 + 2 = (0110)_2$, $7 = (0111)_2$, $8 = (0100)_2$, $9 = (0101)_2$, $A = 2^3+2 = (1010)_2$, $B = A+1 = (1011)_2$, $C = 2^3+2^2 = (1100)_2$, $D = C+1 = (1101)_2$, $E = 2^3+2^2+2 = (1110)_2$, $F = (1111)_2$. Wobec tego na przykład $(35D)_{16} = (0011\ 0101\ 1101)_2$, $(1034)_{16} = (0001\ 0000\ 0011\ 0100)_2$, $(ABCD)_{16} = (1010\ 1011\ 1100\ 1101)_2$.

Ćwiczenie 14.14. Do zapisu liczb naturalnych $1, 2, \ldots, n$ w systemie S_6 zużyto $(6681)_9$ cyfr. Oblicz n.

Ćwiczenie 14.15. Rozwiąż równania w liczbach naturalnych x: (a) $x^2 = (11)_8$, (b) $x^2 = (31)_8$, (c) $x^2 = (61)_8$, (d) $x^2 = (31)_5$, (e) $x^2 = (14)_5$.

14.3 Dodawanie i odejmowanie w systemach pozycyjnych

Niech $g > 1$ będzie dowolną, ustaloną liczbą naturalną. Dodawanie w S_g jest podobne do dodawania w systemie dziesiątkowym, z tym, że rolę dziesiątki pełni teraz podstawa g. Niech a, b będą cyframi w S_g, czyli $a, b \in \{0, 1, \ldots, g-1\}$. Jeśli $a + b < g$, to $a + b$ jest cyfrą w tym systemie. Jeśli $a + b = g$, to $a + b = (10)_g$. Trudności zaczynają się dopiero, gdy $a + b > g$, czyli gdy przekraczamy próg dziesiątkowy. Mianowicie wówczas $a + b < g + g = 2g$ oraz $0 < a + b - g < g$, czyli $a+b-g$ jest cyfrą, skąd $a+b = (1(a+b-g))_g$. Wobec tego w systemie S_g mamy wzór:

$$a + b = \begin{cases} a + b & \text{jeśli} \quad a + b < g, \\ (1(a + b - g))_g & \text{jeśli} \quad a + b \geqslant g \end{cases} . \tag{14.3}$$

Przykład 14.16. W systemie S_{12} mamy, że $1 + A = B$, $A + A = = (18)_{12}$, bo $A+A-12 = 20-12 = 8$. W szkole, to ostatnie dodawanie wykonujemy tak: $A + A = (A + 2) + (A - 2) = (1(A - 2))_{12} = (18)_{12}$.

W systemie S_7: $5 + 6 = 4 + 7 = (14)_7$. W systemie S_9: $7 + 6 = (7 + 2) + (6 - 2) = (14)_9$.

Na wzorze (14.3) opiera się metoda pisemnego dodawania dwóch liczb naturalnych w systemie S_g; mianowicie chodzi o dopełnianie do „dziesiątki" i ewentualne przekazywanie „jeden dalej", gdy suma cyfr jest co najmniej równa g. Zauważmy, że jeśli w pewnym kroku dodawania pisemnego „jeden poszedł dalej" i teraz dodajemy cyfry a i b, to $a + b + 1 \leqslant (g - 1) + (g - 1) + 1 < 2g$, czyli dalej może pójść co najwyżej jeden, a nigdy cyfra większa od jeden. Zilustrujemy to teraz na przykładach. Dla uproszczenia zapisu, gdy będziemy liczyć w ustalonym systemie S_g, to w zapisie liczby $(c_s \dots c_1 c_0)_g$ będziemy opuszczali nawiasy i podstawę g (podobnie jak to robimy w systemie dziesiątkowym). Należy jednak cały czas pamiętać, że rolę dziesiątki pełni podstawa g.

Przykład 14.17. Wykonamy w systemie S_5 dodawanie pisemne liczb 1134 i 444. Rolę dziesiątki pełni teraz liczba 5.

$$\begin{array}{cccc} \overset{1}{1} & \overset{1}{1} & \overset{1}{3} & 4 \\ + & 4 & 4 & 4 \\ \hline 2 & 1 & 3 & 3 \end{array}$$

Przykład 14.18. Wykonamy w systemie S_8 dodawanie pisemne liczb 6754 i 5746. Rolę dziesiątki pełni teraz liczba 8.

$$\begin{array}{ccccc} & \overset{1}{6} & \overset{1}{7} & \overset{1}{5} & 4 \\ + & 5 & 7 & 4 & 6 \\ \hline 1 & 4 & 7 & 2 & 2 \end{array}$$

Przykład 14.19. Wykonamy w systemie S_{12} dodawanie pisemne liczb 6754 i 5746. Rolę dziesiątki pełni teraz liczba 12.

$$\begin{array}{ccccc} & \overset{1}{6} & 7 & 5 & 4 \\ + & 5 & 7 & 4 & 6 \\ \hline 1 & 0 & 2 & 9 & A \end{array}$$

Ćwiczenie 14.20. Oblicz sposobem pisemnym:
(a) $(123)_4 + (333)_4$, (b) $(765)_8 + (107)_8$, (c) $(88)_9 + (77)_9$.

Ćwiczenie 14.21. Rozwiąż równania w S_2:
(a) $x - 1111 = 10001$, (b) $x - 101011 = 11111$.

Przykład 14.22. W systemie dwójkowym $10 - 1 = 2 - 1 = 1$. W systemie czwórkowym: $10 - 1 = 4 - 1 = 3$. W systemie piątkowym: $13 - 4 = (5 - 4) + 3 = 4$.

Przykład 14.23. W systemie S_4 wykonamy pisemne odejmowanie $123123 - 33132$. Rolę dziesiątki pełni tutaj liczba 4.

$$\begin{array}{cccccc} & \overset{1}{2} & \overset{4+2}{3} & \overset{4}{1} & \overset{4+2}{2} & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 \\ - & 3 & 3 & 1 & 3 & 2 \\ \hline & 2 & 3 & 3 & 3 & 1 \end{array}.$$

Możemy wykonać sprawdzenie: $\begin{array}{cccccc} & \overset{1}{2} & \overset{1}{3} & \overset{1}{3} & \overset{1}{3} & 1 \\ + & 3 & 3 & 1 & 3 & 2 \\ \hline 1 & 2 & 3 & 1 & 2 & 3 \end{array}$.

Przykład 14.24. W systemie S_{11} wykonamy pisemne odejmowanie $3123 - A3A$. Rolę dziesiątki pełni tutaj liczba 11.

$$\begin{array}{cccc} \overset{2}{3} & \overset{11}{1} & \overset{11+1}{2} & \overset{11+3}{3} \\ - & A & 3 & A \\ \hline 2 & 1 & 9 & 4 \end{array}.$$ Możemy wykonać sprawdzenie: $\begin{array}{cccc} \overset{1}{2} & \overset{1}{1} & \overset{1}{9} & 4 \\ + & A & 3 & A \\ \hline 3 & 1 & 2 & 3 \end{array}$.

Ćwiczenie 14.25. Wykonaj odejmowanie pisemne w podanych systemach:
(a) $(10024)_7 - (666)_7$, (b) $(345)_{12} - (BA)_{12}$.

14.4 Mnożenie pisemne w systemach pozycyjnych

Niech $g > 1$ będzie dowolną, ustaloną liczbą naturalną. Mnożenie w S_g jest podobne do mnożenia w systemie dziesiątkowym, z tym,

że rolę dziesiątki pełni teraz podstawa g. Aby sprawnie wykonywać mnożenie sposobem pisemnym w systemie S_g należy najpierw znać tabliczkę mnożenia w tym systemie. Dzięki temu będziemy umieli wykonywać mnożenie pisemne liczby naturalnej przez każdą cyfrę z tego systemu. Zauważmy, że dla $g \geqslant 3$: $(g-1)^2 < (g-2)g+g-1 = (g-2\ g-1)_g$, więc "dalej" może pójść co najwyżej cyfra $g-2$. Natomiast mnożenie pisemne dwóch liczb wielocyfrowych jest wzorowane na mnożeniu w systemie dziesiątkowym, co zaprezentujemy na przykładach.

Najprostsza tabliczka mnożenia jest w systemie S_2: $1 \cdot 1 = 1$.

Przykład 14.26. Tabliczka mnożenia w systemie trójkowym ma postać:

$\cdot$	1	2
1	1	2
2	2	11

gdyż $2 \cdot 2 = 2 + 2 = (2 + 1) + 1 = 11$. Możemy teraz w tym systemie obliczyć sposobem pisemnym iloczyn $2012 \cdot 212$:

$$\begin{array}{cccccccc}
 & & & 2 & 0 & 1 & 2 \\
 & & \times & & 2 & 1 & 2 \\
\hline
 & & 1 & 1 & 1 & 0 & 1 \\
 & & 2 & 0 & 1 & 2 & \\
1 & 1 & 1 & 0 & 1 & & \\
\hline
1 & 2 & 1 & 2 & 0 & 2 & 1
\end{array}$$

Przykład 14.27. Tabliczka mnożenia w systemie czwórkowym ma postać:

$\cdot$	1	2	3
1	1	2	3
2	2	10	12
3	3	12	21

bo $2{\cdot}2 = 2{+}2 = 10$, $3{\cdot}2 = 2{\cdot}2{+}2 = 10{+}2 = 12$, $3{\cdot}3 = 2{\cdot}3{+}3 = 12{+}3 = 21$. Możemy teraz w tym systemie obliczyć sposobem pisemnym

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

iloczyn $313 \cdot 232$:

$$\begin{array}{cccccc}
 & & & 3 & 1 & 3 \\
 & & \times & 2 & 3 & 2 \\
\hline
 & & 1 & 2 & 3 & 2 \\
 & 2 & 2 & 1 & 1 & \\
1 & 2 & 3 & 2 & & \\
\hline
2 & 1 & 3 & 2 & 0 & 2
\end{array}.$$

Przykład 14.28. Tabliczka mnożenia w systemie piątkowym ma postać:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	11	13
3	3	5	14	22
4	4	13	22	31

bo $2 \cdot 3 = 3 + 3 = (3 + 2) + 1 = 11$, $2 \cdot 4 = 4 + 4 = (4 + 1) + 3 = 13$, $3 \cdot 3 = 2 \cdot 3 + 3 = 11 + 3 = 14$, $3 \cdot 4 = 3 \cdot 3 + 3 = 14 + 3 = 22$, $4 \cdot 4 = 3 \cdot 4 + 4 = 22 + 4 = 31$. Możemy teraz w tym systemie obliczyć sposobem pisemnym iloczyn $3012 \cdot 432$:

$$\begin{array}{ccccccc}
 & & & 3 & 0 & 1 & 2 \\
 & & \times & & 4 & 3 & 2 \\
\hline
 & & 1 & 1 & 0 & 2 & 4 \\
 & 1 & 4 & 0 & 4 & 1 & \\
2 & 2 & 1 & 0 & 3 & & \\
\hline
2 & 4 & 1 & 2 & 2 & 3 & 4
\end{array}$$

Ćwiczenie 14.29. Ułóż tabelkę mnożenia w systemie szóstkowym i oblicz w tym systemie sposobem pisemnym iloczyn $5043 \cdot 435$.

Ćwiczenie 14.30. Wyznacz wszystkie liczby naturalne x takie, że $(234)_x \cdot (23)_x = (5624)_x$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

14.5 Dzielenie pisemne w systemach pozycyjnych

Niech $g > 1$ będzie dowolną, ustaloną liczbą naturalną. Dzielenie w S_g jest podobne do dzielenia w systemie dziesiątkowym, z tym, że rolę dziesiątki pełni teraz podstawa g. Przy wykonywaniu dzielenia pisemnego przez liczbę naturalną a zapisaną w systemie S_g wygodnie jest najpierw obliczyć w S_g: $1\cdot a$, $2\cdot a$, …, $(g-1)\cdot a$. Następnie postępujemy podobnie jak w systemie dziesiątkowym. Pokażemy to na przykładach.

Przykład 14.31. W systemie piątkowym wykonamy dzielenie z resztą liczby 1204 przez liczbę 34. Aby usprawnić rachunki obliczymy najpierw $1 \cdot 34 = 34$, $2 \cdot 34 = 34 + 34 = 123$, $3 \cdot 34 = 123 + 34 = 212$, $4 \cdot 34 = 212 + 34 = 301$.

$$\begin{array}{rcl} & & 14 \\ \cline{3-3} 1204 & : & 34 \\ -34 & & \\ \cline{3-3} 314 & & \\ -301 & & \\ \cline{3-3} 13 & & \end{array}$$

Wobec tego w S_5: $1204 = 14 \cdot 34 + 13$. Możemy wykonać sprawdzenie:

$$\begin{array}{cccc} & & 3 & 4 \\ & \times & 1 & 4 \\ \cline{1-4} & 3 & 0 & 1 \\ & 3 & 4 & \\ \cline{1-4} 1 & 1 & 4 & 1 \end{array}, \qquad \begin{array}{cccc} 1 & 1 & 4 & 1 \\ & + & 1 & 3 \\ \cline{1-4} 1 & 2 & 0 & 4 \end{array}.$$

Przykład 14.32. W systemie ósemkowym wykonamy pisemnie dzielenie z resztą liczby 17120561 przez liczbę 416. Najpierw wyznaczamy potrzebne nam wielokrotności liczby 416 w tym systemie: $1 \cdot$ $\cdot 416 = 416$, $2 \cdot 416 = 416 + 416 = 1034$, $3 \cdot 416 = 1034 + 416 = 1452$, $4 \cdot 416 = 1452 + 416 = 2070$, $5 \cdot 416 = 2070 + 416 = 2506$, $6 \cdot 416 =$

$= 2506 + 416 = 3124$, $7 \cdot 416 = 3124 + 416 = 3542$.

$$
\begin{array}{rl}
 & 34574 \\
\hline
17120561 & : \quad 416 \\
-1452 & \\
\hline
2400 & \\
-2070 & \\
\hline
3105 & \\
-2506 & \\
\hline
3776 & \\
-3542 & \\
\hline
2341 & \\
-2070 & \\
\hline
251 &
\end{array}
$$

Zatem mamy, że w systemie ósemkowym: $17120561 = 34574 \cdot 416 + 251$.

Omówimy teraz krótko ciekawy problem związany z dodawaniem liczb w różnych systemach pozycyjnych. Zacznijmy od systemu dziesiętnego. Załóżmy, że mamy pewną liczbę naturalną n_0 i, że możemy wykonać na tej liczbie następujące działanie: do liczby n_0 dodajemy liczbę z odwróconą kolejnością cyfr, która powstała z n_0 otrzymując w ten sposób liczbę n_1. Później to samo działanie możemy zastosować do liczby n_1 uzyskując liczbę n_2, i tak dalej. Dla przykładu niech $n_0 = 59$. Wówczas $n_1 = 59 + 95 = 154$, $n_2 = 154 + 451 = 605$, i w końcu $n_3 = 605 + 506 = 1111$. Dla $m_0 = 57$ mamy $m_1 = 57 + 75 = 132$ oraz $m_2 = 132 + 321 = 363$. W przytoczonych przykładach liczby $n_3 = 1111$ oraz $m_2 = 363$ są palindromami, to znaczy, że liczba utworzona z ich cyfr zapisanych w odwrotnej kolejności jest równa liczbie wyjściowej. Wiadomo na przykład, że po wykonaniu 55 opisanych wyżej operacji dla liczby 10911 otrzymamy następujący palindrom 4668731596684224866951378664. Liczbę naturalną n nazywamy **liczbą Lychrela** jeżeli w wyniku wykonywania na niej opisanego algorytmu nigdy nie uzyskamy palindromu. Nie wiadomo czy w systemie dziesiętnym istnieje liczba Lychrela. Liczba 196 jest najmniejszą liczbą naturalną o której nie wiem czy jest liczbą Lychrela; wszystkie liczby

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

naturalne mniejsze niż 196 nie są liczbami Lychrela. Algorytm opisany w tym akapicie jest znany jako 196-**algorytm**. Oczywiście analogiczny problem można sformułować dla innych systemów pozycyjnych. I tak, na przykład udowodniono, że w systemie pozycyjnym o podstawie 2 liczba 10110 jest liczbą Lychrela. Dodatkowo, wiemy, że liczby Lychrela istnieją w systemach pozycyjnych o podstawach: $11, 17, 20, 26$ oraz 2^k dla dowolnego $k \in \mathbb{N}$.

Ćwiczenie 14.33. W jakich systemach pozycyjnych zapisano następujące działania:
(a) $37 + 42 = 101$, (b) $37 \cdot 86 = 2656$, (c) $35 + 54 = 122$,
(d) $32 \cdot 18 = 555$?

Przykład 14.34. Wyznaczymy wszystkie liczby naturalne x takie, że $(321)_x \cdot (47)_x = (16407)_x$. Po pierwsze $x > 7$, bo 7 jest cyfrą w systemie S_x. Po drugie, rozważając pisemny zapis podanego mnożenia zauważamy, że $2 \cdot 7 + 4 \equiv 0 \pmod{x}$, czyli $x \mid 18$. Ale $x > 7$, więc $x = 9$ lub $x = 18$.

Ponieważ w systemie S_9 jest $7 \cdot 2 = 15$, $7 \cdot 3 = 23$ i $4 \cdot 3 = 13$, więc stosując mnożenie sposobem pisemnym uzyskujemy, że $321 \cdot 47 = = 16407$.

Natomiast w systemie S_{18} o kolejnych cyfrach $0, 1, \ldots, 9, A, B, C, D, E, F, G, H$ mamy, że $7 \cdot 2 = E$, $7 \cdot 3 = 13$, $4 \cdot 3 = C$, więc stosując mnożenie pisemne uzyskamy, że wtedy $321 \cdot 47 = E207$.

Wobec tego ostatecznie $x = 9$.

Kryptarytm, to zadanie szaradziarskie, w którym litery należy zastąpić cyframi tak, aby liczby, które w ten sposób powstaną, tworzyły poprawne działania. Każdej literze odpowiada jedna cyfra, różnym literom różne cyfry. Kryptarytmy można rozwiązać za pomocą odpowiedniego rozumowania bez rozważania wielu przypadków. Kryptarytmy na świecie stały się modne w latach sześćdziesiątych dwudziestego wieku, do Polski trafiły w latach siedemdziesiątych za sprawą popularyzatora gier - Lecha Pijanowskiego. Dziś w epoce komputerów rzadko pojawiają się już w prasie. Układanie kryptarytmów nie jest takie proste, podczas układania ich należy zadbać, aby:

- wyrazy tworzyły poprawne i sensowne zdanie.
- było jedno rozwiązanie bez konieczności podawania warunków dodatkowych,
- było dziesięć różnych liter.

Ćwiczenie 14.35. Znajdź wszystkie rozwiązania (w systemie dziesiątkowym) następujących kryptarytmów:

(a)
$$\begin{array}{cccccc} & S & E & N & D \\ + & M & O & R & E \\ \hline M & O & N & E & Y \end{array}$$

(b)
$$\begin{array}{cccccc} & & & U & S & A \\ + & U & S & S & R \\ \hline P & E & A & C & E \end{array}$$

(c)
$$\begin{array}{cccccc} & & W & I & L & K \\ + & U & N & I & K & A \\ \hline & L & U & D & Z & I \end{array}$$

Rozdział 15

Ułamki dziesiętne

15.1 Normalne rozwinięcie liczby rzeczywistej w systemie pozycyjnym

Niech $g > 1$ będzie dowolną, ustaloną liczbą naturalną, która jak wiemy, jest podstawą systemu pozycyjnego S_g, zaś liczby $0, 1, \ldots, g-1$ są cyframi tego systemu.

Niech x będzie dowolną, ustaloną liczbą rzeczywistą. Dla $n \in \mathbb{N}$, n-tym **reduktem** liczby x przy podstawie g nazywamy liczbę $\frac{\lfloor g^n x \rfloor}{g^n}$. Ze wzoru (9.15) mamy, że $g^n x - 1 < \lfloor g^n x \rfloor \leqslant g^n x$, skąd po pomnożeniu przez dodatnią liczbą $\frac{1}{g^n}$ otrzymujemy $x - \frac{1}{g^n} < \frac{\lfloor g^n x \rfloor}{g^n x} \leqslant x$, czyli

$$0 \leqslant x - \frac{\lfloor g^n x \rfloor}{g^n} < \frac{1}{g^n} \text{ dla każdego } n \in \mathbb{N}, \tag{15.1}$$

skąd na mocy stwierdzenia 9.37:

$$0 \leqslant x - \frac{\lfloor g^n x \rfloor}{g^n} < \frac{1}{n} \text{ dla każdego } n \in \mathbb{N}. \tag{15.2}$$

Ponadto $\lim\limits_{n\to\infty} \frac{1}{n} = 0$, więc z twierdzenia o trzech ciągach z analizy matematycznej mamy, że

$$\lim_{n\to\infty} \frac{\lfloor g^n x \rfloor}{g^n} = x. \tag{15.3}$$

W ten sposób udowodniliśmy zatem następujące

Twierdzenie 15.1. *Dla każdej liczby rzeczywistej x ciąg kolejnych jej reduktów $\left(\frac{\lfloor g^n x\rfloor}{g^n}\right)$ przy dowolnej podstawie naturalnej $g > 1$ jest zbieżny do x.*

Twierdzenie 15.2. *Niech $g > 1$ będzie liczbą naturalną i niech $x \in \mathbb{R}$. Niech $c_n = \lfloor g^n x\rfloor - g\lfloor g^{n-1}x\rfloor$ dla $n = 1, 2, \ldots$. Wówczas dla każdej liczby naturalnej n:*

(i) $c_n \in \{0, 1, \ldots, g-1\}$,

(ii) $\frac{\lfloor g^n x\rfloor}{g^n} = \lfloor x\rfloor + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n}$,

(iii) nie istnieje liczba naturalna t taka, że $c_n = g-1$ dla wszystkich $n \geqslant t$.

Dowód. (i). Ze wzoru (9.15) mamy $\lfloor g^{n-1}x\rfloor \leqslant g^{n-1}x$, skąd $g\lfloor g^{n-1}x\rfloor \leqslant g^n x$. Ponadto $g\lfloor g^{n-1}x\rfloor \in \mathbb{Z}$ i $\lfloor g^n x\rfloor$ jest największą liczbą całkowitą nie większą od $g^n x$, więc $g\lfloor g^{n-1}x\rfloor \leqslant \lfloor g^n x\rfloor$, skąd $c_n \geqslant 0$ i $c_n \in \mathbb{Z}$. Ze wzoru (9.15) mamy też, że $g^{n-1}x - 1 < \lfloor g^{n-1}x\rfloor$, skąd $g^n x - g < g\lfloor g^{n-1}x\rfloor$, więc $\lfloor g^n x\rfloor - g\lfloor g^{n-1}x\rfloor < \lfloor g^n x\rfloor - (g^n x - g)$. Ze wzoru (9.15) $\lfloor g^n x\rfloor \leqslant g^n x$, więc $c_n = \lfloor g^n x\rfloor - g\lfloor g^{n-1}x\rfloor < g^n x - g^n x + g$, czyli $c_n < g$. Wobec tego $c_n \in \{0, 1, \ldots, g-1\}$.

(ii). Stosujemy indukcję względem n. Dla $n = 1$, $\lfloor x\rfloor + \frac{c_1}{g} = \lfloor x\rfloor + \frac{\lfloor gx\rfloor - g\lfloor x\rfloor}{g} = \lfloor x\rfloor + \frac{\lfloor gx\rfloor}{g} - \lfloor x\rfloor = \frac{\lfloor gx\rfloor}{g}$, czyli nasz wzór zachodzi. Załóżmy, że ten wzór zachodzi dla pewnego naturalnego n, czyli $\frac{\lfloor g^n x\rfloor}{g^n} = \lfloor x\rfloor + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n}$. Wtedy $\lfloor x\rfloor + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n} + \frac{c_{n+1}}{g^{n+1}} = \frac{\lfloor g^n x\rfloor}{g^n} + \frac{\lfloor g^{n+1}x\rfloor - g\lfloor g^n x\rfloor}{g^{n+1}} =$

$= \frac{\lfloor g^n x\rfloor}{g^n} + \frac{\lfloor g^{n+1}x\rfloor}{g^{n+1}} - \frac{\lfloor g^n x\rfloor}{g^n} = \frac{\lfloor g^{n+1}x\rfloor}{g^{n+1}}$, czyli nasz wzór zachodzi także dla liczby $n+1$. Wobec tego na mocy zasady indukcji matematycznej wzór nasz zachodzi dla każdej liczby naturalnej n.

(iii). Załóżmy, że dla pewnej liczby naturalnej t jest $c_n = g - 1$ dla wszystkich $n \geqslant t$. Oznacza to, że $\lfloor g^n x\rfloor - g\lfloor g^{n-1}x\rfloor = g - 1$ dla wszystkich $n \geqslant t$, czyli

$$\frac{\lfloor g^n x\rfloor}{g^n} + \frac{1}{g^n} = \frac{\lfloor g^{n-1}x\rfloor}{g^{n-1}} + \frac{1}{g^{n-1}}.$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Oznacza to, że dla wszystkich $n \geqslant t$ mamy, że

$$\frac{\lfloor g^n x \rfloor}{g^n} + \frac{1}{g^n} = \frac{\lfloor g^{t-1} x \rfloor}{g^{t-1}} + \frac{1}{g^{t-1}}.$$

Zatem $\lim\limits_{n\to\infty}\left(\frac{\lfloor g^n x \rfloor}{g^n} + \frac{1}{g^n}\right) = \frac{\lfloor g^{t-1} x \rfloor}{g^{t-1}} + \frac{1}{g^{t-1}}$, ale ze stwierdzenia 9.37, $0 < \frac{1}{g^n} < \frac{1}{n}$ dla $n = 1, 2, \ldots$ i $\lim\limits_{n\to\infty} \frac{1}{n} = 0$, więc z twierdzenia o trzech ciągach, $\lim\limits_{n\to\infty} \frac{1}{g^n} = 0$. Ponadto $\lim\limits_{n\to\infty}\left(\frac{\lfloor g^n x \rfloor}{g^n} + \frac{1}{g^n}\right) = \lim\limits_{n\to\infty} \frac{\lfloor g^n x \rfloor}{g^n} + \lim\limits_{n\to\infty} \frac{1}{g^n}$, więc na mocy wzoru (15.3), $\lim\limits_{n\to\infty}\left(\frac{\lfloor g^n x \rfloor}{g^n} + \frac{1}{g^n}\right) = x + 0 = x$. Wobec tego $x = \frac{\lfloor g^{t-1} x \rfloor}{g^{t-1}} + \frac{1}{g^{t-1}}$, skąd $g^{t-1}x - 1 = \lfloor g^{t-1} x \rfloor$, co przeczy wzorowi (9.15). Zatem nie istnieje liczba naturalna t taka, że $c_n = g-1$ dla wszystkich $n \geqslant t$. □

Dla dowolnego $n \in \mathbb{N}$ i dla dowolnych $c_1, \ldots, c_n \in \{0, 1, \ldots, g-1\}$ wprowadzamy oznaczenie:

$$(0, c_1 c_2 \ldots c_n)_g = \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n}, \tag{15.4}$$

które nazywamy **rozwinięciem na ułamek przy podstawie** g. Na przykład przy podstawie 10 jest $0,102 = (0,102)_{10} = \frac{1}{10} + \frac{0}{100} + \frac{2}{1000} = \frac{102}{1000}$.

Zauważmy jeszcze, że przy powyższych oznaczeniach, $\frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n} = \frac{c_1 g^{n-1} + c_2 g^{n-2} + \ldots + c_n}{g^n}$, więc mamy wzór:

$$(0, c_1 c_2 \ldots c_n)_g = \frac{(c_1 c_2 \ldots c_n)_g}{(1\underbrace{0\ldots0}_{n\ \ zer})_g}. \tag{15.5}$$

Wzór (ii) z twierdzenia 15.2 możemy teraz zapisać w postaci:

$$\frac{\lfloor g^n x \rfloor}{g^n} = \lfloor x \rfloor + (0, c_1 c_2 \ldots c_n)_g. \tag{15.6}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stąd wobec wzoru (15.3) wnosimy, że ciąg ułamków przy podstawie g:

$$\lfloor x\rfloor + (0, c_1)_g,\ \lfloor x\rfloor + (0, c_1c_2)_g,\ \lfloor x\rfloor + (0, c_1c_2c_3)_g,\ \ldots$$

jest zbieżny do x. Wyrażamy to też w postaci ułamka nieskończonego:

$$x = \lfloor x\rfloor + (0, c_1c_2c_3\ldots)_g. \tag{15.7}$$

Wobec (15.1) i (15.6) błąd, który popełniamy zatrzymując się na n-tej cyfrze rozwinięcia (15.7) jest mniejszy od $\frac{1}{g^n}$.

Rozwinięcie (15.7), w którym nieskończenie wiele cyfr c_n jest różnych od $g-1$, nazywamy **normalnym**. Ponadto, ciąg cyfr (c_n) w systemie S_g nazywamy **normalnym**, jeżeli nieskończenie wiele jego wyrazów jest różnych od $g-1$, czyli gdy dla każdego $m \in \mathbb{N}$ istnieje $n \geqslant m$ takie, że $a_{n+1} < g-1$. Zatem w punkcie (iii) twierdzenia 15.2 udowodniliśmy, że podane tam rozwinięcie liczby x jest normalne. Wobec tego **każda liczba rzeczywista ma przy każdej podstawie $g > 1$ rozwinięcie normalne na ułamek nieskończony**.

Następne twierdzenie podaje nowy sposób wyznaczania cyfr rozwinięcia normalnego liczby rzeczywistej.

Twierdzenie 15.3. *Dla dowolnej ustalonej liczby rzeczywistej x określamy ciąg (x_n) liczb rzeczywistych przyjmując, że $x_1 = x - \lfloor x\rfloor$ oraz $x_{n+1} = gx_n - \lfloor gx_n\rfloor$ dla $n = 1, 2, \ldots$. Wówczas:*
(i) $x_n = g^{n-1}x - \lfloor g^{n-1}x\rfloor$ dla każdego $n = 1, 2, \ldots$,
(ii) $c_n = \lfloor gx_n\rfloor$ dla każdego $n = 1, 2, \ldots$.

Dowód. (i). Stosujemy indukcję względem n. Dla $n = 1$, $g^0x - \lfloor g^0x\rfloor = x - \lfloor x\rfloor$, bo $g^0 = 1$ i wzór nasz zachodzi. Załóżmy, że nasz wzór zachodzi dla pewnego naturalnego n, czyli $x_n = g^{n-1}x - \lfloor g^{n-1}x\rfloor$. Wtedy $x_{n+1} = gx_n - \lfloor gx_n\rfloor = g^nx - g\lfloor g^{n-1}x\rfloor - \lfloor g^nx - g\lfloor g^{n-1}x\rfloor\rfloor$. Ale na mocy stwierdzenia 9.46 (ii), $\lfloor g^nx - g\lfloor g^{n-1}x\rfloor\rfloor = \lfloor g^nx\rfloor - g\lfloor g^{n-1}x\rfloor$, więc $x_{n+1} = g^nx - g\lfloor g^{n-1}x\rfloor - \lfloor g^nx\rfloor + g\lfloor g^{n-1}x\rfloor = g^nx - \lfloor g^nx\rfloor$, czyli nasz wzór zachodzi także dla liczby $n+1$. Zatem na mocy zasady indukcji matematycznej nasz wzór zachodzi dla każdego naturalnego n.

(ii). Wynika od razu z (i) oraz z twierdzenia 15.2. □

Aby więc znaleźć kolejne cyfry rozwinięcia normalnego liczby rzeczywistej x, wyznaczamy kolejno:
$x_1 = x - \lfloor x \rfloor$, $c_1 = \lfloor gx_1 \rfloor$, $x_2 = gx_1 - \lfloor gx_1 \rfloor$, $c_2 = \lfloor gx_2 \rfloor$, $x_3 = gx_2 - \lfloor gx_2 \rfloor$, $c_3 = \lfloor gx_3 \rfloor$, itd.

Lemat 15.4. *Niech $c_i \in \{0, 1, \ldots, g-1\}$ dla $i = 1, 2, \ldots$. Jeżeli $c_{n+1} < g - 1$ dla pewnego $n \in \mathbb{N}$, to dla każdego $k \in \mathbb{N}$:*

$$0 \leqslant (0, c_1 c_2 \ldots c_n \ldots c_{n+k})_g - (0, c_1 c_2 \ldots c_n)_g < \frac{g-1}{g^{n+1}}.$$

Dowód. Ze wzoru (15.4) wynika, że

$$(0, c_1 c_2 \ldots c_n \ldots c_{n+k})_g - (0, c_1 c_2 \ldots c_n)_g = \frac{c_{n+1}}{g^{n+1}} + \ldots + \frac{c_{n+k}}{g^{n+k}},$$

skąd $0 \leqslant (0, c_1 c_2 \ldots c_n \ldots c_{n+k})_g - (0, c_1 c_2 \ldots c_n)_g$, ale $c_{n+1} \leqslant g - 2$ oraz $c_i \leqslant g - 1$ dla $i = n+2, \ldots, n+k$, więc

$$(0, c_1 c_2 \ldots c_n \ldots c_{n+k})_g - (0, c_1 c_2 \ldots c_n)_g \leqslant \frac{g-2}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots + \frac{g-1}{g^{n+k}}.$$

Ponadto $\frac{g-2}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots + \frac{g-1}{g^{n+k}} = \frac{g-1}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots + \frac{g-1}{g^{n+k}} - \frac{1}{g^{n+1}}$ oraz $\frac{g-1}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots + \frac{g-1}{g^{n+k}} = \frac{g-1}{g^{n+1}}(1 + \frac{1}{g} + \ldots + \frac{1}{g^{k-1}}) = \frac{g-1}{g^{n+1}} \cdot \frac{1-\frac{1}{g^k}}{1-\frac{1}{g}} = = \frac{g-1}{g^{n+1}} \cdot \frac{g-\frac{1}{g^{k-1}}}{g-1} = \frac{g-\frac{1}{g^{k-1}}}{g^{n+1}}$, więc uzyskujemy stąd, że $(0, c_1 c_2 \ldots c_n \ldots c_{n+k})_g - (0, c_1 c_2 \ldots c_n)_g \leqslant \frac{g-\frac{1}{g^{k-1}}-1}{g^{n+1}}$, a zatem $(0, c_1 c_2 \ldots c_n \ldots c_{n+k})_g - (0, c_1 c_2 \ldots c_n)_g < \frac{g-1}{g^{n+1}}$. □

Twierdzenie 15.5. *Niech (c_n) będzie normalnym ciągiem cyfr w systemie pozycyjnym o podstawie g. Wówczas ciąg $((0, c_1 c_2 \ldots c_n)_g)$ jest zbieżny do pewnej liczby rzeczywistej c takiej, że $0 \leqslant c < 1$ oraz $c_n = \lfloor g^n c \rfloor - g \lfloor g^{n-1} c \rfloor$ dla każdego $n = 1, 2, \ldots$.*

Dowód. Oznaczmy $r_n = (0, c_1 c_2 \ldots c_n)_g$ dla $n \in \mathbb{N}$. Wtedy $r_{n+1} - r_n = = \frac{c_{n+1}}{g^{n+1}} \geqslant 0$ dla $n = 1, 2, \ldots$, więc ciąg (r_n) jest niemalejący. Ponadto, na mocy wzoru (15.5) dla każdego $n \in \mathbb{N}$ mamy, że $r_n < 1$.

Zatem ciąg (r_n) jest ograniczony z góry i jest niemalejący, więc z analizy matematycznej wiadomo, że ten ciąg jest zbieżny do pewnej liczby rzeczywistej c, przy czym $c \geqslant r_n$ dla każdego $n \in \mathbb{N}$, skąd $c \geqslant 0$. Z założenia istnieje $n \in \mathbb{N}$ takie, że $c_{n+1} < g-1$. Z lematu 15.4 wynika, że $0 \leqslant r_{n+k} - r_n < \frac{g-1}{g^{n+1}}$ dla każdego $k = 1, 2, \ldots$. Zatem $r_{n+k} < r_n + \frac{g-1}{g^{n+1}}$ dla każdego $k \in \mathbb{N}$. Przechodząc w tej nierówności do granicy względem k uzyskamy, że $c \leqslant r_n + \frac{g-1}{g^{n+1}}$. Ale ze wzoru (15.5), $r_n + \frac{g-1}{g^{n+1}} = \frac{(c_1 c_2 \ldots c_n (g-1))_g}{g^{n+1}} < 1$, więc $c < 1$. Ponadto $r_n \leqslant c \leqslant r_n + \frac{g-1}{g^{n+1}}$, więc $g^n r_n \leqslant g^n c \leqslant g^n r_n + \frac{g-1}{g}$, skąd $g^n r_n \leqslant g^n c < g^n r_n + 1$. Ze wzoru (15.5) mamy, że $g^n r_n = (c_1 c_2 \ldots c_n)_g \in \mathbb{Z}$, więc $(c_1 c_2 \ldots c_n)_g = \lfloor g^n c \rfloor$. Wynika stąd, że dla każdego $m \in \mathbb{N}$ istnieje $n \geqslant m$ takie, że $(c_1 c_2 \ldots c_n)_g = \lfloor g^n c \rfloor$. Oznaczmy $d_n = \lfloor g^n c \rfloor - g \lfloor g^{n-1} c \rfloor$ dla każdego $n = 1, 2, \ldots$. Wówczas z twierdzenia 15.2 i ze wzoru (15.5) uzyskujemy, że $\lfloor g^n c \rfloor = (d_1 d_2 \ldots d_n)_g$ dla każdego $n \in \mathbb{N}$.

Weźmy dowolne $m \in \mathbb{N}$. Wtedy istnieje $n \geqslant m$ takie, że $c_{n+1} < g-1$. Zatem z pierwszej części dowodu $\lfloor g^n c \rfloor = (c_1 c_2 \ldots c_n)_g$ i $\lfloor g^n c \rfloor = (d_1 d_2 \ldots d_n)_g$, więc $(c_1 c_2 \ldots c_n)_g = (d_1 d_2 \ldots d_n)_g$. Wobec tego na mocy stwierdzenia 14.4 uzyskujemy, że $c_i = d_i$ dla każdego $i = 1, 2, \ldots, n$, więc w szczególności $c_m = d_m$.

W ten sposób wykazaliśmy, że dla każdego $n \in \mathbb{N}$ jest $c_n = d_n$. Zatem na mocy twierdzenia 15.2, $c_n = \lfloor g^n c \rfloor - g \lfloor g^{n-1} c \rfloor$ dla każdego $n = 1, 2, \ldots$. □

Liczbę c z twierdzenia 15.5 będziemy oznaczali przez $(0, c_1 c_2 c_3 \ldots)_g$. Zatem w systemie S_g dla dowolnego normalnego ciągu cyfr (c_n) mamy:

$$(0, c_1 c_2 c_3 \ldots)_g = \lim_{n \to \infty} (0, c_1 c_2 \ldots c_n)_g \text{ oraz } 0 \leqslant (0, c_1 c_2 c_3 \ldots)_g < 1. \tag{15.8}$$

Ponadto, z twierdzenia 15.5 wynika, że jeżeli (d_n) jest normalnym ciągiem cyfr w systemie S_g, to

$$(0, c_1 c_2 c_3 \ldots)_g = (0, d_1 d_2 d_3 \ldots)_g \iff [c_n = d_n \text{ dla każdego } n \in \mathbb{N}]. \tag{15.9}$$

Stwierdzenie 15.6. *Dla dowolnych liczb naturalnych $m \geqslant n$ i dla dowolnych cyfr $c_1, \ldots, c_n$ w systemie S_g zachodzi wzór*

$$g^m \cdot (0, c_1 c_2 \ldots c_n)_g = (c_1 c_2 \ldots c_m)_g + (0, c_{m+1} c_{m+2} \ldots c_n)_g. \tag{15.10}$$

Ponadto dla dowolnego normalnego ciągu cyfr (c_n) w systemie S_g i dla dowolnej liczby naturalnej m zachodzi wzór:

$$g^m \cdot (0, c_1c_2c_3\ldots)_g = (c_1c_2\ldots c_m)_g + (0, c_{m+1}c_{m+2}\ldots)_g. \qquad (15.11)$$

Dowód. Ze wzoru (15.5) mamy, że liczb naturalnych $m \geqslant n$: $(0, c_1c_2\ldots c_n)_g = \frac{(c_1c_2\ldots c_n)_g}{g^n} = \frac{g^{n-m}\cdot(c_1c_2\ldots c_m)_g+(c_{m+1}c_{m+2}\ldots c_n)_g}{g^n}$, więc $g^m \cdot (0, c_1c_2\ldots c_n)_g = (c_1c_2\ldots c_m)_g + \frac{(c_{m+1}c_{m+2}\ldots c_n)_g}{g^{n-m}} = (c_1c_2\ldots c_m)_g + +(0, c_{m+1}c_{m+2}\ldots c_n)_g$, co kończy dowód wzoru (15.10).

Przechodząc do granicy względem n we wzorze (15.10) uzyskujemy od razu wzór (15.11). □

Stwierdzenie 15.7. *Niech (c_n) i (d_n) będą ciągami normalnymi cyfr w systemie S_g. Jeżeli $c_i = d_i$ dla $i = 1, 2, \ldots, m-1$ i $c_m < d_m$, to $(0, c_1c_2c_3\ldots)_g < (0, d_1d_2d_3\ldots)_g$.*

Dowód. Wystarczy wykazać, że przy podanych założeniach $g^m \cdot (0, c_1c_2c_3\ldots)_g < g^m \cdot (0, d_1d_2d_3\ldots)_g$, a to na mocy stwierdzenia 15.6 jest równoważne temu, że $(c_1c_2\ldots c_m)_g + (0, c_{m+1}c_{m+2}\ldots)_g < < (d_1d_2\ldots d_m)_g+(0, d_{m+1}d_{m+2}\ldots)_g$. Ponadto mamy, że $(d_1d_2\ldots d_n)_g = = (c_1c_2\ldots c_m)_g+(d_m-c_m)$, skąd $g^m\cdot(0, d_1d_2d_3\ldots)_g \geqslant (d_1d_2\ldots d_m)_g = = (c_1c_2\ldots c_m)_g + (d_m - c_m) \geqslant (c_1c_2\ldots c_m)_g + 1$ oraz $1 > (0, c_{m+1}\ldots)_g$ na mocy wzoru (15.8), więc $(0, c_1c_2c_3\ldots)_g < (0, d_1d_2d_3\ldots)_g$. □

15.2 Ułamki skończone, czysto okresowe i okresowe

Jak wiemy, każdą liczbę wymierną można jednoznacznie zapisać w postaci ułamka nieskracalnego o dodatnim mianowniku, to znaczy w postaci $\frac{k}{n}$, gdzie $k \in \mathbb{Z}$, $n \in \mathbb{N}$ i $\mathrm{NWD}(k, n) = 1$. Z twierdzenia o dzieleniu z resztą $k = qn + r$ dla pewnych $q, r \in \mathbb{Z}$ takich, że $0 \leqslant r < n$. Stąd $q \leqslant \frac{k}{n} = q + \frac{r}{n} < q + 1$, więc $[\frac{k}{n}] = q$. Ponadto w tej sytuacji $\mathrm{NWD}(n, r) = \mathrm{NWD}(n, k)$, więc $\mathrm{NWD}(n, r) = 1$, czyli ułamek $\frac{r}{n}$ jest nieskracalny i właściwy, to znaczy $\frac{r}{n} < 1$. Zatem każda liczba wymierna

jest sumą pewnej liczby całkowitej i pewnego nieujemnego nieskracalnego ułamka właściwego. Przy rozwijaniu liczb wymiernych na ułamki w systemie S_g wystarczy zatem ograniczyć się do rozwijania w tej postaci jedynie właściwych nieujemnych ułamków nieskracalnych.

Każdy ciąg cyfr w systemie S_g postaci $(c_1, c_2, \ldots, c_m, 0, 0, 0, \ldots)$ jest normalny, więc wyznacza on liczbę rzeczywistą $(0, c_1c_2 \ldots c_m000 \ldots)_g = \lim\limits_{n\to\infty} \left(\frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_m}{g^m} + 0 + \ldots + 0 \right) = \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_m}{g^m} = (0, c_1c_2 \ldots c_m)_g$. Zatem mamy wzór:

$$(0, c_1c_2 \ldots c_m000 \ldots)_g = (0, c_1c_2 \ldots c_m)_g. \tag{15.12}$$

Ułamki postaci $(0, c_1c_2 \ldots c_m000 \ldots)_g$ nazywamy **skończonymi**. Są one oczywiście liczbami wymiernymi.

Stwierdzenie 15.8. *Liczba wymierna zapisana w postaci ułamka nieskracalnego $\frac{k}{n} < 1$, gdzie $k \in \mathbb{N}_0$ i $n \in \mathbb{N}$ jest ułamkiem skończonym w systemie pozycyjnym o podstawie g wtedy i tylko wtedy, gdy każda liczba pierwsza dzieląca liczbę n jest dzielnikiem liczby g.*

Dowód. Załóżmy, że $\frac{k}{n} = (0, c_1c_2 \ldots c_m)_g$. Wtedy $\frac{k}{n} = \frac{(c_1c_2 \ldots c_m)_g}{g^m}$, ale $\mathrm{NWD}(k, n) = 1$ oraz $n \cdot (c_1c_2 \ldots c_m)_g = g^m k$, więc z zasadniczego twierdzenia arytmetyki $n | g^m$. Jeśli p jest liczbą pierwszą dzielącą n, to $p | g^m$, skąd $p | g$.

Na odwrót, załóżmy, że każda liczba pierwsza dzieląca liczbę n jest dzielnikiem liczby g. Ponieważ $g > 1$, więc $g = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ dla pewnych różnych liczb pierwszych $p_1, p_2, \ldots, p_s$ i dla pewnych liczb naturalnych $\alpha_1, \alpha_2, \ldots, \alpha_s$, więc $n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$ dla pewnych nieujemnych liczb całkowitych $\beta_1, \beta_2, \ldots, \beta_s$. Istnieje liczba naturalna $m \geqslant \max\{\frac{\beta_1}{\alpha_1}, \ldots, \frac{\beta_s}{\alpha_s}\}$, skąd $m\alpha_i \geqslant \beta_i$ dla każdego $i = 1, 2, \ldots, s$. Wobec tego $n | g^m$, więc $g^m = n \cdot l$ dla pewnego $l \in \mathbb{N}$. Zatem $\frac{k}{n} = \frac{kl}{g^m}$, ale $0 \leqslant \frac{k}{n} < 1$, więc też $0 \leqslant \frac{kl}{g^m} < 1$, skąd na mocy twierdzenia 14.7 mamy, że $kl = (c_1c_2 \ldots c_m)_g$ dla pewnych cyfr $c_1, c_2, \ldots, c_m$ w systemie S_g. Zatem $\frac{k}{n} = (0, c_1c_2 \ldots c_m)_g$. □

Wniosek 15.9. *Liczba wymierna zapisana w postaci ułamka nieskracalnego $\frac{k}{n} < 1$, gdzie $k \in \mathbb{N}_0$ i $n \in \mathbb{N}$ jest ułamkiem dziesiętnym skończonym wtedy i tylko wtedy, gdy $n = 2^\alpha \cdot 5^\beta$ dla pewnych $\alpha, \beta \in \mathbb{N}_0$.*

Niech $c_1, c_2, \ldots, c_m$ będą cyframi w systemie pozycyjnym o podstawie g, niech $x_n = (0, c_1c_2 \ldots c_n)_g$ dla $n = 1, 2, \ldots, m$ i niech $x_n = (0, c_1c_2 \ldots c_m \underbrace{g-1\ g-1 \ldots\ g-1}_{n-m})_g$ dla każdego $n = m+1$, $m+2, \ldots$. Wówczas dla $n > m$ mamy, że $x_n = (0, c_1c_2 \ldots c_m)_g + \frac{g-1}{g^{m+1}} + \ldots + \frac{g-1}{g^n}$, ale $\frac{g-1}{g^{m+1}} + \ldots + \frac{g-1}{g^n} = \frac{g-1}{g^{m+1}} \cdot (1 + \frac{1}{g} + \ldots + \frac{1}{g^{n-m-1}}) = \frac{g-1}{g^{m+1}} \cdot \frac{1-\frac{1}{g^{n-m}}}{1-\frac{1}{g}} = \frac{g-1}{g^{m+1}} \cdot \frac{g}{g-1} \cdot \frac{g^{n-m}-1}{g^{n-m}} = \frac{g^{n-m}-1}{g^n} = \frac{1}{g^m} - \frac{1}{g^n}$, więc $x_n = (0, c_1c_2 \ldots c_m)_g + \frac{1}{g^m} - \frac{1}{g^n}$. Wobec tego $\lim\limits_{n\to\infty} x_n = (0, c_1c_2 \ldots c_m)_g + \dfrac{1}{g^m}$, co możemy zapisać przy pomocy wzoru:

$$(0, c_1c_2 \ldots c_m\ g-1\ g-1\ \ldots)_g = (0, c_1c_2 \ldots c_m)_g + \frac{1}{g^m}. \qquad (15.13)$$

W szczególności ułamek $(0, c_1c_2 \ldots c_m\ \ g-1\ \ g-1\ \ \ldots)_g$ jest skończony oraz jeśli $c_m < g-1$, to $(0, c_1c_2 \ldots c_m\ \ g-1\ \ g-1\ \ \ldots)_g = (0, c_1c_2 \ldots c_{m-1}\ \ c_m+1)_g$. Ponadto ze wzoru (15.13) mamy od razu następujący wzór:

$$(0, g-1\ g-1\ g-1\ \ldots)_g = 1. \qquad (15.14)$$

Na przykład w systemie dziesiątkowym: $0,999\ldots = 1$ oraz $0,8999\ldots = 0,9$. Natomiast w systemie trójkowym: $(0,222\ldots)_3 = 1$ i $(0,1222\ldots)_3 = (0,2)_3$.

Ciąg (c_n) nazywamy **czysto okresowym**, jeżeli istnieje liczba naturalna s zwana okresem taka, że $c_{n+s} = c_n$ dla każdego $n = 1, 2, \ldots$. Zatem w tej sytuacji

$$(c_n) = (c_1, c_2, \ldots, c_s, c_1, c_2, \ldots, c_s, \ldots).$$

Najmniejszy okres czysto okresowego ciągu (c_n) nazywamy **okresem podstawowym (zasadniczym)**.

Mówimy, że liczba rzeczywista x ma rozkład **czysto okresowy** w postaci ułamka w systemie pozycyjnym o podstawie g, jeżeli w jej rozkładzie normalnym $x = [x] + (0, c_1c_2c_3 \ldots)_g$ ciąg cyfr (c_n) jest czysto

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

okresowy i nie składa się z samych zer. Jeżeli s jest okresem ciągu cyfr (c_n) w systemie S_g, to stosujemy następującą notację:

$$(0, c_1c_2c_3\ldots)_g = (0, (c_1c_2\ldots c_s))_g. \tag{15.15}$$

Na przykład w systemie dziesiątkowym: $0,(230) = 0,230230230\ldots$.

Stwierdzenie 15.10. *Dla dowolnego $s \in \mathbb{N}$ i dla dowolnych cyfr $c_1, c_2, \ldots, c_s$ w systemie pozycyjnym o podstawie g zachodzi wzór:*

$$(0, (c_1c_2\ldots c_s))_g = \frac{(c_1c_2\ldots c_s)_g}{\underbrace{(g-1\ g-1\ \ldots\ g-1)}_{s\ \ cyfr}{}_g} = \frac{(c_1c_2\ldots c_s)_g}{g^s-1}. \tag{15.16}$$

W szczególności istnieją $k \in \mathbb{N}_0$, $n \in \mathbb{N}$ takie, że $\mathrm{NWD}(k,n) = \mathrm{NWD}(n,g) = 1$ *oraz* $(0, (c_1c_2\ldots c_s))_g = \frac{k}{n}$ *i* $g^s \equiv 1 \pmod{n}$.

Dowód. Jeżeli $c_1 = c_2 = \ldots = c_s = g-1$, to ze wzoru (15.14), $(0, (c_1c_2\ldots c_s))_g = 1$ oraz $\frac{(c_1c_2\ldots c_s)_g}{\underbrace{(g-1\ g-1\ \ldots\ g-1)}_{s\ \ cyfr}{}_g} = \frac{(c_1c_2\ldots c_s)_g}{g^s-1} = 1$, więc wzór (15.16) zachodzi. Ponadto $1 = \frac{1}{1}$ i wystarczy przyjąć $k = n = 1$.

Załóżmy dalej, że $c_i < g-1$ dla pewnego $i = 1, 2, \ldots, s$. Wtedy ciąg (c_n) jest normalny, więc z twierdzenia 15.5 istnieje liczba rzeczywista x taka, że $0 \leqslant x < 1$ oraz $x = (0, (c_1c_2\ldots c_s))_g$. Ze wzoru (15.11), $g^s x = (c_1c_2\ldots c_s)_g + x$, więc $(g^s-1)x = (c_1c_2\ldots c_s)_g$. Ponadto $g^s - 1 = \underbrace{(g-1\ g-1\ \ldots\ g-1)}_{s}{}_g$, więc

$$x = \frac{(c_1c_2\ldots c_s)_g}{\underbrace{(g-1\ g-1\ \ldots\ g-1)}_{s\ \ cyfr}{}_g} = \frac{(c_1c_2\ldots c_s)_g}{g^s-1}.$$

Wobec tego x jest liczbą wymierną. Zatem istnieją $k \in \mathbb{N}_0$ i $n \in \mathbb{N}$ takie, że $\mathrm{NWD}(k,n) = 1$ oraz $x = \frac{k}{n}$. Stąd $n \cdot (c_1c_2\ldots c_s)_g = k \cdot (g^s-1)$ i z zasadniczego twierdzenia arytmetyki $n | g^s - 1$, ale $\mathrm{NWD}(g, g^s-1) = 1$, więc też $\mathrm{NWD}(g,n) = 1$. □

Przykład 15.11. Przedstawimy w postaci ułamka zwykłego nieskracalnego w systemie dziesiątkowym liczbę wymierną $x = 0,(120)$. Ze wzoru (15.16) mamy, że $x = \frac{120}{999}$. Stosując algorytm Euklidesa znajdujemy $\mathrm{NWD}(120, 999) = \mathrm{NWD}(120, 39) = \mathrm{NWD}(39, 3) = 3$, więc po skróceniu przez 3 otrzymamy $x = \frac{40}{333}$ i ten ułamek jest nieskracalny.

Zauważmy, że możemy nie stosować wzoru (15.16), lecz zastosować metodę użytą do jego dowodu uzyskując, że $1000x = 120 + x$, skąd $x = \frac{120}{999}$.

Stwierdzenie 15.12. *Niech $k, n, g \in \mathbb{N}$, niech $k < n$ oraz niech $\mathrm{NWD}(k, n) = \mathrm{NWD}(n, g) = 1$. Wówczas liczba wymierna $x = \frac{k}{n}$ ma rozkład czysto okresowy w postaci ułamka w systemie pozycyjnym o podstawie g i okres zasadniczy s jest krótszy niż n oraz $g^s \equiv 1 \pmod{n}$.*

Dowód. Z naszych założeń wynika, że liczby $g, g^2, \ldots, g^n$ są względnie pierwsze z liczbą n, a więc każda z nich daje z dzielenia przez n resztę różną od 0. Ponieważ z dzielenia przez n mamy dokładnie n reszt, więc pewne dwie spośród tych liczb g^i i g^{i+s} dają tę samą resztę z dzielenia przez n. Stąd $n | g^{i+s} - g^i$, a ponieważ $g^{i+s} - g^i = g^i(g^s - 1)$ i $i + s \leqslant n$, więc $s < n$ i z zasadniczego twierdzenia arytmetyki $n | g^s - 1$. Zatem $g^s - 1 = n \cdot m$ dla pewnego $m \in \mathbb{N}$ oraz $x = \frac{km}{nm} = \frac{km}{g^s - 1}$. Ponadto $x < 1$, więc $km < g^s - 1$ i z twierdzenia 14.7 istnieją cyfry $c_1, c_2, \ldots, c_s$ w systemie S_g nie wszystkie równe 0 i nie wszystkie równe $g - 1$ takie, że $km = (c_1 c_2 \ldots c_s)_g$. Stąd i ze wzoru (15.16), $x = (0, (c_1 c_2 \ldots c_s))_g$, przy czym rozkład ten jest czysto okresowy. □

Mówimy, że liczba rzeczywista x ma rozkład **okresowy** w postaci ułamka w systemie pozycyjnym o podstawie g, jeżeli jej rozkład normalny nie jest czysto okresowy oraz ma postać

$$x = [x] + (0, d_1 d_2 \ldots d_r c_1 c_2 \ldots c_s c_1 c_2 \ldots c_s \ldots)_g$$

i $c_i > 0$ dla pewnego $i = 1, 2, \ldots, s$. Liczbę s nazywamy okresem tego rozkładu, zaś najmniejszy okres nazywamy okresem podstawowym. Stosujemy wówczas następującą notację:

$$(0, d_1 d_2 \ldots d_r c_1 c_2 \ldots c_s c_1 c_2 \ldots c_s \ldots)_g = (0, d_1 d_2 \ldots d_r (c_1 c_2 \ldots c_s))_g. \tag{15.17}$$

Na przykład w systemie dziesiątkowym: $0,1579(230) = 0,1579230230230\ldots$.

Stwierdzenie 15.13. *Dla dowolnych $r, s \in \mathbb{N}$ i dla dowolnych cyfr $d_1, d_2, \ldots, d_r, c_1, c_2, \ldots, c_s$ w systemie pozycyjnym o podstawie g zachodzą wzory:*

$$(0, d_1d_2\ldots d_r(c_1c_2\ldots c_s))_g = \frac{(d_1d_2\ldots d_rc_1c_2\ldots c_s)_g - (d_1d_2\ldots d_r)_g}{(\underbrace{g-1\ g-1\ \ldots\ g-1}_{s\ cyfr}\underbrace{00\ldots0}_{r\ cyfr})_g}, \tag{15.18}$$

$$(0, d_1d_2\ldots d_r(c_1c_2\ldots c_s))_g = \frac{(d_1d_2\ldots d_rc_1c_2\ldots c_s)_g - (d_1d_2\ldots d_r)_g}{(g^s-1)g^r}. \tag{15.19}$$

Dowód. Oznaczmy $x = (0, d_1d_2\ldots d_r(c_1c_2\ldots c_s))_g$. Ze wzorów (15.10) i (15.16) mamy, że
$g^rx = (d_1d_2\ldots d_r)_g + (0, (c_1c_2\ldots c_s))_g = (d_1d_2\ldots d_r)_g + \frac{(c_1c_2\ldots c_s)_g}{g^s-1}$, więc

$$x = \frac{(d_1d_2\ldots d_r)_gg^s + (c_1c_2\ldots c_s)_g - (d_1d_2\ldots d_r)_g}{(g^s-1)g^r},$$

czyli

$$x = \frac{(d_1d_2\ldots d_rc_1c_2\ldots c_s)_g - (d_1d_2\ldots d_r)_g}{(g^s-1)g^r}.$$

Ponadto $(g^s-1)g^r = (\underbrace{g-1\ g-1\ \ldots\ g-1}_{s\ cyfr}\underbrace{00\ldots0}_{r\ cyfr})_g$, więc nasze stwierdzenie jest udowodnione. □

Przykład 15.14. W systemie dziesiątkowym dla $x = 0,1579(230)$ na mocy stwierdzenia 15.13 mamy, że $x = \frac{1579230-1579}{9990000} = \frac{1577651}{9990000}$.

Stwierdzenie 15.15. *Niech $k, n, m, g \in \mathbb{N}$, $m, n > 1$, $k < nm$ oraz niech $\mathrm{NWD}(k, nm) = \mathrm{NWD}(n, g) = 1$ i niech każda liczba pierwsza wchodząca w rozkład kanoniczny liczby m będzie dzielnikiem liczby g. Wówczas liczba wymierna $x = \frac{k}{nm}$ ma rozkład okresowy w postaci ułamka w systemie pozycyjnym o podstawie g i okres zasadniczy jest krótszy niż n.*

Dowód. Z dowodu stwierdzenia 15.8 istnieje liczba naturalna r taka, że $m|g^r$. Stąd $g^r = mu$ dla pewnego $u \in \mathbb{N}$, ale $\mathrm{NWD}(n, g) = 1$, więc stąd $\mathrm{NWD}(n, u) = 1$. Ponadto, $\mathrm{NWD}(k, nm) = 1$, więc $\mathrm{NWD}((k, n) = 1$ i wobec tego $\mathrm{NWD}(ku, n) = 1$. Dalej, $g^r x = \frac{kg^r}{mn} = \frac{ku}{n}$ i $0 < g^r x < < g^r$, bo $0 < x < 1$. Z twierdzenia o dzieleniu z resztą $ku = qn + t$ dla pewnych $q \in \mathbb{N}_0$ i $t \in \mathbb{N}$ takich, że $t < n$. Stąd $g^r x = q + \frac{t}{n}$ oraz $\mathrm{NWD}(t, n) = \mathrm{NWD}(ku, n) = 1$. Zatem $q < g^r x < g^r$, skąd $q = = (d_1 d_2 \dots d_r)_g$ dla pewnych cyfr $d_1, d_2, \dots, d_r$ w systemie S_g. Ponadto ze stwierdzenia 15.12 rozkład normalny liczby $\frac{t}{n}$ jest czysto okresowy i ma postać $\frac{t}{n} = (0, (c_1 c_2 \dots c_s))_g$. Wobec tego $g^r x = (d_1 d_2 \dots d_r)_g + +(0, (c_1 c_2 \dots c_s))_g$, skąd $x = (0, d_1 d_2 \dots d_r (c_1 c_2 \dots c_s))_g$. Ze stwierdzenia 15.10 rozkład normalny liczby x na ułamek w systemie S_g nie jest czysto okresowy, a ze stwierdzenia 15.8 ten rozkład nie jest skończony. Wobec tego rozkład normalny liczby x na ułamek w systemie S_g jest okresowy. □

Przykład 15.16. Zauważmy, że jeśli ciąg cyfr (c_n) w systemie pozycyjnym o podstawie g nie jest okresowy, to na mocy uzyskanych przez nas wyników liczba rzeczywista $x = (0, c_1 c_2 c_3 \dots)_g$ nie jest wymierna. Łatwo zauważyć, że na przykład ciąg $(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, \dots)$ nie jest okresowy, gdyż po każdej jedynce występuje coraz więcej zer. Wobec tego w dowolnym systemie S_g, $(0, 10100100010000 \dots)_g$ jest liczbą niewymierną.

Podsumujmy wyniki uzyskane przez nas w następującym twierdzeniu.

Twierdzenie 15.17. *Ciąg cyfr w rozkładzie normalnym liczby rzeczywistej x w systemie pozycyjnym o podstawie g jest okresowy wtedy i tylko wtedy, gdy ta liczba jest wymierna. Ponadto, jeśli $p_1, p_2, \dots, p_s$ są wszystkimi liczbami pierwszymi występującymi w rozkładzie kanonicznym liczby g i $x = \frac{k}{n}$, gdzie $k \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(k, n) = 1$, to liczba x ma rozkład w systemie S_g na ułamek*

(i) skończony wtedy i tylko wtedy, gdy $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ dla pewnych $\alpha_1, \alpha_2, \dots, \alpha_s \in \mathbb{N}_0$,

(ii) czysto okresowy wtedy i tylko wtedy, gdy $n > 1$ i w rozkładzie kanonicznym liczby n nie występuje żadna z liczb $p_1, p_2, \dots, p_s$,

(iii) okresowy wtedy i tylko wtedy, gdy $n > 1$ i w rozkładzie kanonicznym liczby n występuje pewna z liczb $p_1, p_2, \ldots, p_s$ oraz wystąpi liczba pierwsza p różna od każdej z liczb $p_1, p_2, \ldots, p_s$.

Ćwiczenie 15.18. Z ilu co najwyżej różnych cyfr może się składać okres ułamka $\frac{1}{7}$?

Ćwiczenie 15.19. Które z ułamków: $\frac{14}{34}$, $\frac{1}{125}$, $\frac{12}{8}$, $\frac{13}{20}$ mają tylko rozwinięcie dziesiętne okresowe?

Ćwiczenie 15.20. Zapisz w postaci ułamka zwykłego nieskracalnego następujące liczby:
(a) $7,5(3)$, (b) $2,1(32)$, (c) $\frac{0,23(7)+\frac{43}{450}}{0,5(6)-\frac{113}{495}}$, (d) $\frac{0,1(6)+0,(3)}{0,(3)+1,1(6)}$.

Ćwiczenie 15.21. Przedstaw liczby: $\frac{1}{2}$, $\frac{2}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, $\frac{3}{7}$ w systemach:
(a) dwójkowym, (b) trójkowym, (c) czwórkowym.

Twierdzenie 15.22. *Nie istnieje ciąg (a_n) taki, że $\{a_n : n \in \mathbb{N}\} = (0,1)$.*

Dowód. Załóżmy, że taki ciąg istnieje. Wtedy istnieje też ciąg (b_n), którego wyrazami są wszystkie liczby rzeczywiste z przedziału $(0,1)$, które w systemie trójkowym są postaci $0,c_1c_2\ldots$, gdzie $c_i \in \{0,1\}$ dla każdego $i = 1,2,\ldots$. Zdefiniujemy liczbę $c \in (0,1)$ następująco w systemie trójkowym: $c = 0,c_1c_2\ldots$, gdzie $c_i = 0$, jeśli i-cyfra liczby b_i jest równa 1 oraz $c_i = 1$, jeśli i-ta cyfra liczby b_i jest równa 0. Wtedy rozkład liczby c na ułamek dziesiętny w systemie trójkowym jest normalny oraz $c \in (0,1)$ i każda cyfra tego rozwinięcia jest równa 0 lub 1. Wobec tego na mocy wzoru (15.9), $c = b_n$ dla pewnego $n \in \mathbb{N}$. Ale wtedy c_n jest równe n-tej cyfrze rozwinięcia liczby b_n, co przeczy określeniu liczby c. □ □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 16

Liniowe równania diofantyczne

Diofantos (III wiek n.e.) jest nazywany ojcem algebry. Zasłynął on dzięki dziełu *Arithmetica* oraz dzięki rezultatom osiągniętym w teorii równań algebraicznych oraz badaniom w teorii liczb. Dzieło Diofantosa jest arytmetyczno-algebraiczne, w odróżnieniu od geometrycznych dzieł innych matematyków tamtych czasów. Traktuje on ułamki jak inne liczby, wprowadza zapis symboliczny, a także poszerza zakres sposobów rozwiązywania równań do trzeciego stopnia włącznie.

Równaniem diofantycznym nazywamy równanie postaci:

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{16.1}$$

gdzie f jest funkcją n-zmiennych i $n \geqslant 2$, a jego **rozwiązaniem** jest każdy ciąg $(a_1, a_2, \ldots, a_n)$ liczb całkowitych taki, że $f(a_1, a_2, \ldots, a_n) = 0$. Równanie diofantyczne posiadające co najmniej jedno rozwiązanie nazywamy **rozwiązalnym**. Jeśli f jest wielomianem o współczynnikach całkowitych, to (16.1) nazywamy **algebraicznym równaniem diofantycznym**.

Z równaniem diofantycznym są związane następujące fundamentalne problemy:

Problem 1. Czy jest ono rozwiązalne?

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Problem 2. Jeśli jest rozwiązalne, to czy liczba wszystkich jego rozwiązań jest skończona czy nieskończona?

Problem 3. Jeśli jest rozwiązalne, to wyznaczyć wszystkie jego rozwiązania.

Prace Diofantosa związane z równaniem (16.1) były kontynuowane przez chińskich matematyków (III wiek), arabskich (VIII-XII wiek) i później przy zastosowaniu bardziej zaawansowanych metod przez Fermata, Eulera, Lagrange'a, Gaussa i wielu innych matematyków. Równania diofantyczne mają nadal wielkie znaczenie we współczesnej matematyce i jej zastosowaniach.

W kontekście tych pytań warto wspomnieć o słynnym dziesiątym problemie Hilberta postawionym w roku 1900, które brzmi: „Czy dla każdego równania diofantycznego istnieje algorytm, który pozwala w skończonej liczbie kroków rozstrzygnąć, czy to równanie ma rozwiązanie?". Dziesiąty problem Hilberta ma duże znaczenie historyczne, ponieważ próby jego rozwiązania doprowadziły do znacznego rozwoju ścisłej notacji „obliczalności". W latach trzydziestych ubiegłego wieku trzej matematycy Kurt Gödel, Alan Turing i Alonzo Church zaproponowali niezależnie trzy precyzyjne definicje obliczalności, które okazały się równoważne. Od tego czasu dziesiąty problem Hilberta zaczęto precyzować jako pytanie o maszynę Turinga, która, działając na podaną listę współczynników równania diofantycznego, kończy pracę wtedy i tylko wtedy, gdy równanie o takich współczynnikach nie posiada rozwiązania. Nad rozwiązaniem tego problemu pracowało przez kilkadziesiąt lat wielu wybitnych matematyków. Ostateczne negatywne rozwiązanie tego problemu podał w 1970 roku rosyjski matematyk J. Matijasevic (por. [23]). Ogólnie dowód sprowadza się do pokazania, w jaki sposób działanie dowolnej maszyny Turinga można zakodować w postaci układu równań diofantycznych. To pozwala na sprowadzenie pytania o własność stopu dowolnej maszyny Turinga do pytania o rozwiązywalność pewnego równania diofantycznego. Należy podkreślić, że negatywne rozwiązanie dziesiątego problemu Hilberta nie oznacza, że istnieją problemy dotyczące rozwiązywalności równań diofantycznych, które są matematycznie nierozstrzygalne. Pytanie o istnienie takich problemów pozostaje otwarte.

Około 1637 roku Pierre de Fermat na marginesie czytanej przez siebie książki Diofantosa *Arithmetica*, zanotował po łacinie uwagę:

> „Wiadomo, że nie można rozłożyć sześcianu na dwa sześciany ani bikwadratu na dwa bikwadraty, ani żadnej potęgi, oprócz kwadratu, na dwie inne potęgi o tym samym wykładniku. Odkryłem prawdziwie cudowny dowód tego faktu, jednakże ten margines jest zbyt wąski, by go zmieścić."

W języku współczesnym Wielkie Twierdzenie Fermata można wypowiedzieć następująco: **Dla dowolnej liczby naturalnej** $n > 2$ **równanie**

$$x^n + y^n = z^n$$

nie posiada rozwiązania w niezerowych liczbach całkowitych x, y, z.

Jak pisze Aczel w [1], „to tajemnicze zdanie zapewniło zajęcie wielu pokoleniom matematyków, próbujących zrekonstruować „prawdziwie cudowny dowód", który rzekomo Fermat znał".

W XIX wieku akademie nauk we Francji i Niemczech zaoferowały nagrody dla autora dowodu. Od tej pory co roku tysiące matematyków i nawiedzonych amatorów wysyłało „dowody"do czasopism matematycznych i wydających osąd ekspertów. Na próżno.

Początkowo udało się wykazać słuszność dla poszczególnych małych wykładników. Przypadek $n = 4$ udowodnił sam Fermat, przypadek $n = 5$ udowodnił dopiero w 1828 roku Peter Gustaw Lejeune Dirichlet. Gabriel Lame i Henri Lebesgue stwierdzili, że teza twierdzenia jest prawdziwa dla $n = 7$. W przypadku wykładnika $n = 3$ dowód przedstawił Leonard Euler już w 1775 roku. Korzystał w nim z własności arytmetycznych formy kwadratowej $x^2 + 3y^2$, nie podając ich uzasadnienia. Tak więc przez długi czas dowód ten uważano za niekompletny. Dopiero Carl Friedrich Gauss zauważył, że stosunkowo prosty dowód wyniku można uzyskać przy użyciu własności pierścienia Eisensteina. Zatem po upływie dwustu lat od chwili, gdy Fermat dopisał swoją sławną uwagę na marginesie dzieła Diofantosa, jego twier-

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

dzenie było udowodnione tylko dla wykładników 3, 4, 5, 6 i 7 (i dla ich wielokrotności).

Późniejsze prace innych matematyków i obliczenia numeryczne pozwoliły udowodnić wielkie twierdzenie Fermata dla wszystkich $n < 1000000$.

Dowód ostatecznie został przeprowadzony przez angielskiego matematyka Andrew Johna Wilesa dopiero w roku 1994, co było jedną z największych sensacji naukowych XX wieku. Zajmował około 100 stron A4 i wyrażony był w języku form modularnych, reprezentacji Galois i krzywych eliptycznych.

W 1844 roku belgijski matematyk E. Catalan napisał: „Dwie kolejne liczby naturalne różne od 8 i 9 nie mogą być równocześnie pełnymi potęgami". Oznacza to, że równanie: $x^n - y^m = 1$ ma w liczbach naturalnych x, y, n, m takich, że $n, m > 1$ dokładnie jedno rozwiązanie: $x = m = 3$ i $y = n = 2$. Od tego czasu problem ten był nazywany **hipotezą Catalana**.

Już w 1850 roku Victor Amédée Lebesgue (1791-1875) udowodnił, że hipoteza Catalana jest prawdziwa dla parzystych m. Przypadek parzystego n ma jednak długą historię. W 1738 roku L. Euler udowodnił hipotezę Catalana w przypadku, gdy $2 \mid n$ i $3 \mid m$. W 1932 roku Selberg udowodnił prawdziwość hipotezy Catalana w przypadku, gdy $4 \mid n$. Dopiero w 1965 roku dzięki twierdzeniu Chao Ko zakończono dowodzenie tej hipotezy dla parzystych n.

Pierwszy dowód hipotezy Catalana podał dopiero w 2002 roku rumuński matematyk Pred Mihăilescu (por. [25]). Dowód ten jest zadziwiająco krótki, lecz bazuje na specyficznych własnościach tak zwanych ciał cyklotomicznych. Od tej pory tę hipotezę nazywa się twierdzeniem Mihăilescu.

Dużo ciekawych informacji o hipotezie Catalana i próbach jej udowodnienia można znaleźć w artykule przeglądowym [24] oraz monografii [32].

16.1 Liniowe równania diofantyczne

Definicja 16.1. Liniowym równaniem diofantycznym nazywamy równanie postaci:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{16.2}$$

gdzie $b \in \mathbb{Z}$ i liczba naturalna $n \geqslant 2$ oraz dane liczby całkowite $a_1, a_2, \ldots, a_n$ nie wszystkie są równe zero, a niewiadome $x_1, x_2, \ldots, x_n$ są liczbami całkowitymi.

Twierdzenie 16.2. *Liniowe równanie diofantyczne* (16.2) *posiada rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(a_1, a_2, \ldots, a_n) \mid b$. *Ponadto, jeżeli* $\mathrm{NWD}(a_1, a_2, \ldots, a_n) \mid b$, *to równanie* (16.2) *posiada nieskończenie wiele rozwiązań.*

Dowód. Załóżmy, że $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ dla pewnych liczb całkowitych $x_1, x_2, \ldots, x_n$. Ponieważ pewna z liczb $a_1, a_2, \ldots, a_n$ jest różna od zera, więc istnieje $d = \mathrm{NWD}(a_1, a_2, \ldots, a_n)$. Wtedy dla $i = 1, 2, \ldots, n$ istnieje $b_i \in \mathbb{Z}$ takie, że $a_i = db_i$. Stąd $b = d(b_1x_1 + b_2x_2 + \ldots + b_nx_n)$, a zatem $d \mid b$.

Na odwrót, załóżmy, że $\mathrm{NWD}(a_1, a_2, \ldots, a_n) \mid b$. Wtedy mamy, że $b = a \cdot \mathrm{NWD}(a_1, a_2, \ldots, a_n)$ dla pewnego $a \in \mathbb{Z}$. Z twierdzenia 8.28 istnieją $u_1, u_2, \ldots, u_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, a_2, \ldots, a_n) = a_1u_1 + a_2u_2 + \ldots + a_nu_n$. Zatem $b = a_1x_1 + a_2x_2 + \ldots + a_nx_n$, gdzie $x_i = au_i \in \mathbb{Z}$ dla $i = 1, 2, \ldots, n$. Jeżeli $a_i = 0$ dla pewnego $i = 1, 2, \ldots, n$, to dla każdego $k \in \mathbb{Z}$ ciąg $(x_1, \ldots, x_i + k, \ldots, x_n)$ też jest rozwiązaniem równania (16.2). Jeżeli zaś $a_j \neq 0$ dla wszystkich $j = 1, 2, \ldots, n$, to dla każdego $k \in \mathbb{N}$ ciąg $(x_1 - a_2k, x_2 + a_1k, x_3, \ldots, x_n)$ jest rozwiązaniem równania (16.2). Wobec tego równanie to posiada nieskończenie wiele rozwiązań. □

Uwaga 16.3. Zauważmy, że każde równanie postaci (16.2) takie, że $\mathrm{NWD}(a_1, \ldots, a_n) \mid b$, można za pomocą algorytmu Euklidesa sprowadzić do równania postaci

$$y_1 + 0 \cdot y_2 + \ldots + 0 \cdot y_n = c \tag{16.3}$$

dla pewnego $c \in \mathbb{Z}$. Rzeczywiście, w pierwszym kroku wybieramy niezerowy współczynnik a_i o najmniejszym module. Bez zmniejszania ogólności możemy zakładać, że jest nim a_1. Następnie z twierdzenia o dzieleniu z resztą dla każdego $i = 2, 3, \ldots, n$ dobieramy liczby całkowite q_i, r_i takie, że $a_i = q_i a_1 + r_i$ oraz $0 \leqslant r_i < |a_1|$. Wtedy z algorytmu Euklidesa: $\mathrm{NWD}(a_1, a_2, \ldots, a_n) = \mathrm{NWD}(a_1, r_2, \ldots, r_n)$. W następnym kroku robimy podstawienie:

$$z_1 = x_1 + a_2 q_2 x_2 + \ldots + a_n q_n x_n. \tag{16.4}$$

Stąd:

$$x_1 = z_1 - (a_2 q_2 x_2 + \ldots + a_n q_n x_n). \tag{16.5}$$

Teraz zauważamy, że jeżeli $(x_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania (16.2) to dla z_1 danego wzorem (16.4), $(z_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania:

$$a_1 z_1 + r_2 x_2 + \ldots + r_n x_n = b. \tag{16.6}$$

Na odwrót, jeśli $(z_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania (16.6), to dla x_1 danego wzorem (16.5), $(x_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania (16.2).
Stąd problem znalezienia wszystkich rozwiązań równania (16.2) został sprowadzony do problemu znalezienia wszystkich rozwiązań równania (16.6). Teraz, jeśli $r_2 = r_3 = \ldots = r_n = 0$, to $x_2, \ldots, x_n$ są dowolnymi liczbami całkowitymi, zaś $z_1 = \frac{b}{a_1} \in \mathbb{Z}$, bo $|a_1| = \mathrm{NWD}(a_1, \ldots, a_n)$. Jeżeli zaś pewne $r_i \neq 0$, to $0 < r_i < |a_1|$ i najmniejszy co do modułu niezerowy współczynnik przy niewiadomych w równaniu (16.6) jest mniejszy od $|a_1|$, które jest najmniejszym co do modułu niezerowym współczynnikiem przy niewiadomych w równaniu (16.2).

Następnie z równaniem (16.6) postępujemy według tej samej procedury, którą stosowaliśmy do równania (16.2). Po skończonej liczbie kroków, zgodnie z algorytmem Euklidesa, dojdziemy do równania postaci: $dy_1 + 0 \cdot y_2 + \ldots + 0 \cdot y_n = b$, gdzie $d \mid b$, więc po skróceniu przez d uzyskamy równanie postaci (16.3). W tym równaniu $y_2, \ldots, y_n$ są dowolnymi liczbami całkowitymi, zaś $y_1 = c$. Teraz cofając się z naszymi podstawieniami uzyskujemy po skończonej liczbie kroków wszystkie rozwiązania równania (16.2) i zauważamy, że będą one zależały od dokładnie $n - 1$ parametrów całkowitych.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zilustrujmy algorytm przedstawiony w uwadze 16.3 następującymi przykładami.

Przykład 16.4. Rozwiążemy liniowe równanie diofantyczne

$$6x + 10y + 15z = 1.$$

Ponieważ $\mathrm{NWD}(6, 10, 15) = \mathrm{NWD}(6, 4, 3) = \mathrm{NWD}(3, 1, 0) = 1$ i $1 \mid 1$, więc na mocy twierdzenia 16.2 nasze równanie posiada nieskończenie wiele rozwiązań. Nasze równanie możemy zapisać w postaci:

$$6(x + y + 2z) + 4y + 3z = 1.$$

Robimy podstawienie:

$$x + y + 2z = x_1.$$

Wtedy

$$x = x_1 - y - 2z$$

oraz

$$6x_1 + 4y + 3z = 1.$$

Zatem

$$0 \cdot x_1 + y + 3(2x_1 + y + z) = 1.$$

Wobec tego $x_1 = k$ oraz $2x_1 + y + z = l$ i $y = 1 - 3l$, gdzie k i l są dowolnymi liczbami całkowitymi. Zatem $z = 1 - 2k - (1 - 3l) = = 4l - 2k - 1$ oraz $x = k - (1 - 3l) - 2(4l - 2k - 1) = 5k - 5l + 1$. Wobec tego: $x = 5k - 5l + 1$, $y = 1 - 3l$ i $z = 4l - 2k - 1$, gdzie k i l są dowolnymi liczbami całkowitymi (parametrami).

Przykład 16.5. Rozwiążemy liniowe równanie diofantyczne

$$40x + 250y + 15z = 75.$$

Zauważmy, że to równanie można zapisać w postaci:

$$-5x - 5y + 15(z + 3x + 17y) = 75.$$

Wprowadzamy zatem nową niewiadomą

$$z_1 = z + 3x + 17y. \tag{16.7}$$

Wtedy

$$z = z_1 - 3x - 17y \tag{16.8}$$

oraz $-5x - 5y + 15z_1 = 75$, czyli po skróceniu przez -5:

$$x + y - 3z_1 = -15. \tag{16.9}$$

Wobec tego $y = k \in \mathbb{Z}$ i $z_1 = l \in \mathbb{Z}$ są dowolne oraz $x = -15 + 3l - k$. Ze wzoru (16.8), $z = l - 3(-15 + 3l - k) - 17k = l + 45 - 9l + 3k - 17k$, czyli $z = 45 - 14k - 8l$.

Wobec tego nasze równanie posiada nieskończenie wiele rozwiązań danych wzorami: $x = -15 + 3l - k$, $y = k$ i $z = 45 - 14k - 8l$, gdzie k i l są dowolnymi liczbami całkowitymi.

16.2 Diofantyczne równania liniowe z dwiema niewiadomymi

Ogólna postać diofantycznego równania liniowego z dwiema niewiadomymi:

$$ax + by = c, \tag{16.10}$$

gdzie a, b, c są danymi liczbami całkowitymi takimi, że $a \neq 0$ lub $b \neq 0$.

Twierdzenie 16.6. *Diofantyczne równanie liniowe* (16.10) *posiada rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(a, b) \mid c$. *Ponadto, jeśli* $\mathrm{NWD}(a, b) \mid c$ *i* $ax_0 + by_0 = c$ *dla pewnych* $x_0, y_0 \in \mathbb{Z}$, *to wszystkie rozwiązania równania* (16.10) *dane są wzorami:*

$$\begin{cases} x = x_0 + \frac{b}{\mathrm{NWD}(a,b)} \cdot k \\ y = y_0 - \frac{a}{\mathrm{NWD}(a,b)} \cdot k \end{cases}, \tag{16.11}$$

gdzie k *jest dowolną liczbą całkowitą.*

Dowód. Pierwsza część twierdzenia wynika od razu z twierdzenia 16.2. Niech dalej $\mathrm{NWD}(a, b) \mid c$. Wtedy z twierdzenia 16.2 istnieją $x_0, y_0 \in \mathbb{Z}$ takie, że $ax_0 + by_0 = c$. Dla dowolnego $k \in \mathbb{Z}$ liczby x i y dane wzorem

(16.11) są całkowite oraz $ax+by = ax_0+by_0+\frac{ab}{\mathrm{NWD}(a,b)}\cdot k-\frac{ab}{\mathrm{NWD}(a,b)}\cdot k = = ax_0 + by_0 = c$, czyli (x, y) jest rozwiązaniem równania (16.10).

Na odwrót, niech para (x, y) będzie rozwiązaniem równania (16.10). Wtedy $ax + by = ax_0 + by_0$, skąd $a(x - x_0) = b(y_0 - y)$. Zatem $\frac{a}{\mathrm{NWD}(a,b)}(x - x_0) = \frac{b}{\mathrm{NWD}(a,b)}(y_0 - y)$. Z twierdzenia 8.32 liczby $\frac{a}{\mathrm{NWD}(a,b)}$ i $\frac{b}{\mathrm{NWD}(a,b)}$ są względnie pierwsze, więc z zasadniczego twierdzenia arytmetyki, $\frac{b}{\mathrm{NWD}} \mid x - x_0$. Zatem $x - x_0 = \frac{b}{\mathrm{NWD}(a,b)} \cdot k$ dla pewnego $k \in \mathbb{Z}$ i $x = x_0+\frac{b}{\mathrm{NWD}(a,b)}\cdot k$ oraz $\frac{a}{\mathrm{NWD}(a,b)}\cdot\frac{b}{\mathrm{NWD}(a,b)}\cdot k = \frac{b}{\mathrm{NWD}(a,b)}(y_0-y)$. Stąd dla $b \neq 0$, $y_0 - y = \frac{a}{\mathrm{NWD}(a,b)} \cdot k$, czyli $y = y_0 - \frac{a}{\mathrm{NWD}(a,b)} \cdot k$. Jeżeli zaś $b = 0$, to $x = x_0$ i $a \neq 0$ oraz $\mathrm{NWD}(a, b) = |a|$, skąd $\frac{a}{\mathrm{NWD}(a,b)} = \pm 1$, więc $y = y_0 - \frac{a}{\mathrm{NWD}(a,b)} \cdot k$ dla $k = \pm(y_0 - y)$ i wtedy $x = x_0 + \frac{b}{\mathrm{NWD}(a,b)} \cdot k$. □

Uwaga 16.7. Opiszemy metodę wyznaczania jakichkolwiek liczb całkowitych x, y spełniających równanie:

$$ax + by = \mathrm{NWD}(a, b)$$

dla ustalonych liczb całkowitych a i b takich, że $a \neq 0$ lub $b \neq 0$.
Jeśli $a \mid b$, to $a \neq 0$, bo inaczej $a = b = 0$, więc $\mathrm{NWD}(a, b) = |a|$ i wystarczy przyjąć $x_0 = \pm 1$ oraz $y_0 = 0$ ($x_0 = -1$ dla $a < 0$ i $x_0 = 1$ dla $a > 0$). Podobnie jest w przypadku, gdy $b \mid a$.

Niech dalej $a \nmid b$ i $b \nmid a$. Wtedy $a \neq 0$ i $b \neq 0$. Bez zmniejszania ogólności możemy zakładać, że $|a| \leqslant |b|$. Ponieważ $a \nmid b$, więc z twierdzenia o dzieleniu z resztą $b = q_1a + r_1$ dla pewnych $q_1 \in \in \mathbb{Z}$ i $r_1 \in \mathbb{N}$ takich, że $r_1 < |a|$. Z algorytmu Euklidesa wiemy, że $\mathrm{NWD}(a, b) = \mathrm{NWD}(r_1, a)$. Jeśli więc $r_1 \mid a$, to $r_1 = \mathrm{NWD}(a, b)$ i $r_1 = a\cdot(-q_1)+b\cdot 1$. Niech dalej $r_1 \nmid a$. Wtedy z twierdzenia o dzieleniu z resztą $a = q_2r_1 + r_2$ dla pewnego $q_2 \in \mathbb{Z}$ i dla pewnego $r_2 \in \mathbb{N}$ takiego, że $r_2 < r_1$, przy czym $\mathrm{NWD}(a, b) = \mathrm{NWD}(r_2, r_1)$. Jeśli $r_2 \mid r_1$, to $\mathrm{NWD}(a, b) = r_2$ i $r_2 = a-q_2r_1 = a-q_2(b-q_1a) = a(1+q_2q_1)+b(-q_2)$, więc $\mathrm{NWD}(a, b) = a(1 + q_2q_1) + b(-q_2)$. Niech dalej $r_2 \nmid r_1$. Wtedy z twierdzenia o dzieleniu z resztą istnieją $q_3 \in \mathbb{Z}$ i $r_3 \in \mathbb{N}$ takie, że $r_1 = q_3r_2 + r_3$ oraz $r_3 < r_2$. Postępując tak dalej uzyskujemy istnienie liczby naturalnej n i liczb całkowitych $q_1, q_2, \ldots, q_n$ oraz liczb naturalnych $r_1, r_2, \ldots, r_n$ takich, że $r_1 > r_2 > \ldots > r_n$, przy czym $r_{n+1} = 0$,

$r_{-1} = b$ i $r_0 = a$ oraz mamy spełnione tożsamości:

$$r_{i-1} = q_{i+1} \cdot r_i + r_{i+1} \quad \text{dla każdego} \quad i = 0, 1, \ldots, n. \tag{16.12}$$

Wtedy z algorytmu Euklidesa $\mathrm{NWD}(a, b) = r_n$.

Teraz zapiszemy r_i w postaci $ax_i + by_i$ dla pewnych $x_i, y_i \in \mathbb{Z}$ dla każdego $i = -1, 0, 1, \ldots, n$. Mamy kolejno: $r_{-1} = b = a \cdot 0 + b \cdot 1$, więc możemy przyjąć: $x_{-1} = 0$ i $y_{-1} = 1$. Dalej, $r_0 = a = a \cdot 1 + b \cdot 0$, więc na przykład $x_0 = 1$ i $y_0 = 0$. Jeśli $x_{-1}, x_0, \ldots, x_i \in \mathbb{Z}$ oraz $y_{-1}, y_0, \ldots, y_i \in \mathbb{Z}$ są już wyznaczone dla pewnego całkowitego $i \geqslant 0$, przy czym $r_k = ax_k + by_k$ dla każdego $k = -1, 0, \ldots, i$, to ze wzoru (16.12), $r_{i+1} = r_{i-1} - q_{i+1}r_i = [ax_{i-1} + by_{i-1}] - q_{i+1}[ax_i + by_i] = a(x_{i-1} - q_{i+1}x_i) + b(y_{i-1} - q_{i+1}y_i)$, więc wystarczy przyjąć $x_{i+1} = x_{i-1} - q_{i+1}x_i$ oraz $y_{i+1} = y_{i-1} - q_{i+1}y_i$. Po skończonej liczbie kroków uzyskamy zatem, że $r_n = ax_n + by_n$ dla pewnych $x_n, y_n \in \mathbb{Z}$, ale $r_n = \mathrm{NWD}(a, b)$, więc $\mathrm{NWD}(a, b) = a \cdot x_n + b \cdot y_n$.

Przykład 16.8. Zilustrujemy uwagę 16.7 wyznaczając liczby całkowite x, y spełniające równanie diofantyczne:

$$252x + 574y = \mathrm{NWD}(252, 574).$$

Zapiszmy kolejne dzielenia z resztą w algorytmie Euklidesa wyznaczania $\mathrm{NWD}(252, 574)$:

$$\begin{aligned} 574 &= 2 \cdot 252 + 70 \\ 252 &= 3 \cdot 70 + 42 \\ 70 &= 1 \cdot 42 + 28 \\ 42 &= 1 \cdot 28 + 14 \\ 28 &= 2 \cdot 14 \end{aligned} \quad . \tag{16.13}$$

Zatem ostatnią dodatnią resztą jest liczba 14, więc $\mathrm{NWD}(252, 574) = 14$. Teraz kolejno, z pierwszej równości $70 = 252 \cdot (-2) + 574 \cdot 1$, więc po podstawieniu w drugiej równości za 70, $42 = 252 \cdot 1 - (252 \cdot (-2) + 574 \cdot 1) \cdot 3 = 252 \cdot 7 + 574 \cdot (-3)$. Dalej, z trzeciej równości $28 = 70 - 42 \cdot 1 = [252 \cdot (-2) + 574 \cdot 1] - [252 \cdot 7 + 574 \cdot (-3)] \cdot 1 = 252 \cdot (-9) + 574 \cdot 4$. W końcu z czwartej równości: $14 = 42 - 28 =$

$= [252 \cdot 7 + 574 \cdot (-3)] - [252 \cdot (-9) + 574 \cdot 4] = 252 \cdot 16 + 574 \cdot (-7)$, czyli $252 \cdot 16 + 574 \cdot (-7) = \mathrm{NWD}(252, 574)$.

Na mocy twierdzenia 16.6, wszystkie rozwiązania naszego równania diofantycznego dane są wzorami: $x = 16 + \frac{574}{14}k = 16 + 41k$, $y = -7 - \frac{252}{14}k = -7 - 18k$, gdzie k jest dowolną liczbą całkowitą.

Uwaga 16.9. Metoda opisana w uwadze 16.7 i twierdzenie 16.6 umożliwiają szybkie rozwiązywanie równań diofantycznych postaci $ax+by = c$. Mianowicie najpierw obliczamy $\mathrm{NWD}(a, b)$. Jeśli będziemy mieli, że $\mathrm{NWD}(a, b) \nmid c$, to równanie nasze nie posiada rozwiązania. W przypadku, gdy $\mathrm{NWD}(a, b) \mid c$, metodą opisaną w uwadze 16.7 znajdujemy $u, v \in \mathbb{Z}$ takie, że $au+bv = \mathrm{NWD}(a, b)$. Wtedy $x_0 = \frac{c}{NWD(a,b)}u$ i $y_0 = \frac{c}{NWD(a,b)}v$ są liczbami całkowitymi i $ax_0 + by_0 = c$. Zatem na mocy twierdzenia 16.6 wszystkie rozwiązania równania diofantycznego $ax + by = c$ dane są wzorami (16.11).

Przykład 16.10. Zastosujemy uwagę 16.9 do wyznaczenia wszystkich rozwiązań równania diofantycznego:

$$15x + 98y = 4.$$

Ponieważ $\mathrm{NWD}(15, 98) = \mathrm{NWD}(15, 8) = \mathrm{NWD}(8, -1) = 1$ i oczywiście $1 \mid 4$, więc najpierw wyznaczamy $u, v \in \mathbb{Z}$ takie, że $15u + 98v = 1$. Ponadto $98 = 6 \cdot 15 + 8$ i $15 = 2 \cdot 8 - 1$, więc $8 = 15 \cdot (-6) + 98 \cdot 1$ i $1 = 8 \cdot 2 - 15 = [15 \cdot (-6) + 98 \cdot 1] \cdot 2 + 15 \cdot (-1) = 15 \cdot (-13) + 98 \cdot 2$. Możemy zatem wziąć $u = -13$ i $v = 2$. Stąd $x_0 = 4 \cdot (-13) = -52$ i $y_0 = 4 \cdot 2 = 8$. Z twierdzenia 16.6 wszystkie rozwiązania naszego równania diofantycznego dane są zatem wzorami: $x = -52 + 98k$, $y = 8 - 15k$, gdzie k jest dowolną liczbą całkowitą.

Twierdzenie 16.11. (Sylvestera). *Niech a i b będą względnie pierwszymi liczbami naturalnymi. Wówczas każdą liczbę naturalną $c > ab-a-b$ można zapisać w postaci $c = ax+by$ dla pewnych $x, y \in \mathbb{N}_0$. Ponadto nie istnieją $x, y \in \mathbb{N}_0$ takie, że $ax + by = ab - a - b$.*

Dowód. Załóżmy, że $ax + by = ab - a - b$ dla pewnych $x, y \in \mathbb{N}_0$. Wtedy $a(x + 1) + b(y + 1) = ab$. Stąd $a \mid b(y + 1)$, więc z zasadniczego

twierdzenia arytmetyki, $a \mid y+1$, skąd $y+1 \geqslant a$. Podobnie pokazujemy, że $x+1 \geqslant b$. Wobec tego $ab = a(x+1) + b(y+1) \geqslant ab + ab$, skąd $ab \leqslant 0$, co prowadzi do sprzeczności.

Pozostaje udowodnić pierwszą część naszego twierdzenia. Z twierdzenia 16.6 istnieją $x_0, y_0 \in \mathbb{Z}$ takie, że $ax_0 + by_0 = c$. Z twierdzenia o dzieleniu z resztą wynika, że istnieją liczby całkowite k i r takie, że $y_0 = ka + r$ i $0 \leqslant r < a$. Stąd $0 \leqslant y = y_0 - ka \leqslant a - 1$, ale dla $x = x_0 + ka$ na mocy twierdzenia 16.6 mamy, że $ax + by = c$, więc $ax = c - by \geqslant c - (a-1)b$. Ponadto $c > ab - a - b$, więc $ax > ab - a - b - (a-1)b = -a$, skąd $x > -1$, czyli $x \geqslant 0$. Wobec tego $x, y \in \mathbb{N}_0$, co kończy dowód. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 17

Wybrane nieliniowe równania diofantyczne

17.1 Elementarne metody rozwiązywania równań diofantycznych

W tym podrozdziale omówiono krótko o cztery elementarne metody rozwiązywania równań diofantycznych, jakimi są: metoda kongruencyjna, zastosowanie zasady minimum, metoda faktoryzacji i metoda wykorzystująca nierówności. Więcej przykładów stosowania tych metod zostanie podana w rozdziale 19. Szerzej ten temat został przedstawiony w monografiach [3] i [4].

Metoda kongruencyjna. W wielu sytuacjach proste rozważania z użyciem kongruencji prowadzą do wniosku, że dane równanie diofantyczne nie posiada rozwiązania lub umożliwiają ograniczenie zbioru wszystkich rozwiązań tego równania.

Stwierdzenie 17.1. *Jeżeli a jest liczbą całkowitą niepodzielną przez 3, to $a^3 \equiv \pm 1 \pmod 9$.*

Dowód. Z twierdzenia o dzieleniu z resztą wynika, że $a \equiv 1, 2, 4, 5, 7, 8 \pmod 9$, skąd $a \equiv 1, 2, 4, -4, -2, -1 \pmod 9$. Ponadto mamy, że $1^3 \equiv 1 \pmod 9$, $2^3 \equiv 8 \equiv -1 \pmod 9$, $4^3 \equiv (2^3)^2 \equiv (-1)^2 \equiv 1$

$(\mathrm{mod}\ 9)$, $(-4)^3 \equiv -4^3 \equiv -1\ (\mathrm{mod}\ 9)$, $(-2)^3 \equiv -8 \equiv 1\ (\mathrm{mod}\ 9)$ i $(-1)^3 \equiv -1\ (\mathrm{mod}\ 9)$, więc $a^3 \equiv \pm 1\ (\mathrm{mod}\ 9)$. □

Przykład 17.2. Udowodnimy, że jeżeli liczby całkowite a, x, y, z są takie, że $a \equiv 2, 3, 4, 5, 6, 7\ (\mathrm{mod}\ 9)$ oraz $x^3 + ay^3 = 9z^3$, to $3 \mid x$ i $3 \mid y$ i $3 \mid z$.

Jeżeli $3 \mid x$, to $9 \mid x^3$ i $9 \mid 9z^3$, więc $9 \mid ay^3$. Dodatkowo $9 \nmid a$, więc $3 \mid y^3$, skąd $3 \mid y$. Wobec tego $27 \mid x^3 + ay^3$, skąd $27 \mid 9z^3$, więc $3 \mid z^3$, czyli $3 \mid z$.

Podobnie, jeśli $3 \mid y$, to $3 \mid ay^3$ i $3 \mid 9z^3$, więc $3 \mid x^3$, skąd $3 \mid x$ i z pierwszej części rozumowania $3 \mid z$.

Pozostaje do rozważenia przypadek, gdy $3 \nmid x$ i $3 \nmid y$. Wtedy ze stwierdzenia 17.1, $x^3 \equiv \pm 1\ (\mathrm{mod}\ 9)$ i $y^3 \equiv \pm 1\ (\mathrm{mod}\ 9)$. Zatem $x^3 + ay^3 \equiv 1 + a, 1 - a, -1 + a, -1 - a\ (\mathrm{mod}\ 9)$. Ponadto $a \equiv 2, 3, 4, 5, 6, 7\ (\mathrm{mod}\ 9)$, więc $x^3 + ay^3 \equiv 1, 2, 3, 4, 5, 6, 7, 8\ (\mathrm{mod}\ 9)$. Tymczasem $x^3 + ay^3 = 9z^3 \equiv 0\ (\mathrm{mod}\ 9)$, więc uzyskaliśmy sprzeczność.

Stąd $3 \mid x$ i $3 \mid y$ i $3 \mid z$.

Przykład 17.3. Udowodnimy, że jeżeli liczby całkowite x, y, z są takie, że $5x^3 + 11y^3 + 13z^3 = 0$, to każda z nich jest podzielna przez 13. Najpierw pokażemy, że jeżeli $a \in \mathbb{Z}$ i $13 \nmid a$, to $a^3 \equiv \pm 1, \pm 5\ (\mathrm{mod}\ 13)$. Rzeczywiście, $a \equiv \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6\ (\mathrm{mod}\ 13)$ oraz $1^3 \equiv 1\ (\mathrm{mod}\ 13)$, $2^3 = 8 \equiv -5\ (\mathrm{mod}\ 13)$, $3^3 = 17 \equiv 1\ (\mathrm{mod}\ 13)$, $4^3 = 64 \equiv -1\ (\mathrm{mod}\ 13)$, $5^3 = 5^2 \cdot 5 \equiv (-1) \cdot 5 \equiv -5\ (\mathrm{mod}\ 13)$, $6^3 = 2^3 \cdot 3^3 \equiv (-5) \cdot 1 \equiv -5\ (\mathrm{mod}\ 13)$, skąd wynika, że $a^3 \equiv \pm 1, \pm 5\ (\mathrm{mod}\ 13)$.

Przypuśćmy teraz, że $13 \nmid x$ i $13 \nmid y$. Wtedy $x^3, y^3 \equiv \pm 1, \pm 1\ (\mathrm{mod}\ 13)$ i $5x^3 + 11y^3 \equiv 5x^3 - 2y^3\ (\mathrm{mod}\ 13)$, skąd $5x^3 + 11y^3 \equiv 5a - 2b\ (\mathrm{mod}\ 13)$, gdzie $a, b \in \{1, -1, 5, -5\}$. Ponadto $5x^3 + 11y^3 = -13z^3 \equiv 0\ (\mathrm{mod}\ 13)$, więc $5a \equiv 2b\ (\mathrm{mod}\ 13)$. Stąd po pomnożeniu przez 5 obu stron tej kongruencji, $-a \equiv -3b\ (\mathrm{mod}\ 13)$, czyli $a \equiv 3b\ (\mathrm{mod}\ 13)$. Lecz $3b \equiv 3, -3, 2, -2\ (\mathrm{mod}\ 13)$, zaś $a \equiv 1, -1, 5, -5\ (\mathrm{mod}\ 13)$, więc uzyskujemy sprzeczność.

Wobec tego $13 \mid x$ lub $13 \mid y$. W pierwszym przypadku mamy, że $13 \mid 5x^3 + 13z^3$, więc $13 \mid 11y^3$, skąd $13 \mid y$. Podobnie w drugim

przypadku, $13 \mid 5x^3$, skąd $13 \mid x$. Wobec tego $13 \mid x$ i $13 \mid y$. Zatem $13^3 \mid 5x^3 + 11y^3$, czyli $13^3 \mid 13z^3$, skąd $13 \mid z$.

Ćwiczenie 17.4. Niech liczby całkowite a, x, y i z będą takie, że $a \equiv \pm 2, \pm 3, \pm 4, \pm 6 \pmod{13}$ i $x^3 + ay^3 = 13z^3$. Udowodnij, że wtedy $13 \mid x$, $13 \mid y$ i $13 \mid z$.

Wykorzystanie zasady minimum. Rozumowania, które teraz zostaną zaprezentowane były, w innej postaci, już znane i używane przez Starożytnych, (pojawiły się na przykład w *Elementach* Euklidesa). Metoda ta została później rozwinięta przez Fermata, który używał jej do rozwiązywania równań diofantycznych, dlatego w literaturze tego typu dowody nazywa się **metodą nieskończonego zejścia** Fermata. Metoda ta jest szczególnym rodzajem dowodu „nie wprost", i polega na wykazaniu, że dane zdanie nie może zachodzić dla żadnej liczby naturalnej, gdyż gdyby zdanie miało zachodzić dla pewnej liczby naturalnej k, to byłoby ono prawdziwe dla liczby naturalnej mniejszej od k, co prowadziłoby do nieskończonego, malejącego ciągu liczb naturalnych, prowadząc ostatecznie do sprzeczności. Zatem ta metoda opiera się na zasadzie minimum. Fermat był w stanie wykazać nieistnienie rozwiązań wielu klasycznych równań diofantycznych (na przykład problem czterech doskonałych kwadratów w postępie arytmetycznym).

W XX wieku metoda nieskończonego zejścia była używana w algebraicznej teorii liczb i do badania tak zwanych L-funkcji. Także Mordell udowodnił bardzo ważny wynik mówiący, że wymierne punkty na krzywej eliptycznej E tworzą skończenie generowaną grupę abelową wykorzystując metodę Fermata.

Przykład 17.5. Udowodnimy, że jeżeli liczby całkowite a, x, y, z są takie, że $a \equiv 2, 3, 4, 5, 6, 7 \pmod{9}$ oraz $x^3 + ay^3 = 9z^3$, to $x = y = z = 0$.

Załóżmy, że istnieją liczby całkowite a, x, y, z takie, że $x^3 + ay^3 = 9z^3$ oraz $a \equiv 2, 3, 4, 5, 6, 7 \pmod{9}$ i $(x, y, z) \neq (0, 0, 0)$. Wtedy na mocy zasady minimum możemy zakładać, że $|x| + |y| + |z|$ jest najmniejsze z możliwych. Z przykładu 17.2 wynika, że $x = 3X$, $y = 3Y$ i $z = 3Z$ dla pewnych $X, Y, Z \in \mathbb{Z}$, więc $(X, Y, Z) \neq (0, 0, 0)$ oraz

$3^3X^3 + a \cdot 3^3Y^3 = 9 \cdot 3^3Z^3$, skąd $X^3 + aY^3 = 9Z^3$. Ponadto $|X| + |Y| + |Z| = \frac{|z|}{3} \cdot (|x| + |y| + |z|) < |x| + |y| + |z|$, więc mamy sprzeczność z minimalnością $|x| + |y| + |z|$.

Nasze przypuszczenie doprowadziło zatem do sprzeczności. Wobec tego $x = y = z = 0$ oraz $0^3 + a \cdot 0^3 = 9 \cdot 0^3$, więc jedynym rozwiązaniem równania diofantycznego $x^3 + ay^3 = 9z^3$ jest $x = y = z = 0$.

Przykład 17.6. Udowodnimy, że jedynym rozwiązaniem równania diofantycznego $5x^3 + 11y^3 + 13z^3 = 0$ jest $x = y = z = 0$. Przypuśćmy, że tak nie jest. Wtedy z zasady minimum wynika, że istnieje takie rozwiązanie $(x, y, z) \neq (0, 0, 0)$, że $|x| + |y| + |z|$ jest najmniejsze. Z przykładu 17.3, $x = 13X$, $y = 13Y$ i $z = 13Z$ dla pewnych liczb całkowitych X, Y, Z, skąd $(X, Y, Z) \neq (0, 0, 0)$, $|X| + |Y| + |Z| = \frac{1}{3} \cdot (|x| + |y| + |z|) < |x| + |y| + |z|$ i $5 \cdot 13^3X^3 + 11 \cdot 13^3Y^3 + 13 \cdot 13^3Z^3 = 0$, skąd $5X^3 + 11Y^3 + 13Z^3 = 0$, co przeczy minimalności $|x| + |y| + |z|$.

Nasze przypuszczenie doprowadziło zatem do sprzeczności. Wobec tego $x = y = z = 0$ oraz $5 \cdot 0^3 + 11 \cdot 0^3 + 13 \cdot 0^3 = 0$, więc jedynym rozwiązaniem równania diofantycznego $5x^3 + 11y^3 + 13z^3 = 0$ jest $x = y = z = 0$.

Ćwiczenie 17.7. Niech liczby całkowite a, x, y i z będą takie, że $a \equiv \pm 2, \pm 3, \pm 4, \pm 6 \pmod{13}$ i $x^3 + ay^3 = 13z^3$. Udowodnij, że wtedy $x = y = z = 0$.

Metoda faktoryzacji polega na tym, aby dane równanie diofantyczne sprowadzić do równoważnego mu równania postaci

$$f_1(x_1, \ldots, x_n) \cdot \ldots \cdot f_s(x_1, \ldots, x_n) = a,$$

gdzie $a \in \mathbb{Z}$ oraz funkcje $f_1, \ldots, f_s$ przyjmują wartości całkowite dla wszystkich wartości całkowitych argumentów $x_1, \ldots, x_n$.

Jeżeli $a = 0$, to $f_1(x_1, \ldots, x_n) = 0$ lub $f_2(x_1, \ldots, x_n) = 0$ lub $\ldots$ lub $f_s(x_1, \ldots, x_n) = 0$.

Natomiast dla $a \neq 0$ należy wyznaczyć wszystkie $(a_1, \ldots, a_s) \in \mathbb{Z}^s$ takie, że $a_1 \cdot \ldots \cdot a_s = a$ i następnie rozwiązać wszystkie układy równań diofantycznych $f_k(x_1, \ldots, x_n) = a_k$ dla $k = 1, \ldots, s$.

Przykład 17.8. Wyznaczymy wszystkie rozwiązania równania

$$x^4 + 4 = p^y,$$

gdzie $x, y \in \mathbb{N}$ i $p \in \mathbb{P}$. Zauważmy, że $x^4 + 4 = (x^2 + 2)^2 - 4x^2 = (x^2 + 2 - 2x)(x^2 + 2 + 2x)$. Zatem $(x^2 - 2x + 2)(x^2 + 2x + 2) = p^y$. Ponadto $x^2 - 2x + 2 = (x - 1)^2 + 1 \geqslant 1$, $x^2 - 2x + 2 < x^2 + 2x + 2$ i $p \in \mathbb{P}$, więc $x^2 - 2x + 2 = p^a$ oraz $x^2 + 2x + 2 = p^b$, gdzie $a \in \mathbb{N}_0$, $b \in \mathbb{N}$ i $a < b$.

Załóżmy, że $a > 0$. Wtedy $p \mid (x^2+2x+2)-(x^2-2x+2)$, czyli $p \mid 4x$, więc $p \mid 2$ lub $p \mid x$. Ponadto $p \mid x^2 + 2x + 2$, więc jeśli $p \mid x$, to $p \mid 2$. Wobec tego $p = 2$. Stąd $x^4 + 4 = 2^y$, więc $y > 2$ i wobec tego $x = 2X$ dla pewnego $X \in \mathbb{N}$. Zatem $16X^4 + 4 = 2^y$, skąd $4X^4 + 1 = 2^{y-2}$. Dodatkowo $y > 2$, więc prawa strona tej równości jest parzysta, a lewa strona jest nieparzysta. Otrzymaliśmy zatem sprzeczność.

Wobec tego $a = 0$, skąd $(x - 1)^2 + 1 = 1$, więc $x = 1$ i $5 = p^y$, a zatem $p = 5$ i $y = 1$. Ponadto $1^4 + 5 = 5^1$. Wobec tego jedynym rozwiązaniem naszego równania jest $x = y = 1$ i $p = 5$.

Otrzymany przez nas rezultat jest uogólnieniem twierdzenia Sophie Germain, które mówi, że dla liczb naturalnych n liczba n^4+4 jest liczbą pierwszą wtedy i tylko wtedy, gdy $n = 1$.

Przykład 17.9. Wyznaczymy wszystkie $x, y \in \mathbb{N}$ takie, że

$$(xy - 47)^2 = x^2 + y^2.$$

W tym celu do obu stron tego równania dodajmy $2xy$. Uzyskamy równanie równoważne: $(xy)^2 - 94xy + 47^2 + 2xy = (x + y)^2$, a to z kolei jest równoważne równaniu $(xy - 46)^2 - 46^2 + 47^2 = (x + y)^2$. Wobec tego mamy takie równanie równoważne danemu:

$$(xy - 46)^2 - (x + y)^2 = -93.$$

Ze wzoru skróconego mnożenia uzyskujemy następną postać równoważną:

$$(xy - x - y - 46)(xy + x + y - 46) = -93.$$

Ponadto $(xy+x+y-46)-(xy-x-y-46)=2(x+y)>0$, więc stąd $xy+x+y-46\in\mathbb{N}$ i $xy+x+y-46$ dzieli liczbę $93=3\cdot 31$. Wobec tego $xy+x+y-46\in\{1,3,31,93\}$ i odpowiednio $xy-x-y-46=$ $=-93,-31,-3,-1$ oraz $x+y=47,17,17,47$, więc początkowe równanie jest równoważne czterem układom równań:

$$\begin{cases} xy+x+y=47 \\ x+y=47 \end{cases}, \quad \begin{cases} xy+x+y=49 \\ x+y=17 \end{cases},$$

$$\begin{cases} xy+x+y=77 \\ x+y=17 \end{cases}, \quad \begin{cases} xy+x+y=139 \\ x+y=47 \end{cases}.$$

Po prostych rachunkach znajdujemy wszystkie rozwiązania: $x=5$ i $y=12$ oraz $x=12$ i $y=5$.

Ćwiczenie 17.10. Wyznacz wszystkie liczby naturalne x i y takie, że $(xy-103)^2=x^2+y^2$.

Metody stosujące nierówności.

Przykład 17.11. Wyznaczymy wszystkie liczby naturalne x,y,z takie, że $x+y+z=xyz$. Zauważmy, że ze względu na symetrię zmiennych możemy najpierw rozważać przypadek, gdy $x\leqslant y\leqslant z$. Wtedy $x+y+z\leqslant 3z$, więc $x^2z\leqslant xyz\leqslant 3z$, skąd $x^2\leqslant 3$, więc $x=1$. Zatem $yz=y+z+1$, a to jest równoważne równaniu $(y-1)(z-1)=2$. Ponadto $y\leqslant z$, więc $y-1=1$ i $z-1=2$, skąd $y=2$ i $z=3$.

Ostatecznie mamy zatem dokładnie 6 rozwiązań: $(1,2,3)$, $(1,3,2)$, $(2,1,3)$, $(2,3,1)$, $(3,1,2)$ i $(3,2,1)$.

Przykład 17.12. Wyznaczymy wszystkie liczby naturalne x,y,z,t takie, że $x+y+z+t=xyzt$. Zauważmy, że ze względu na symetrię zmiennych możemy najpierw rozważać przypadek, gdy $x\leqslant y\leqslant z\leqslant t$. Wtedy $xyzt=x+y+z+t\leqslant 4t$, skąd $xyz\leqslant 4$. Zatem $x^3\leqslant 4$, skąd $x=1$ i $yz\leqslant 4$. Mamy zatem takie przypadki:

1. $x=1$, $y=1$,$z=1$. Wtedy $3+t=t$, co prowadzi do sprzeczności.

2. $x=1$, $y=1$, $z=2$. Wtedy $4+t=2t$, skąd $t=4$.

3. $x=1$, $y=1$, $z=3$. Wtedy $5+t=3t$, co jest niemożliwe.

4. $x=1$, $y=1$, $z=4$. Wtedy $6+t=4t$, skąd $t=2$ i mamy sprzeczność.

5. $x=1$, $y=2$, $z=2$. Wtedy $5+t=4t$, co jest niemożliwe.

Podsumowując mamy zatem 12 wszystkich rozwiązań:
$(1,1,2,4)$, $(1,1,4,2)$, $(1,2,1,4)$, $(1,4,1,2)$, $(1,2,4,1)$, $(1,4,2,1)$, $(2,1,1,4)$, $(4,1,1,2)$, $(2,1,4,1)$, $(4,1,2,1)$, $(2,4,1,1)$, $(4,2,1,1)$.

Ćwiczenie 17.13. Wyznacz wszystkie liczby naturalne x, y, z, t, u takie, że $x + y + z + t + u = xyztu$.

17.2 Równanie Pella

Niech D będzie liczbą naturalną. Jeśli $D = k^2$ dla pewnego $k \in \mathbb{N}$, to dla dowolnych $x, y \in \mathbb{N}$ jest $x^2 - Dy^2 \neq 1$, bo inaczej $1 = (x - ky)(x + +ky)$, skąd $x + ky \mid 1$, co jest niemożliwe, gdyż $x + ky > 1$. Okazuje się, że jeśli D nie jest kwadratem liczby naturalnej, to równanie:

$$x^2 - Dy^2 = 1 \tag{17.1}$$

zwane **równaniem Pella** lub **nieoznaczonym równaniem Fermata**, posiada rozwiązanie w liczbach naturalnych x i y. Równanie Pella, jest jednym z najważniejszych równań diofantycznych ponieważ stanowi klucz do rozwiązań kwadratowych równań diofantycznych. Ponadto, równanie to odegrało ważną rolę w rozwiązaniu Dziesiątego problem Hilberta, który dotyczył nieistnienia algorytmu rozwiązywania dowolnego równania diofantycznego. Równanie Pella było badane przez wielu wybitnych matematyków między innymi przez Fermata i Eulera. Jednak to Lagrange usystematyzował te badania w latach 60. XVIII wieku. W szczególności Lagrange jako pierwszy udowodnił, że rozwiązanie równania Pella zawsze istnieje i opracował metodę znajdowania wszystkich jego rozwiązań przy użyciu **ułamków łańcuchowych**, które zostaną omówione w następnym rozdziale. Warto tu podkreślić, że Lagrange używał liczb niewymiernych oraz liczb zespolonych do rozwiązywania równań w liczbach całkowitych, rozszerzając w ten sposób niektóre pomysły Eulera. Kiedy Euler usłyszał o tych podejściach, zauważył: „Bardzo podziwiam twoją metodę używania liczb niewymiernych, a nawet urojonych w tego rodzaju analizie, która nie zajmuje się niczym innym jak liczbami wymiernymi. Już od kilku lat mam podobne pomysły" (por. [35], s. 240). Dużo ciekawych informacji,

konkretnych przykładów i analiz równań „typu Pella" można znaleźć w pracy A. Nowickiego [29].

Przedstawimy teraz elementarny dowód tego, że jeśli liczba naturalna D nie jest kwadratem liczby naturalnej, to równanie 17.1 posiada rozwiązanie w liczbach naturalnych. Pokażemy też w jaki sposób uzyskać wszystkie takie rozwiązania w oparciu o tak zwane rozwiązanie minimalne. Pokażemy też, że dla wielu postaci liczby D można elementarnie wyliczyć rozwiązanie minimalne. Okazuje się jednak, że w przypadku ogólnym efektywny algorytm znajdowania rozwiązania minimalnego wymaga zastosowania bardziej skomplikowanego aparatu w postaci ułamków łańcuchowych. Z tego powodu i w dbałości o kompletność dowodów, temat ten szerzej zostanie omówiony w rozdziale 19.

Rozpoczynamy od lematu odkrytego przez Dirichleta:

Lemat 17.14. *Niech α będzie dowolną niewymierną liczbą rzeczywistą. Wówczas dla każdego naturalnego N istnieją liczby całkowite p i q takie, że $0 < q \leqslant N$ oraz*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}.$$

Dowód. Oznaczmy przez $[x]$ część całkowitą liczby rzeczywistej x, czyli największą liczbą całkowitą k mniejszą lub równą liczbie x. Wówczas $[x] \leqslant x < [x] + 1$, skąd $0 \leqslant x - [x] < 1$. Zatem dla niewymiernych x jest $0 < x - [x] < 1$.

Odcinek $(0, 1]$ dzielimy na N odcinków: $(0, \frac{1}{N}], (\frac{1}{N}, \frac{2}{N}], \ldots, (\frac{N-1}{N}, 1]$ długości $\frac{1}{N}$. Zauważmy, że dla $n = 1, 2, \ldots, N+1$ liczby $n\alpha - [n\alpha]$ są niewymierne i należą do przedziału $(0, 1]$. Ponadto tych liczb jest dokładnie $N + 1$, a małych przedziałów mamy dokładnie N, więc w pewnym przedziale $(\frac{k}{N}, \frac{k+1}{N}]$ leżą pewne dwie takie liczby: $n\alpha - [n\alpha]$ i $m\alpha - +[m\alpha]$, gdzie $1 \leqslant m < n \leqslant N + 1$. Stąd i z niewymierności tych liczb wynika, że ich odległość jest mniejsza od $\frac{1}{N}$. Wobec tego, $|(n - m)\alpha - ([n\alpha] - [m\alpha])| < \frac{1}{N}$. Dalej, $a = n - m \in \mathbb{N}$, przy czym $a \leqslant N$ i $b = [n\alpha] - [m\alpha] \in \mathbb{Z}$ oraz $|a\alpha - b| < \frac{1}{N}$, skąd $|\alpha - \frac{b}{a}| < \frac{1}{Na}$, co kończy nasz dowód. □

Twierdzenie 17.15. *Niech D będzie liczbą naturalną, która nie jest kwadratem liczby całkowitej. Wówczas równanie Pella $x^2 - Dy^2 = 1$ posiada rozwiązanie w liczbach naturalnych x i y.*

Dowód. Z założenia wynika, że liczba rzeczywista $\alpha = \sqrt{D}$ jest niewymierna. Oznaczmy przez U zbiór wszystkich liczb wymiernych $\frac{x}{y}$ takich, że $x \in \mathbb{Z}$, $y \in \mathbb{N}$ i $|\sqrt{D} - \frac{x}{y}| < \frac{1}{y^2}$. Z lematu 17.14 zastosowanego dla $N = 2$ wynika, że istnieją takie, że $x \in \mathbb{Z}$, $y \in \mathbb{N}$, $y \leqslant 2$ i $|\sqrt{D} - \frac{x}{y}| < \frac{1}{2y}$, skąd $|\sqrt{D} - \frac{x}{y}| < \frac{1}{y^2}$. Zatem zbiór U jest niepusty. Niech $q_1, \ldots, q_n$ będą różnymi elementami zbioru U. Z niewymierności liczby $\sqrt{D}$ wynika, że $|\sqrt{D} - q_i| > 0$ dla każdego $i = 1, \ldots, n$. Istnieje zatem liczba naturalna N taka, że $\frac{1}{N} < |\sqrt{D} - q_i| > 0$ dla każdego $i = 1, \ldots, n$. Stosując znowu lematu 17.14 uzyskujemy istnienie $x, y \in \mathbb{Z}$ takich, że $1 \leqslant y \leqslant N$ oraz $|\sqrt{D} - \frac{x}{y}| < \frac{1}{Ny} \leqslant \frac{1}{N}$, skąd $|\sqrt{D} - \frac{x}{y}| < \frac{1}{y^2}$ oraz $|\sqrt{D} - \frac{x}{y}| < |\sqrt{D} - q_i|$ dla każdego $i = 1, \ldots, n$. Wobec tego $\frac{x}{y} \in U \setminus \{q_1, \ldots, q_n\}$. W ten sposób pokazaliśmy, że zbiór U jest nieskończony.

Weźmy dowolne $q \in U$. Wtedy $q = \frac{x}{y}$ dla pewnych $x, y \in \mathbb{Z}$ takich, że $y > 0$ i $|\sqrt{D} - \frac{x}{y}| < \frac{1}{y^2}$. Zatem z nierówności trójkąta otrzymujemy, że $|\frac{x}{y}| \leqslant |\frac{x}{y} - \sqrt{D}| + |\sqrt{D}| = |\sqrt{D} - \frac{x}{y}| + \sqrt{D} < \frac{1}{y^2} + \sqrt{D}$, skąd $|\sqrt{D} + \frac{x}{y}| \leqslant$ $\leqslant |\sqrt{D}| + |\frac{x}{y}| < \frac{1}{y^2} + 2\sqrt{D} \leqslant 1 + 2\sqrt{D}$. Stąd $|x^2 - Dy^2| =$ $= y^2|D - \frac{x^2}{y^2}| = y^2|\sqrt{D} - \frac{x}{y}| \cdot |\sqrt{D} + \frac{x}{y}|$, czyli $|x^2 - Dy^2| < y^2 \cdot \frac{1}{y^2} \cdot (1 + 2\sqrt{D})$, a więc $|x^2 - Dy^2| < 1 + 2\sqrt{D}$. Ponadto $|\sqrt{D} - \frac{x}{y}| > 0$, więc $0 <$ $< |x^2 - Dy^2| < 1 + 2\sqrt{D}$. Ponieważ zbiór U jest nieskończony, więc istnieje niezerowe $c \in \mathbb{Z}$ takie, że $|c| = m < 1 + 2\sqrt{D}$ oraz dla nieskończenie wielu $q = \frac{x}{y} \in U$ będziemy mieli, że $x^2 - Dy^2 = c$. Ponadto zbiór $\mathbb{Z}_m$ wszystkich reszt z dzielenia przez m jest skończony, bo ma dokładnie m elementów, a więc zbiór $\mathbb{Z}_m \times \mathbb{Z}_m$ też jest skończony i w takim razie istnieją $r, s \in \mathbb{Z}_m$ takie, że dla nieskończenie wielu $q = \frac{x}{y} \in U$ będziemy mieli, że $x^2 - Dy^2 = c$ oraz $x \equiv r \pmod{m}$ i $y \equiv s \pmod{m}$.

W szczególności istnieją różne liczby $q_1 = \frac{x_1}{y_1}, q_2 = \frac{x_2}{y_2} \in U$ takie, że $y_1, y_2 \in \mathbb{N}$, $x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = c$, $x_2 \equiv x_1 \pmod{|c|}$ i $y_2 \equiv y_1 \pmod{|c|}$. Stąd $x_1x_2 - Dy_1y_2 \equiv x_1^2 - Dy_1^2 = c \equiv 0 \pmod{|c|}$ i $x_2y_1 - x_1y_2 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|c|}$, czyli $x_1x_2 - Dy_1y_2 = cx_0$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

oraz $x_2y_1 - x_1y_2 = cy_0$ dla pewnych $x_0, y_0 \in \mathbb{Z}$. Jeśli $y_0 = 0$, to $x_2y_1 = x_1y_2$, skąd $q_1 = q_2$, wbrew założeniu. Wobec tego $y_0 \neq 0$.

Dalej, $c^2x_0^2 - Dc^2y_0^2 = (x_1x_2 - Dy_1y_2)^2 - D(x_2y_1 - x_1y_2)^2 = x_1^2x_2^2 - 2Dx_1x_2y_1y_2 + D^2y_1^2y_2^2 - Dx_2^2y_1^2 + 2Dx_1x_2y_1y_2 - Dx_1^2y_2^2 = x_2^2(x_1^2 - Dy_1^2) - Dy_2^2(x_1^2 - Dy_1^2) = x_2^2c - Dy_2^2c = c(x_2^2 - Dy_2^2) = c^2$, więc po skróceniu przez $c^2 \neq 0$, $x_0^2 - Dy_0^2 = 1$. Ponadto, jak pokazaliśmy, $y_0 \neq 0$, więc też $x_0 \neq 0$ i stąd $|x_0|, |y_0| \in \mathbb{N}$ oraz $|x_0|^2 - D|y_0|^2 = 1$, co kończy dowód naszego twierdzenia. □

W dalszej części tego paragrafu D oznacza liczbę naturalną, która nie jest kwadratem liczby naturalnej. Najpierw omówimy pojęcie tak zwanego **rozwiązania minimalnego** równania $x^2 - Dy^2 = 1$. W tym celu udowodnimy następujące dwa lematy.

Lemat 17.16. *Dla liczb całkowitych x i y takich, że $x^2 - Dy^2 = 1$ równoważne są warunki:*

(i) $x + y\sqrt{D} > 1$,

(ii) $x, y \in \mathbb{N}$.

Dowód. Jeśli $x, y \in \mathbb{N}$, to $x + y\sqrt{D} > \sqrt{D} > 1$, gdyż $D > 1$, bo D nie jest kwadratem liczby naturalnej. Na odwrót, niech $x + y\sqrt{D} > 1$. Ponieważ $0 < 1 = x^2 - Dy^2 = (x - y\sqrt{D})(x + y\sqrt{D})$, więc stąd $x - y\sqrt{D} > 0$. Zatem $(x + y\sqrt{D}) + (x - y\sqrt{D}) > 0$, czyli $2x > 0$, skąd $x > 0$, czyli $x \in \mathbb{N}$. Ponadto $1 = (x - y\sqrt{D})(x + y\sqrt{D})$ i $x + y\sqrt{D} > 1$, więc $x - y\sqrt{D} < 1$, czyli $y\sqrt{D} > x - 1 \geqslant 0$, a zatem $y\sqrt{D} > 0$, więc $y > 0$ i wobec tego $y \in \mathbb{N}$. □

Lemat 17.17. *Załóżmy, że dla pewnej liczby całkowitej C zbiór $U = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x^2 - Dy^2 = C\}$ jest niepusty. Wówczas dla dowolnego $(x_0, y_0) \in U$ następujące warunki są równoważne:*

(i) x_0 jest najmniejszą liczbą naturalną k taką, że $(k, y) \in U$ dla pewnego $y \in \mathbb{N}$,

(ii) y_0 jest najmniejszą liczbą naturalną l taką, że $(x, l) \in U$ dla pewnego $x \in \mathbb{N}$,

(iii) $x_0 \leqslant x$ i $y_0 \leqslant y$ dla każdej pary $(x, y) \in U$,

(iv) $x_0 + y_0\sqrt{D}$ jest najmniejszą liczbą w zbiorze $\{x + y\sqrt{D} : (x, y) \in U\}$.

Dowód. $(i) \Rightarrow (ii)$. Weźmy dowolne $x, l \in \mathbb{N}$ takie, że $(x, l) \in U$. Wtedy $x \geqslant x_0$. Ponadto $x^2 - Dl^2 = x_0^2 - Dy_0^2$, więc $D(l^2 - y_0^2) = x^2 - x_0^2 \geqslant 0$, skąd $l^2 \geqslant y_0^2$, czyli $l \geqslant y_0$, bo $l, y_0 \in \mathbb{N}$. Zatem y_0 jest najmniejszą liczbą naturalną l taką, że $(x, l) \in U$ dla pewnego $x \in \mathbb{N}$.

$(ii) \Rightarrow (iii)$. Weźmy dowolną parę $(x, y) \in U$. Wtedy $x, y \in \mathbb{N}$ i na mocy założenia, $y \geqslant y_0$, ale $x^2 - Dy^2 = x_0^2 - Dy_0^2$, więc $x^2 - x_0^2 = D(y^2 - y_0^2) \geqslant 0$, skąd $x^2 \geqslant x_0^2$, więc $x \geqslant x_0$, bo $x, x_0 \in \mathbb{N}$.

$(iii) \Rightarrow (iv)$. Weźmy dowolną parę $(x, y) \in U$. Wtedy na mocy założenia $x_0 \leqslant x$ i $y_0 \leqslant y$, więc $x_0 + y_0\sqrt{D} \leqslant x + y\sqrt{D}$. Wobec tego $x_0 + y_0\sqrt{D}$ jest najmniejszą liczbą w zbiorze $\{x + y\sqrt{D} : (x, y) \in U\}$.

$(iv) \Rightarrow (i)$. Weźmy dowolną parę $(k, y) \in U$. Wtedy $x_0 + y_0\sqrt{D} \leqslant k + y\sqrt{D}$. Załóżmy, że $k < x_0$. Wtedy $k^2 < x_0^2$, ale $k^2 - Dy^2 = x_0^2 - Dy_0^2$, więc $D(y^2 - y_0^2) = k^2 - x_0^2 < 0$, skąd $y^2 < y_0^2$ i $y < y_0$. Zatem $x + y\sqrt{D} < x_0 + y_0\sqrt{D}$, co prowadzi do sprzeczności. Wobec tego $x_0 \leqslant k$, czyli x_0 jest najmniejszą liczbą naturalną k taką, że $(k, y) \in U$ dla pewnego $y \in \mathbb{N}$. □

Definicja 17.18. Załóżmy, że dla pewnego całkowitego C równanie

$$x^2 - Dy^2 = C$$

posiada rozwiązanie w liczbach naturalnych x i y. Wówczas parę (x_0, y_0) liczb naturalnych spełniającą którykolwiek z równoważnych warunków (i)-(iv) lematu 17.17 nazywamy **rozwiązaniem minimalnym (podstawowym, fundamentalnym)** tego równania.

Przykład 17.19. Niech $a \in \mathbb{N}$ i $a > 1$. Wtedy $a^2 - 1 < a^2$ i $(a-1)^2 = a^2 - 2a + 1 < a^2 - 1$. Zatem $a - 1 < \sqrt{a^2 - 1} < a$, skąd liczba naturalna $D = a^2 - 1$ nie jest kwadratem liczby naturalnej. Ponadto $a^2 - D \cdot 1^2 = 1$ i 1 jest najmniejszą liczbą naturalną. Wobec tego na mocy lematu 17.17, para $(a, 1)$ jest rozwiązaniem minimalnym równania $x^2 - (a^2 - 1)y^2 = 1$.

Przykład 17.20. Niech $a \in \mathbb{N}$. Wtedy $a^2 < a^2 + 1 < (a+1)^2$, więc liczba naturalna $D = a^2 + 1$ nie jest kwadratem liczby naturalnej. Zauważmy, że $(2a^2 + 1)^2 - D(2a)^2 = 1$. Weźmy dowolne $x, y \in \mathbb{N}$ takie, że $x^2 - Dy^2 = 1$. Wtedy $x^2 - Dy^2 > 0$ oraz $D > a^2$, więc

$x^2 > Dy^2 > (ay)^2$, czyli $x > ay$. Zatem $x \geqslant ay + 1$ i $1 = x^2 - Dy^2 \geqslant$ $\geqslant (ay+1)^2 - Dy^2 = (ay+1)^2 - (a^2+1)y^2 = 1 + 2ay - y^2$. Zatem $y^2 \geqslant 2ay$, skąd $y \geqslant 2a$. W konsekwencji tego i na mocy lematu 8.4, $(2a^2 + 1, 2a)$ jest rozwiązaniem minimalnym równania $x^2 - (a^2 + 1)y^2 = 1$.

Przykład 17.21. Niech $a \in \mathbb{N}$. Wtedy $a^2 < a^2 + 2 < (a + 1)^2$, więc liczba naturalna $D = a^2 + 2$ nie jest kwadratem liczby naturalnej. Zauważmy, że $(a^2 + 1)^2 - Da^2 = 1$. Weźmy dowolne $x, y \in \mathbb{N}$ takie, że $x^2 - Dy^2 = 1$. Wtedy $x^2 - Dy^2 > 0$ oraz $D > a^2$, więc $x^2 > Dy^2 > (ay)^2$, czyli $x > ay$. Zatem $x \geqslant ay + 1$ i $1 = x^2 - Dy^2 \geqslant (ay + 1)^2 - Dy^2 =$ $= (ay+1)^2 - (a^2+2)y^2 = 1 + 2ay - 2y^2$. Zatem $2y^2 \geqslant 2ay$, skąd $y \geqslant a$. W konsekwencji tego i na mocy lematu 17.17, $(a^2 + 1, a)$ jest rozwiązaniem minimalnym równania $x^2 - (a^2 + 2)y^2 = 1$.

Możemy teraz sformułować podstawowe twierdzenie o równaniu Pella:

Twierdzenie 17.22. *Równanie Pella $x^2 - Dy^2 = 1$ posiada rozwiązanie minimalne (x_0, y_0) i dla każdego $n \in \mathbb{N}_0$ istnieją $x_n, y_n \in \mathbb{N}$ takie, że $x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^{n+1}$. Ponadto (x_n, y_n) są wszystkimi rozwiązaniami równania $x^2 - Dy^2 = 1$ w liczbach naturalnych x, y oraz dla każdego $n \in \mathbb{N}_0$:*

$$x_{n+1} = x_0x_n + Dy_0y_n \quad \text{i} \quad y_{n+1} = y_0x_n + x_0y_n.$$

W szczególności każde równanie Pella posiada nieskończenie wiele rozwiązań w liczbach naturalnych.

Dowód. Z twierdzenia 17.15 zbiór rozwiązań w liczbach naturalnych równania Pella $x^2 - Dy^2 = 1$ jest niepusty. Stąd na mocy lematu 17.17 istnieje rozwiązanie minimalne (x_0, y_0) tego równania. Z założenia, $x_0, y_0 \in \mathbb{N}$ i $x_0^2 - Dy_0^2 = 1$. Przypuśćmy, że dla pewnego $n \in \mathbb{N}_0$ istnieją $x_n, y_n \in \mathbb{N}$ takie, że $x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^{n+1}$ oraz $x_n^2 - Dy_n^2 = 1$. Wtedy $(x_0 + y_0\sqrt{D})^{n+2} = (x_0 + y_0\sqrt{D})(x_0 + y_0\sqrt{D})^{n+1} =$ $= (x_0 + y_0\sqrt{D})(x_n + y_n\sqrt{D}) = (x_0x_n + Dy_0y_n) + (x_0y_n + y_0x_n)\sqrt{D}$, więc $x_{n+1} = x_0x_n + Dy_0y_n \in \mathbb{N}$ i $y_{n+1} = x_0y_n + y_0x_n \in \mathbb{N}$. Ponadto $x_{n+1}^2 - Dy_{n+1}^2 = (x_0x_n + Dy_0y_n)^2 - D(x_0y_n + y_0x_n)^2 = x_0^2x_n^2 +$

$+2Dx_0x_ny_0y_n + D^2y_0^2y_n^2 - Dx_0^2y_n^2 - 2Dx_0y_ny_0x_n - Dy_0^2x_n^2 = = x_n^2(x_0^2-Dy_0^2)-Dy_n^2(x_0^2-Dy_0^2) = x_n^2\cdot 1-Dy_n^2\cdot 1 = x_n^2-Dy_n^2 = 1$. Stąd na mocy zasady indukcji matematycznej $x_n, y_n \in \mathbb{N}$ i $x_n^2 - Dy_n^2 = 1$ dla każdego $n \in \mathbb{N}_0$, ale $x_{n+1} = x_0x_n + Dy_0y_n > x_n$ dla $n \in \mathbb{N}_0$, więc zbiór $\{(x_n, y_n) : n \in \mathbb{N}_0\}$ jest nieskończony. Zatem każde równanie Pella posiada nieskończenie wiele rozwiązań w liczbach naturalnych.

Weźmy teraz dowolne $x, y \in \mathbb{N}$ takie, że $x^2-Dy^2 = 1$. Z minimalności rozwiązania (x_0, y_0) na mocy lematu 17.17, $x_0+y_0\sqrt{D} \leqslant x+y\sqrt{D}$, ale $x_0 + y_0\sqrt{D} > 1$, więc dla pewnego $s \in \mathbb{N}$ jest $(x_0 + y_0\sqrt{D})^s > x + y\sqrt{D}$. Zatem z zasady maksimum istnieje największa liczba naturalna m taka, że $(x_0+y_0\sqrt{D})^m \leqslant x+y\sqrt{D}$. Stąd $x+y\sqrt{D} < (x_0+y_0\sqrt{D})^{m+1}$. Wobec tego

$$1 \leqslant \frac{x + y\sqrt{D}}{(x_0 + y_0\sqrt{D})^m} < x_0 + y_0\sqrt{D}. \tag{17.2}$$

Ponadto, $\frac{x+y\sqrt{D}}{(x_0+y_0\sqrt{D})^m} = \frac{x+y\sqrt{D}}{x_{m-1}+y_{m-1}\sqrt{D}} = \frac{(x+y\sqrt{D})(x_{m-1}-y_{m-1}\sqrt{D})}{(x_{m-1}+y_{m-1}\sqrt{D})(x_{m-1}-y_{m-1}\sqrt{D})}$, więc $\frac{x+y\sqrt{D}}{(x_0+y_0\sqrt{D})^m} = \frac{(xx_{m-1}-Dyy_{m-1})+(yx_{m-1}-xy_{m-1})\sqrt{D}}{x_{m-1}^2-Dy_{m-1}^2}$ i $x_{m-1}^2 - Dy_{m-1}^2 = 1$, czyli

$$\frac{x + y\sqrt{D}}{(x_0 + y_0\sqrt{D})^m} = (xx_{m-1}-Dyy_{m-1})+(yx_{m-1}-xy_{m-1})\sqrt{D} = a+b\sqrt{D},$$

gdzie $a = xx_{m-1}-Dyy_{m-1} \in \mathbb{Z}$ i $b = yx_{m-1}-xy_{m-1} \in \mathbb{Z}$. Stąd na mocy (17.2), $a + b\sqrt{D} \geqslant 1$. Przypuśćmy, że $a + b\sqrt{D} > 1$. Wtedy z lematu 17.16, $a, b \in \mathbb{N}$, ale na mocy (17.2), $a+b\sqrt{D} < x_0+y_0\sqrt{D}$, więc zgodnie z lematem 17.17, przeczy to minimalności rozwiązania (x_0, y_0). Wobec tego musi być, $a + b\sqrt{D} = 1$, skąd $x + y\sqrt{D} = (x_0 + y_0\sqrt{D})^m$, a zatem $(x, y) = (x_{m-1}, y_{m-1})$, co kończy dowód naszego twierdzenia. □

Z twierdzenia 17.22 oraz z przykładów 17.19 - 17.21 otrzymujemy od razu następujące wnioski:

Wniosek 17.23. *Niech $a \in \mathbb{N}$ i $a > 1$. Wówczas wszystkimi rozwiązaniami równania Pella $x^2 - (a^2 - 1)y^2 = 1$ w liczbach naturalnych x i y są pary (x_n, y_n) dla $n \in \mathbb{N}_0$ takie, że:*

$$x_n + y_n\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^{n+1}. \tag{17.3}$$

Wniosek 17.24. *Niech $a \in \mathbb{N}$. Wówczas wszystkimi rozwiązaniami równania Pella $x^2-(a^2+1)y^2=1$ w liczbach naturalnych x i y są pary (x_n, y_n) dla $n \in \mathbb{N}_0$ takie, że:*

$$x_n + y_n\sqrt{a^2+1} = (2a^2+1+2a\sqrt{a^2+1})^{n+1}. \tag{17.4}$$

Wniosek 17.25. *Niech $a \in \mathbb{N}$. Wówczas wszystkimi rozwiązaniami równania Pella $x^2-(a^2+2)y^2=1$ w liczbach naturalnych x i y są pary (x_n, y_n) dla $n \in \mathbb{N}_0$ takie, że:*

$$x_n + y_n\sqrt{a^2+2} = (a^2+1+a\sqrt{a^2+2})^{n+1}. \tag{17.5}$$

Lemat 17.26. *Niech x i y będą liczbami całkowitymi takimi, że $x^2 - Dy^2 = -1$ i $x + y\sqrt{D} > 1$. Wtedy $x, y \in \mathbb{N}$.*

Dowód. Ponieważ $(x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2 = -1$ i $x+y\sqrt{D} > 1$, więc $x+y\sqrt{D} > 0$ oraz $0 > x-y\sqrt{D}$. Po dodaniu stronami dwóch ostatnich nierówności uzyskamy, że $x+y\sqrt{D} > x-y\sqrt{D}$, skąd $2y\sqrt{D} > 0$, czyli $y > 0$, ale $y \in \mathbb{Z}$, więc $y \in \mathbb{N}$. Przypuśćmy, że $x \leqslant 0$. Wtedy $|x| = -x < y\sqrt{D}-1$, bo $x+y\sqrt{D} > 1$, ale $y \in \mathbb{N}$ i $D > 1$, więc $y\sqrt{D}-1 > 0$. Zatem $x^2 = |x|^2 < (y\sqrt{D}-1)^2 = Dy^2 - 2y\sqrt{D}+1$, czyli $-1 = x^2-Dy^2 < -2y\sqrt{D}+1$. Stąd $-2 < -2y\sqrt{D}$, czyli $1 > y\sqrt{D}$, ale $y \geqslant 1$ i $\sqrt{D} > 1$, więc otrzymujemy sprzeczność. Zatem $x > 0$, czyli $x \in \mathbb{N}$. □

Twierdzenie 17.27. *Załóżmy, że (u_0, v_0) jest rozwiązaniem minimalnym równania $x^2 - Dy^2 = -1$ w liczbach naturalnych. Wówczas $(u_0^2 + Dv_0^2, 2u_0v_0)$ jest rozwiązaniem minimalnym równania Pella $x^2 - Dy^2 = 1$.*

Dowód. Z twierdzenia 17.22 istnieje rozwiązanie minimalne (x_0, y_0) równania Pella $x^2 - Dy^2 = 1$. Oznaczmy $\alpha = x_0 + y_0\sqrt{D}$ i $\beta = u_0 + v_0\sqrt{D}$. Najpierw pokażemy, że $\beta < \alpha$. W tym celu załóżmy, że tak nie jest. Wtedy $\beta \geqslant \alpha$, ale jeśli $\beta = \alpha$, to z niewymierności $\sqrt{D}$, $u_0 = x_0$ i $v_0 = y_0$, skąd $-1 = u_0^2 - Dv_0^2 = x_0^2 - Dy_0^2 = 1$, co prowadzi do sprzeczności. Zatem $\beta > \alpha$, a ponieważ $\alpha > 0$, więc $\frac{\beta}{\alpha} > 1$. Dalej, $\frac{\beta}{\alpha} = \frac{u_0+v_0\sqrt{D}}{x_0+y_0\sqrt{D}} = \frac{(u_0+v_0\sqrt{D})(x_0-y_0\sqrt{D})}{x_0^2-Dy_0^2} = (u_0x_0-Dv_0y_0)+(v_0x_0-u_0y_0)\sqrt{D}$,

bo $x_0^2 - Dy_0^2 = 1$. Liczby $u = u_0x_0 - Dv_0y_0$ i $v = v_0x_0 - u_0y_0$ są całkowite i $u + v\sqrt{D} > 1$. Ponadto $u^2 - Dv^2 = u_0^2x_0^2 - 2Du_0x_0v_0y_0 + D^2v_0^2y_0^2 - +Dv_0^2x_0^2 + 2Dv_0x_0u_0y_0 - Du_0^2y_0^2 = u_0^2(x_0^2 - Dy_0^2) - Dv_0^2(x_0^2 - Dy_0^2) = = (u_0^2 - Dv_0^2)(x_0^2 - Dy_0^2) = (-1) \cdot 1 = -1$. Z lematu 17.26 wynika, że $u, v \in \mathbb{N}$. Stąd oraz z minimalności (u_0, v_0) i z lematu 17.17, $\frac{\beta}{\alpha} = u + +v\sqrt{D} \geqslant \beta$, skąd $\alpha \leqslant 1$ i mamy sprzeczność. Wobec tego $\beta < \alpha$.

Dalej, $\beta^2 = (u_0^2 + Dv_0^2) + 2u_0v_0\sqrt{D}$ oraz $(u_0^2 + Dv_0^2)^2 - D(2u_0v_0)^2 = = u_0^4 + 2Du_0^2v_0^2 + D^2v_0^4 - 4Du_0^2v_0^2 = (u_0^2 - Dv_0^2)^2 = (-1)^2 = 1$, więc na mocy twierdzenia 17.22, $\beta^2 = \alpha^m$ dla pewnego $m \in \mathbb{N}$. Ponadto dla $m \geqslant 2$ mamy, że $\alpha^m \geqslant \alpha^2 > \beta^2$, bo $\alpha > \beta > 1$, więc $m = 1$ i $\alpha = \beta^2$. Wobec tego, $x_0 = u_0^2 + Dv_0^2$ i $y_0 = 2u_0v_0$. □

Przykład 17.28. Znajdziemy rozwiązanie minimalne równania Pella $x^2 - 13y^2 = 1$. W tym celu wyznaczamy najpierw rozwiązanie minimalne równania $x^2 - 13y^2 = -1$. Mamy, że $13 \cdot 1^2 - 1 = 12$, $13 \cdot 2^2 - 1 = 51$, $13 \cdot 3^2 - 1 = 116$, $13 \cdot 4^2 - 1 = 207$, $13 \cdot 5^2 - 1 = 324 = 18^2$. Wobec tego rozwiązaniem minimalnym równania $x^2 - 13y^2 = -1$ jest $(18, 5)$. Na mocy twierdzenia 17.27 rozwiązaniem minimalnym równania Pella $x^2 - 13y^2 = 1$ jest $(18^2 + 13 \cdot 5^2, 2 \cdot 18 \cdot 5) = (649, 180)$.

Równania Pella „wróci” jeszcze w podrozdziale 19.4, gdzie zostanie podany między innymi algorytm znajdowania rozwiązania podstawowego, oparty na przedstawieniu liczby $\sqrt{D}$ w postaci ułamka łańcuchowego.

17.3 Równanie Pitagorasa

Równaniem Pitagorasa nazywamy równanie

$$x^2 + y^2 = z^2, \tag{17.6}$$

w którym niewiadome x, y i z są liczbami naturalnymi.

Definicja 17.29. Rozwiązaniem pierwotnym równania Pitagorasa nazywamy taką trójkę (a, b, c) liczb naturalnych, że $a^2 + b^2 = c^2$ oraz $\mathrm{NWD}(a, b, c) = 1$.

Następne stwierdzenie sprowadza problem wyznaczenia wszystkich rozwiązań równania Pitagorasa do problemu wyznaczenia wszystkich jego rozwiązań pierwotnych.

Stwierdzenie 17.30. *Trójka (x, y, z) liczb naturalnych jest rozwiązaniem równania Pitagorasa wtedy i tylko wtedy, gdy istnieje liczba naturalna d i istnieje rozwiązanie pierwotne (a, b, c) równania Pitagorasa takie, że $x = da$, $y = db$ i $z = dc$.*

Dowód. Niech $d = \mathrm{NWD}(x, y, z)$. Wtedy na mocy twierdzenia 8.32 liczby naturalne $a = \frac{x}{d}, b = \frac{y}{d}, c = \frac{z}{d}$ są względnie pierwsze, ale $x^2 + y^2 = z^2$, więc po podzieleniu obu stron tej równości przez d^2 uzyskamy, że $a^2 + b^2 = c^2$. Zatem (a, b, c) jest rozwiązaniem pierwotnym równania Pitagorasa.

Implikacja odwrotna jest oczywista ze względu na to, że obie strony równości wystarczy pomnożyć przez d^2. □

Stwierdzenie 17.31. *Jeżeli (a, b, c) jest rozwiązaniem pierwotnym równania Pitagorasa, to:*

(i) $\mathrm{NWD}(a, b) = \mathrm{NWD}(a, c) = \mathrm{NWD}(b, c) = 1$,

(ii) liczby a i b są różnej parzystości.

Dowód. (i). Przypuśćmy, że $\mathrm{NWD}(a, b) > 1$. Wtedy istnieje liczba pierwsza p taka, że $p \mid a$ i $p \mid b$, ale $a^2 + b^2 = c^2$, więc $p \mid c^2$, skąd $p \mid c$. Zatem p jest wspólnym dzielnikiem liczb a, b, c, co przeczy temu, że $\mathrm{NWD}(a, b, c) = 1$. Wobec tego $\mathrm{NWD}(a, b) = 1$.

Załóżmy, że $\mathrm{NWD}(a,c) > 1$. Wtedy istnieje liczba pierwsza p taka, że $p \mid a$ i $p \mid c$, ale $b^2 = c^2 - a^2$, więc $p \mid b^2$, skąd $p \mid b$. Zatem p jest wspólnym dzielnikiem liczb a i b, co jak wiemy, prowadzi do sprzeczności. Wobec tego $\mathrm{NWD}(a,c) = 1$.

Załóżmy, że $\mathrm{NWD}(b,c) > 1$. Wtedy istnieje liczba pierwsza p taka, że $p \mid b$ i $p \mid c$, ale $a^2 = c^2 - b^2$, więc $p \mid a^2$, skąd $p \mid a$ i znowu mamy sprzeczność. Wobec tego $\mathrm{NWD}(b,c) = 1$.

(ii). Na mocy (i) obie liczby a i b nie mogą być parzyste. Gdyby obie te liczby były nieparzyste, to liczba c musiałaby być parzysta, więc $4 \mid a^2 + b^2$. Ponadto, jak wiemy, kwadrat liczby nieparzystej daje resztę 1 z dzielenia przez 4, więc $a^2 + b^2 \equiv 2 \pmod 4$. Stąd $2 \equiv 0 \pmod 4$ i mamy sprzeczność. Zatem liczby a i b są różnej parzystości. □

Twierdzenie 17.32. *Trójka (a,b,c) liczb naturalnych takich, że a jest liczbą parzystą, jest rozwiązaniem pierwotnym równania Pitagorasa wtedy i tylko wtedy, gdy $a = 2mn$, $b = m^2 - n^2$ i $z = m^2 + n^2$, gdzie $m > n$ i liczby naturalne m i n są względnie pierwsze oraz są różnej parzystości.*

Dowód. $\Rightarrow$. Ze stwierdzenia 17.31 mamy $\mathrm{NWD}(a,b) = \mathrm{NWD}(a,c) = \mathrm{NWD}(b,c) = 1$, $a = 2k$ dla pewnego $k \in \mathbb{N}$ i liczba b jest nieparzysta oraz liczba c też jest nieparzysta. Ponadto $c > b$ i $4k^2 = a^2 = c^2 - b^2 = (c-b)(c+b)$, ale liczby $c-b$ i $c+b$ są parzyste, więc $\frac{c-b}{2}, \frac{c+b}{2} \in \mathbb{N}$ oraz $\frac{c-b}{2} \cdot \frac{c+b}{2} = k^2$. Niech $d \in \mathbb{N}$ będzie wspólnym dzielnikiem liczb $\frac{c-b}{2}$ i $\frac{c+b}{2}$. Wtedy d dzieli sumę i różnicę tych liczb, czyli $d \mid c$ i $d \mid b$, skąd $d = 1$. Wobec tego liczby $\frac{c-b}{2}$ i $\frac{c+b}{2}$ są względnie pierwsze. Zatem z twierdzenia 9.45, $\frac{c-b}{2} = n^2$ i $\frac{c+b}{2} = m^2$ dla pewnych liczb naturalnych m i n, ale $m^2 > n^2$, więc $m > n$. Ponadto, $\mathrm{NWD}(m^2, n^2) = 1$, więc $\mathrm{NWD}(m,n) = 1$. Dalej, $m^2 \cdot n^2 = k^2$, więc $k = mn$, skąd $a = 2mn$. Mamy też, że $c = \frac{c-b}{2} + \frac{c+b}{2} = m^2 + n^2$ oraz $b = \frac{c+b}{2} - \frac{c-b}{2} = m^2 - n^2$. Ponadto, liczba b jest nieparzysta, więc dodatkowo liczby m i n muszą być różnej parzystości.

$\Leftarrow$. Niech teraz m i n będą względnie pierwszymi liczbami naturalnymi różnej parzystości takimi, że $m > n$. Wtedy $a = 2mn$, $b = m^2 - n^2$ i $c = m^2 + n^2$ są liczbami naturalnymi i a jest liczbą parzystą, przy czym $a^2 + b^2 = 4m^2n^2 + m^4 - 2m^2n^2 + n^4 =$

$m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2$. Przypuśćmy, że liczby b i c nie są względnie pierwsze. Wtedy istnieje $p \in \mathbb{P}$ takie, że $p \mid b$ i $p \mid c$. Dodatkowo liczby b i c są nieparzyste, gdyż liczby m oraz n są nieparzyste, więc stąd $p > 2$. Ponadto $p \mid b + c$ i $p \mid c - b$, więc $p \mid 2m^2$ i $p \mid 2n^2$, skąd $p \mid m^2$ i $p \mid n^2$. Zatem $p \mid m$ i $p \mid n$, co przeczy temu, że liczby m i n są względnie pierwsze. Wobec tego liczby b i c są względnie pierwsze, a stąd $\mathrm{NWD}(a, b, c) = 1$. Zatem (a, b, c) jest rozwiązaniem pierwotnym równania Pitagorasa. □

Przykład 17.33. Na mocy twierdzenia 17.32 dla każdego $k \in \mathbb{N}$ trójka $(4k^2 - 1, 4k, 4k^2 + 1)$ jest rozwiązaniem pierwotnym równania Pitagorasa. Wobec tego istnieje nieskończenie wiele rozwiązań pierwotnych równania Pitagorasa.

Twierdzenie 17.34. *Równanie $x^4 + y^4 = z^2$ nie posiada rozwiązania w liczbach naturalnych x, y, z.*

Dowód. Załóżmy, że tak nie jest. Wtedy z zasady minimum istnieje najmniejsza liczba naturalna z taka, że $z^2 = x^4 + y^4$ dla pewnych $x, y \in \mathbb{N}$. Niech $d = \mathrm{NWD}(x, y)$. Wtedy $d^4 \mid x^4$ i $d^4 \mid y^4$, więc $d^4 \mid z^2$ i z twierdzenia 8.52, $d^2 \mid z$. Zatem $\frac{z}{d^2}, \frac{x}{d}, \frac{y}{d} \in \mathbb{N}$ i $(\frac{z}{d^2})^2 = (\frac{x}{d})^4 + (\frac{y}{d})^4$, więc z minimalności z, $\frac{z}{d^2} \geqslant z$, skąd $d = 1$. Wobec tego $\mathrm{NWD}(x, y) = 1$. Stąd na mocy stwierdzenia 8.49, $\mathrm{NWD}(x^2, y^2) = 1$, ale $(x^2)^2 + (y^2)^2 = z^2$, więc (x^2, y^2, z) jest rozwiązaniem pierwotnym równania Pitagorasa. Ze stwierdzenia 17.31 wynika, że x^2 jest parzyste lub y^2 jest parzyste. Bez zmniejszania ogólności możemy zakładać, że x^2 jest parzyste, a y^2 jest nieparzyste. Na mocy twierdzenia 17.32 istnieją względnie pierwsze liczby naturalne różnej parzystości m i n takie, że $m > n$ oraz $x^2 = 2mn$, $y^2 = m^2 - n^2$ i $z = m^2 + n^2$.

Stąd $n^2 + y^2 = m^2$, przy czym $\mathrm{NWD}(n, y, m) = 1$, bo $\mathrm{NWD}(m, n) = 1$, więc ze stwierdzenia 17.31, n jest parzyste. Wobec tego m jest nieparzyste i na mocy twierdzenia 17.32 istnieją względnie pierwsze liczby naturalne różnej parzystości r i s takie, że $r > s$ oraz $n = 2rs$, $y = r^2 - s^2$ i $m = r^2 + s^2$.

Zatem $x^2 = 4rs(r^2 + s^2)$. Ponadto, stąd $x = 2t$ dla pewnego $t \in \mathbb{N}$ i po skróceniu przez 4, $t^2 = rs(r^2 + s^2)$. Jeśli $\mathrm{NWD}(r, r^2 + s^2) > 1$, to

$p \mid r$ i $p \mid r^2 + s^2$ dla pewnej liczby pierwszej p, ale wtedy $p \mid s^2$, skąd $p \mid s$. Zatem p byłoby wspólnym dzielnikiem pierwszym liczb względnie pierwszych r i s, co prowadzi do sprzeczności. Zatem $\mathrm{NWD}(r, r^2+s^2) = 1$. Analogicznie pokazujemy, że $\mathrm{NWD}(s, r^2+s^2) = 1$. Ponadto mamy, że $rs(r^2+s^2) = t^2$, więc z twierdzenia 9.45, $r = a^2$, $s = b^2$ i $r^2+s^2 = c^2$ dla pewnych $a, b, c \in \mathbb{N}$. Stąd $a^4 + b^4 = c^2$ i z minimalności z, $c \geqslant z$, ale $c^2 = m < m^2 + n^2 = z$, więc mamy sprzeczność.

Przypuszczenie, że $x^4 + y^4 = z^2$ dla pewnych $x, y, z \in \mathbb{N}$ doprowadziło nas zatem do sprzeczności. Wobec tego takich liczb naturalnych x, y, z nie ma. □

Ponieważ $z^4 = (z^2)^2$, więc bezpośrednio z twierdzenia 17.34 otrzymujemy jako wniosek dowód wielkiego twierdzenia Fermata dla wykładnika 4:

Wniosek 17.35. *Równanie $x^4 + y^4 = z^4$ nie posiada rozwiązania w liczbach naturalnych x, y, z.*

Twierdzenie 17.36. *Równanie $x^4 - y^4 = z^2$ nie posiada rozwiązania w liczbach naturalnych x, y, z.*

Dowód. Przypuśćmy, że tak nie jest. Wtedy istnieje najmniejsza liczba naturalna x taka, że $x^4 - y^4 = z^2$ dla pewnych $y, z \in \mathbb{N}$. Niech $d = \mathrm{NWD}(x, y)$. Wtedy $d^4 \mid x^4$ i $d^4 \mid y^4$, skąd $d^4 \mid x^4 - y^4$, czyli $d^4 \mid z^2$, a więc $d^2 \mid z$. Wobec tego $\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2} \in \mathbb{N}$ oraz $(\frac{x}{d})^4 - (\frac{y}{d})^4 = (\frac{z}{d^2})^2$. Zauważmy, że $\frac{x}{d} \leqslant x$, więc z minimalności x, $d = 1$. Zatem liczby x i y są względnie pierwsze. Ponadto $x^4 - y^4 = z^2$, więc liczby x, y, z są parami względnie pierwsze. Dodatkowo $z^2 + (y^2)^2 = (x^2)^2$, więc na mocy stwierdzenia 17.31 liczby z i y^2 są różnej parzystości.

Niech najpierw liczba z będzie parzysta. Wtedy z twierdzenia 17.32 wynika, że $z = 2mn$, $y^2 = m^2 - n^2$ i $x^2 = m^2 + n^2$, gdzie $m > n$ i liczby naturalne m i n są względnie pierwsze oraz są różnej parzystości. Stąd $(xy)^2 = (m^2+n^2)(m^2-n^2) = m^4 - n^4$ oraz $m^2 < m^2 + n^2 = x^2$, więc $m < x$, co przeczy minimalności liczby x.

Pozostaje do rozważenia przypadek, gdy liczba z jest nieparzysta. Wtedy z twierdzenia 17.32 wynika, że $y^2 = 2mn$, $z = m^2 - n^2$ i $x^2 = m^2 + n^2$, gdzie $m > n$ i liczby naturalne m i n są względnie pierwsze

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

oraz są różnej parzystości. Jeśli liczba m jest parzysta, to liczby $2m$ i n są względnie pierwsze i $(2m)n = y^2$. Zatem z twierdzenia 9.45 mamy, że $2m = a^2$ i $n = b^2$ dla pewnych $a, b \in \mathbb{N}$. Stąd $a = 2c$ dla pewnego $c \in \mathbb{N}$ i $m = 2c^2$. Dodatkowo $x^2 = m^2 + n^2$, więc z twierdzenia 17.32 otrzymujemy, że $2c^2 = m = 2kl$, $n = k^2 - l^2$ i $x = k^2 + l^2$ dla pewnych względnie pierwszych liczb naturalnych $k > l$ różnej parzystości. Zatem $kl = c^2$, więc z twierdzenia 9.45 wynika, że $k = u^2$ i $l = v^2$ dla pewnych $u, v \in \mathbb{N}$. Wobec tego $b^2 = n = k^2 - l^2 = u^4 - v^4$, czyli $u^4 - v^4 = b^2$. Ponadto $u \leqslant u^2 = k \leqslant k^2 < k^2 + l^2 = x$, więc $u < x$, co przeczy minimalności x.

Wobec tego liczba m jest nieparzysta. Wtedy liczby m i $2n$ są względnie pierwsze i $(2n)m = y^2$. Zatem z twierdzenia 9.45 wynika, że $2n = A^2$ i $m = B^2$ dla pewnych $A, B \in \mathbb{N}$. Stąd $A = 2C$ dla pewnego $C \in \mathbb{N}$ i $n = 2C^2$. Dodatkowo $x^2 = m^2 + n^2$, więc z twierdzenia 17.32 mamy, że $2C^2 = n = 2KL$, $m = K^2 - L^2$ oraz $x = K^2 + L^2$ dla pewnych względnie pierwszych liczb naturalnych $K > L$ różnej parzystości. Zatem $KL = C^2$, więc z twierdzenia 9.45 otrzymujemy, że $K = U^2$ i $L = V^2$ dla pewnych $U, V \in \mathbb{N}$. Wobec tego $B^2 = m = K^2 - L^2 = U^4 - V^4$, czyli $U^4 - V^4 = B^2$. Ponadto $U \leqslant U^2 = K \leqslant K^2 < K^2 + L^2 = x$, więc $U < x$, co przeczy minimalności x. Kończy to dowód naszego twierdzenia. □

Wniosek 17.37. *Nie istnieją liczby naturalne x i y takie, że x^2+y^2 i $x^2 - y^2$ są kwadratami liczb naturalnych.*

Dowód. Załóżmy, że istnieją liczby naturalne x, y, a, b takie, że $x^2 + y^2 = a^2$ i $x^2 - y^2 = b^2$. Wtedy $(ab)^2 = (x^2 + y^2)(x^2 - y^2) = x^4 - y^4$, co przeczy twierdzeniu 17.36. □

Zadanie 17.38. Udowodnij twierdzenie Fermata, które głosi, że nie istnieje trójkąt prostokątny o bokach, których długości są liczbami naturalnymi i o polu, które jest kwadratem liczby naturalnej.

Zadanie 17.39. Udowodnij twierdzenie Eulera, które głosi, że nie istnieje trójkąt prostokątny o bokach i środkowych, których długości są liczbami naturalnymi.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 18

Ułamki łańcuchowe

18.1 Podstawy teoretyczne

Ułamki łańcuchowe początkowo były używane głównie do rozwiązywania równań diofantycznych, w szczególności równania Pella. W XX wieku stały się one bardziej powszechne w innych działach matematyki. Na przykład Robert M. Corless w artykule [8] z 1992 roku przedstawia związek między teorią chaosu a ułamkami łańcuchowymi. Są one obecnie wykorzystywane w algorytmach komputerowych do obliczania wymiernych przybliżeń liczb rzeczywistych. Dodatkowe informacje o ułamkach łańcuchowych można znaleźć na przykład w publikacjach [6] i [21].

Niech $(a_0, a_1, a_2, \ldots)$ będzie ciągiem liczb rzeczywistych takim, że $a_k \geqslant 1$ dla każdego $k = 1, 2, \ldots$. Definiujemy ciąg $(\langle a_0, \ldots, a_n \rangle)_{n=0}^{\infty}$ przyjmując, że $\langle a_0 \rangle = a_0$ oraz:

$$\langle a_0, a_1, \ldots, a_n \rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n \rangle} \quad \text{dla} \quad n = 1, 2, \ldots. \tag{18.1}$$

Przykład 18.1. Ze wzoru (18.1) kolejno uzyskujemy, że

$$\langle a_0, a_1 \rangle = a_0 + \frac{1}{a_1},$$

$$\langle a_0, a_1, a_2 \rangle = a_0 + \frac{1}{\langle a_1, a_2 \rangle} = a_0 + \frac{1}{a_1 + \frac{1}{a_2}},$$

$$\langle a_0, a_1, a_2, a_3\rangle = a_0 + \frac{1}{\langle a_1, a_2, a_3\rangle} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}}.$$

Lemat 18.2. *Niech n będzie liczbą naturalną i niech $a_0, a_1, \ldots, a_n \in \mathbb{R}$, przy czym $a_k \geqslant 1$ dla każdego $k = 1, 2, \ldots, n$. Wówczas:*

(i) $\langle a_1, a_2, \ldots, a_n\rangle \geqslant 1$,

(ii) jeśli $n > 1$ lub $n = 1$ i $a_1 > 1$, to

$$\langle a_1, a_2, \ldots, a_n\rangle > 1 \text{ oraz } a_0 < \langle a_0, a_1, \ldots, a_n\rangle < a_0 + 1.$$

Dowód. (i). Indukcja względem n przy dowolnych liczbach rzeczywistych $a_0, a_1, \ldots, a_n$ takich, że $a_k \geqslant 1$ dla każdego $k = 1, 2, \ldots, n$. Dla $n = 1$ z (18.1), $\langle a_1\rangle = a_1 \geqslant 1$. Załóżmy, że teza zachodzi dla pewnego $n \in \mathbb{N}$ i niech $a_0, a_1, \ldots, a_n, a_{n+1} \in \mathbb{R}$ będą takie, że $a_k \geqslant 1$ dla każdego $k = 1, \ldots, n, n+1$. Wtedy na mocy (18.1), $\langle a_1, a_2, \ldots, a_n, a_{n+1}\rangle = a_1 + \frac{1}{\langle a_2, \ldots, a_{n+1}\rangle}$. Ponadto $a_1 \geqslant 1$ i z założenia indukcyjnego mamy, że $\langle a_2, \ldots, a_{n+1}\rangle > 0$, więc $\langle a_1, \ldots, a_n, a_{n+1}\rangle \geqslant 1$.

(ii). Jeśli $a_1 > 1$, to na mocy (18.1), $\langle a_1\rangle = a_1 > 1$. Jeśli zaś $n > 1$, to z (i) oraz z (18.1), $\langle a_1, a_2, \ldots, a_n\rangle = a_1 + \frac{1}{\langle a_2, \ldots, a_n\rangle} > a_1 \geqslant 1$, skąd $\langle a_1, a_2, \ldots, a_n\rangle > 1$. Na mocy (18.1), $\langle a_0, a_1, \ldots, a_n\rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n\rangle}$, więc skoro $n > 1$ lub $n = 1$ i $a_1 > 1$, to $a_0 < \langle a_0, a_1, \ldots, a_n\rangle < a_0 + 1$. □

Pokażemy, że dla dowolnych $m, n \in \mathbb{N}$ i dla dowolnego $a_0 \in \mathbb{R}$ i dla dowolnych liczb rzeczywistych $a_1, a_2, \ldots, a_{n+m} \geqslant 1$ zachodzi wzór:

$$\langle a_0, \ldots, a_n, \ldots, a_{n+m}\rangle = \langle a_0, \ldots, a_{n-1}, \langle a_n, \ldots, a_{n+m}\rangle\rangle. \tag{18.2}$$

Na mocy (18.1) wzór (18.2) zachodzi dla $n = 1$ przy dowolnym $m \in \mathbb{N}$. Przypuśćmy, że wzór (18.2) zachodzi dla pewnego naturalnego n przy dowolnym $m \in \mathbb{N}$. Wtedy dla dowolnego $m \in \mathbb{N}$ na mocy (18.1) mamy, że $\langle a_0, a_1, \ldots, a_{n+1+m}\rangle = a_0 + \frac{1}{\langle a_1, a_2, \ldots, a_{n+1+m}\rangle}$ i z założenia indukcyjnego $\langle a_1, a_2, \ldots, a_{n+1+m}\rangle = \langle a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+1+m}\rangle\rangle$, więc stąd i na mocy (18.1):

$$\langle a_0, a_1, \ldots, a_{n+1+m}\rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+1+m}\rangle\rangle} =$$

$$= \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+1+m} \rangle \rangle,$$

co oznacza, że wzór (18.2) zachodzi też dla liczby $n+1$. Wobec tego na mocy zasady indukcji matematycznej wzór (18.2) zachodzi dla dowolnych $n, m \in \mathbb{N}$.

Stosując wzór (18.2) dla $m = 1$ uzyskujemy następującą zależność:

$$\langle a_0, a_1, \ldots, a_{n-1}, a_n, a_{n+1} \rangle = \left\langle a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}} \right\rangle. \quad (18.3)$$

Lemat 18.3. *Niech (b_n) będzie zbieżnym ciągiem liczb rzeczywistych i $b_n \geqslant 1$ dla każdego $n \in \mathbb{N}$. Niech $k \in \mathbb{N}_0$ i niech $a_0, a_1, \ldots, a_k \in \mathbb{R}$, przy czym $a_i \geqslant 1$ dla $i = 1, 2, \ldots, k$. Wówczas zachodzi wzór:*

$$\lim_{n\to\infty} \langle a_0, a_1, \ldots, a_k, b_n \rangle = \langle a_0, a_1, \ldots, a_k, \lim_{n\to\infty} b_n \rangle. \quad (18.4)$$

Dowód. Ponieważ $b_n \geqslant 1$ dla każdego $n \in \mathbb{N}$ i ciąg (b_n) jest zbieżny, więc $b = \lim\limits_{n\to\infty} b_n \geqslant 1$ i $\langle a_0, a_1, \ldots, a_k, b \rangle$ jest dobrze zdefiniowane. Wzór (18.4) udowodnimy przez indukcję względem k. Dla $k = 0$, $\langle a_0, b_n \rangle = a_0 + \frac{1}{b_n}$, więc z arytmetycznych twierdzeń o granicy ciągu uzyskujemy, że $\lim\limits_{n\to\infty} \langle a_0, b_n \rangle = \lim\limits_{n\to\infty} \left(a_0 + \frac{1}{b_n} \right) = a_0 + \frac{1}{b} = \langle a_0, b \rangle$. Przypuśćmy teraz, że teza zachodzi dla pewnego $k \in \mathbb{N}_0$. Wtedy dla $k+1$ na mocy wzoru (18.3) mamy, że $\langle a_0, a_1, \ldots, a_k, a_{k+1}, b_n \rangle = \langle a_0, a_1, \ldots, a_k, \langle a_{k+1}, b_n \rangle \rangle$. Ponadto $\langle a_{k+1}, b_n \rangle \geqslant 1$ dla $n \in \mathbb{N}$ i jak pokazaliśmy $\lim\limits_{n\to\infty} \langle a_{k+1}, b_n \rangle = \langle a_{k+1}, b \rangle \geqslant 1$, więc stąd i z założenia indukcyjnego otrzymujemy, że $\lim\limits_{n\to\infty} \langle a_0, \ldots, a_{k+1}, b_n \rangle = \langle a_0, \ldots, a_k, \langle a_{k+1}, b \rangle \rangle = \langle a_0, \ldots, a_k, a_{k+1}, b \rangle$ na mocy (18.3). □

Niech $x_0, x_1, x_2, \ldots$ będą niezależnymi zmiennymi. Definiujemy rekurencyjnie dwa ciągi wielomianów $(p_n)_{n=0}^{\infty}$ i $(q_n)_{n=0}^{\infty}$ przy pomocy formuł:

$$p_0 = x_0, \quad p_1 = x_0 x_1 + 1, \quad q_0 = 1, \quad q_1 = x_1 \quad (18.5)$$

$$\begin{cases} p_{n+1} = p_n x_{n+1} + p_{n-1} & \text{dla } n = 1, 2, \ldots \\ q_{n+1} = q_n x_{n+1} + q_{n-1} & \text{dla } n = 1, 2, \ldots \end{cases} \quad (18.6)$$

Stwierdzenie 18.4. *Dla każdego $n \in \mathbb{N}_0$, p_n i q_n są wielomianami o współczynnikach całkowitych zmiennych $x_0, x_1, \ldots, x_n$.*

Dowód. Dla $n = 0$ i dla $n = 1$ teza zachodzi. Przypuśćmy, że $n \geqslant 2$ jest liczbą naturalną taką, że teza zachodzi dla każdego $k = 0, 1, \ldots, n-1$. Wtedy p_{n-1} i q_{n-1} są wielomianami zmiennych $x_0, x_1, \ldots, x_{n-1}$ o współczynnikach całkowitych oraz p_{n-2} i q_{n-2} też są wielomianami o współczynnikach całkowitych zmiennych $x_0, x_1, \ldots, x_{n-2}$. Zatem na mocy (18.6), p_n i q_n są wielomianami o współczynnikach całkowitych zmiennych $x_0, x_1, \ldots, n$. Stąd na mocy zasady indukcji matematycznej mamy tezę. □

Stwierdzenie 18.5. *Dla każdego naturalnego n zachodzi wzór:*

$$p_{n-1} \cdot q_n - q_{n-1} \cdot p_n = (-1)^n. \tag{18.7}$$

Dowód. Zastosujemy indukcję względem $n \in \mathbb{N}$. Dla $n = 1$ teza zachodzi, bo $p_0 \cdot q_1 - q_0 \cdot p_1 = x_0 x_1 - 1 \cdot (x_0 x_1 + 1) = -1 = (-1)^1$. Przypuśćmy, że wzór (18.7) zachodzi dla pewnego naturalnego n. Wtedy z (18.6),

$$p_n \cdot q_{n+1} - q_n \cdot p_{n+1} =$$

$$= p_n \cdot (q_n x_{n+1} + q_{n-1}) - q_n \cdot (p_n x_{n+1} + p_{n-1}) =$$

$$= p_n q_n x_{n+1} + p_n q_{n-1} - q_n p_n x_{n+1} - q_n p_{n-1} = -(p_{n-1} \cdot q_n - q_{n-1} \cdot p_n) =$$

$$= (-1) \cdot (-1)^n = (-1)^{n+1},$$

czyli wtedy wzór (18.7) zachodzi dla liczby $n + 1$. Zatem na mocy zasady indukcji matematycznej mamy tezę. □

Twierdzenie 18.6. *Niech $n \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n \in \mathbb{R}$ i $a_k \geqslant 1$ dla każdego $k = 1, 2, \ldots, n$, gdy $n \geqslant 1$. Wówczas*

$$\langle a_0, a_1, \ldots, a_n \rangle = \frac{p_n(a_0, a_1, \ldots, a_n)}{q_n(a_0, a_1, \ldots, a_n)}. \tag{18.8}$$

Dowód. Zastosujemy indukcję względem $n \in \mathbb{N}_0$. Ponieważ na mocy wzoru (18.5) jest $\frac{p_0(a_0)}{q_0(a_0)} = \frac{a_0}{1} = a_0 = \langle a_0 \rangle$, $\frac{p_1(a_0,a_1)}{q_1(a_0,a_1)} =$

$= \frac{a_0a_1+1}{a_1} = a_0 + \frac{1}{a_1} = \langle a_0, a_1\rangle$ oraz $\frac{p_2(a_0,a_1,a_2)}{q_2(a_0,a_1,a_2)} = \frac{(a_0a_1+1)a_2+a_0}{a_1a_2+1} = \frac{a_0(a_1a_2+1)+a_2}{a_1a_2+1} = a_0 + \frac{a_2}{a_1a_2+1} = a_0 + \frac{1}{a_1+\frac{1}{a_2}} = \langle a_0, a_1, a_2\rangle$, więc wzór (18.8) zachodzi dla $n = 0, 1, 2$. Niech teraz wzór (18.8) zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ przy dowolnych $a_0, a_1, \ldots, a_n$. Weźmy dowolne liczby rzeczywiste $a_0, a_1, \ldots, a_n, a_{n+1}$ takie, że $a_k \geqslant 1$ dla $k = 1, \ldots, n, n+1$. Wtedy ze wzoru (18.3),

$$\langle a_0, a_1, \ldots, a_n, a_{n+1}\rangle = \left\langle a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right\rangle.$$

Zatem na mocy założenia indukcyjnego

$$\langle a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\rangle = \frac{p_n(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}})}{q_n(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}})}.$$

Ponadto z (18.6),

$$p_n\left(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right) =$$

$$= p_{n-1}(a_0, \ldots, a_{n-1})\left(a_n + \frac{1}{a_{n+1}}\right) + p_{n-2}(a_0, \ldots, a_{n-2}),$$

więc na mocy (18.6),

$$p_n\left(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right) =$$

$$= p_{n-1}(a_0, \ldots, a_{n-1})a_n + p_{n-2}(a_0, \ldots, a_{n-2}) +$$

$$+ \frac{1}{a_{n+1}} p_{n-1}(a_0, \ldots, a_{n-1}) =$$

$$= p_n(a_0, \ldots, a_n) + \frac{1}{a_{n+1}} p_{n-1}(a_0, \ldots, a_{n-1}) =$$

$$= \frac{1}{a_{n+1}}\left(p_n(a_0, \ldots, a_n)a_{n+1} + p_{n-1}(a_0, \ldots, a_{n-1})\right) =$$

$$= \frac{1}{a_{n+1}} p_{n+1}\left(a_0, \ldots, a_n, a_{n+1}\right).$$

Analogicznie pokazujemy, że

$$q_n(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}) = \frac{1}{a_{n+1}} q_{n+1}(a_0, \ldots, a_n, a_{n+1}).$$

Zatem po skróceniu przez $\frac{1}{a_{n+1}}$ uzyskujemy, że

$$\langle a_0, a_1, \ldots, a_n, a_{n+1}\rangle = \frac{p_{n+1}(a_0, a_1, \ldots, a_n, a_{n+1})}{q_{n+1}(a_0, a_1, \ldots, a_n, a_{n+1})},$$

co oznacza, że wzór (18.8) zachodzi dla liczby $n+1$. Kończy to więc nasz dowód. □

Twierdzenie 18.7. *Niech $(a_0, a_1, a_2, \ldots)$ będzie ciągiem takim, że $a_k \geqslant 1$ dla $k \in \mathbb{N}$. Niech $P_n = p_n(a_0, \ldots, a_n)$ i $Q_n = q_n(a_0, \ldots, a_n)$ i $R_n = \frac{P_n}{Q_n}$ dla każdego $n \in \mathbb{N}_0$. Wówczas:*

(i) $P_0 = a_0$, $P_1 = a_0 a_1 + 1$, $Q_0 = 1$ oraz $Q_1 = a_1$,

(ii) $P_{n+1} = P_n a_{n+1} + P_{n-1}$ oraz $Q_{n+1} = Q_n a_{n+1} + Q_{n-1}$ dla $n = 1, 2, \ldots$,

(iii) $P_{n-1}Q_n - Q_{n-1}P_n = (-1)^n$ dla każdego $n \in \mathbb{N}$,

(iv) $\langle a_0, a_1, \ldots, a_n\rangle = \frac{P_n}{Q_n} = R_n$ dla $n = 0, 1, 2, \ldots$,

(v) $Q_0 \leqslant Q_1 < Q_2 < Q_3 < \ldots$ i $Q_n \geqslant n$ dla $n = 1, 2, \ldots$,

(vi) $R_k - R_{k+1} = \frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{(-1)^{k+1}}{Q_k Q_{k+1}}$ dla każdego $k \in \mathbb{N}_0$,

(vii) $R_0 < R_2 < R_4 < \ldots$ oraz $R_1 > R_3 > R_5 > \ldots$,

(viii) $R_{2k} < R_{2l+1}$ dla dowolnych $k, l \in \mathbb{N}_0$,

(ix) $\lim\limits_{n\to\infty} R_n = \sup\{R_0, R_2, \ldots\} = \inf\{R_1, R_3, \ldots\}$.

Dowód. Podpunkt (i) wynika z (18.5), a z (18.6) wynika od razu (ii). Z (18.7) uzyskujemy podpunkt (iii). Natomiast (iv) jest konsekwencją twierdzenia 18.6. (v). Z (i), $Q_0 = 1$ oraz $Q_1 = a_1 \geqslant 1$. Natomiast z (ii), $Q_2 = a_2 Q_1 + Q_0 = a_2 a_1 + 1 \geqslant 2$, bo $a_1 \geqslant 1$ i $a_2 \geqslant 1$. Weźmy dowolne $n \in \mathbb{N}$ takie, że $n \geqslant 2$ i $Q_{n-1} \geqslant n-1$ oraz $Q_n \geqslant n$. Wtedy z (ii), $Q_{n+1} = a_{n+1}Q_n + Q_{n-1} \geqslant Q_n + Q_{n-1} \geqslant n + (n-1) \geqslant n+1$, bo $a_{n+1} \geqslant 1$ i $n \geqslant 2$. Zatem przez indukcje mamy, że $Q_n \geqslant n$ dla $n = 1, 2, \ldots$. Dalej, z

(i) mamy, że $Q_1 = a_1 \geqslant 1 = Q_0$. Natomiast z (ii) dla dowolnego $n \in \mathbb{N}$ uzyskujemy, że $Q_{n+1} = a_{n+1}Q_n + Q_{n-1}$. Jak pokazaliśmy, $Q_{n-1} \geqslant 1$ i na mocy założenia $a_{n+1} \geqslant 1$, więc $Q_{n+1} \geqslant Q_n + 1$, skąd $Q_{n+1} > Q_n$. Zatem $Q_0 \leqslant Q_1 < Q_2 < Q_3 < \ldots$.

(vi). Z (ii) mamy, że dla $k \in \mathbb{N}_0$: $\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{P_kQ_{k+1} - Q_kP_{k+1}}{Q_kQ_{k+1}} = \frac{(-1)^{k+1}}{Q_kQ_{k+1}}$. Dla dowodu (vii) weźmy dowolne $k \in \mathbb{N}_0$. Zauważmy, że $R_k - R_{k+2} = (R_k - R_{k+1}) + (R_{k+1} - R_{k+2})$, więc na mocy (vi), $R_k - R_{k+2} = \frac{(-1)^{k+1}}{Q_kQ_{k+1}} + \frac{(-1)^{k+2}}{Q_{k+1}Q_{k+2}}$. Zatem $R_k - R_{k+2} = (-1)^{k+1} \cdot \frac{Q_{k+2} - Q_k}{Q_kQ_{k+1}Q_{k+2}}$. Na mocy (v), $Q_{k+2} - Q_k > 0$ oraz $Q_k, Q_{k+1}, Q_{k+2} > 0$, więc dla parzystego k będziemy mieli, że $R_k - R_{k+2} < 0$, zaś dla nieparzystego k: $R_k - R_{k+2} > 0$. Stąd $R_0 < R_2 < R_4 < \ldots$ oraz $R_1 > R_3 > R_5 > \ldots$.

$(viii)$. Weźmy dowolne $k, l \in \mathbb{N}_0$. Na mocy (vi) i (v), $R_{2k} - R_{2k+1} < 0$, czyli $R_{2k} < R_{2k+1}$. Jeśli $k \leqslant l$, to z (vii), $R_{2k+1} \leqslant R_{2l+1}$, więc wtedy $R_{2k} < R_{2l+1}$. W przeciwnym przypadku, czyli gdy $k > l$, na mocy (vii), $R_{2k} < R_{2l}$. Jak pokazaliśmy, $R_{2l} < R_{2l+1}$, więc też $R_{2k} < R_{2l+1}$.

(ix). Weźmy dowolne $l \in \mathbb{N}_0$. Z (vii) i $(viii)$ ciąg $(R_{2k})_{k=0}^{\infty}$ jest rosnący i ograniczony z góry przez liczbę R_{2l+3}. Zatem z twierdzenia o ciągu monotonicznym ten ciąg posiada granicę α, przy czym $\alpha \leqslant R_{2l+3}$, skąd na mocy (vii), $\alpha < R_{2l+1}$ oraz α jest kresem górnym zbioru $\{R_{2k} : k \in \mathbb{N}_0\}$. Wobec tego na mocy (vii), $R_{2k} < \alpha$ dla każdego $k \in \mathbb{N}_0$.

Weźmy teraz dowolne $k \in \mathbb{N}_0$. Z $(viii)$, i (vii) ciąg $(R_{2l+1})_{l=0}^{\infty}$ jest malejący i ograniczony z dołu przez liczbę R_{2k+2}. Zatem z twierdzenia o ciągu monotonicznym ten ciąg posiada granicę β, przy czym $\beta \geqslant R_{2k+2}$, skąd na mocy (vii), $\beta > R_{2k}$ oraz β jest kresem dolnym zbioru $\{R_{2l+1} : k \in \mathbb{N}_0\}$. Wobec tego na mocy (vii), $\beta < R_{2l+1}$ dla każdego $l \in \mathbb{N}_0$.

Stąd dla każdego $k \in \mathbb{N}$, $\alpha, \beta \in (R_{2k}, R_{2k+1})$, więc $|\alpha - \beta| < R_{2k+1} - R_{2k} = \frac{1}{Q_{2k}Q_{2k+1}}$ na mocy (vi). Zatem na mocy (v), $|\alpha - \beta| < \frac{1}{2k(2k+1)} < \frac{1}{k}$. Z dowolności k wynika zatem, że $\alpha = \beta$. Weźmy dowolne $\varepsilon > 0$. Wtedy istnieje $n_0 \in \mathbb{N}$ takie, że $n_0 > \frac{1}{\varepsilon}$. Niech $n \in \mathbb{N}$ i $n \geqslant n_0$. Wtedy $n > \frac{1}{\varepsilon}$, więc $\frac{1}{n} < \varepsilon$. Ponadto, jedna z liczb n i $n+1$ jest parzysta, a druga jest nieparzysta, więc α należy do przedziału otwartego o końcach R_n

i R_{n+1}. Wobec tego $|\alpha - R_n| < |R_n - R_{n+1}| = \frac{1}{Q_n Q_{n+1}} \leqslant \frac{1}{n(n+1)} < \frac{1}{n}$ na mocy (v) i (vi). Stąd $|\alpha - R_n| < \varepsilon$ i wobec tego $\lim\limits_{n\to\infty} R_n = \alpha$. □

18.2 Skończone ułamki łańcuchowe

Definicja 18.8. Skończonym ułamkiem łańcuchowym nazywamy liczbę postaci $\langle a_0, a_1, \ldots, a_n\rangle$, gdzie $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{N}$ i $a_n > 1$, o ile $n > 0$.

Uwaga 18.9. Warto dodać, że u niektórych autorów (na przykład [27]) w definicji skończonego ułamka łańcuchowego dopuszcza się przypadki, gdy $a_n = 1$. My postępujemy inaczej w celu uzyskania jednoznaczności zapisu liczby wymiernej w postaci skończonego ułamka łańcuchowego (patrz twierdzenie 18.15). Ponadto, wzorujemy się też na monografii [7].

Przykład 18.10. Zauważmy, że $\langle 1, 2, 1\rangle = \langle 1, 3\rangle$ i $\langle 1, 2, 1\rangle$ nie jest skończonym ułamkiem łańcuchowym, zaś $\langle 1, 3\rangle$ jest skończonym ułamkiem łańcuchowym.

Z twierdzenia 18.7 i ze stwierdzenia 18.4 otrzymujemy od razu następujące

Twierdzenie 18.11. *Niech $n \in \mathbb{N}_0$, niech $a_0 \in \mathbb{Z}$ i niech $a_k \in \mathbb{N}$ dla $k = 1, 2, \ldots, n$. Niech $P_k = p_k(a_0, \ldots, a_k)$ i $Q_k = q_k(a_0, \ldots, a_k)$ oraz niech $R_k = \frac{P_k}{Q_k}$ dla każdego $k = 0, 1, \ldots, n$. Wówczas:*

(i) $P_k \in \mathbb{Z}$, $Q_k \in \mathbb{N}$ i $\mathrm{NWD}(P_k, Q_k) = 1$ dla każdego $k = 0, 1, \ldots, n$,

(ii) $P_0 = a_0$, $P_1 = a_0 a_1 + 1$, $Q_0 = 1$ oraz $Q_1 = a_1$,

(iii) $P_{k+1} = P_k a_{k+1} + P_{k-1}$ i $Q_{k+1} = Q_k a_{k+1} + Q_{k-1}$ dla każdego $k = 1, 2, \ldots, n-1$,

(iv) $P_{k-1}Q_k - Q_{k-1}P_k = (-1)^k$ dla każdego $k = 1, 2, \ldots, n$,

(v) $\langle a_0, a_1, \ldots, a_k\rangle = \frac{P_k}{Q_k} = R_k$ dla $k = 0, 1, 2, \ldots, n$.

W szczególności każdy skończony ułamek łańcuchowy jest liczbą wymierną.

Przykład 18.12. Zastosujemy twierdzenie 18.11 do obliczenia skończonego ułamka łańcuchowego $\langle 1, 2, 3, 4, 5, 6\rangle$. Mamy tutaj $n = 5$. Budujemy tabelkę:

k	0	1	2	3	4	5
a_k	1	2	3	4	5	6
P_k	1	3	10	43	225	1393
Q_k	1	2	7	30	157	972

Wobec tego $\langle 1,2,3,4,5,6\rangle = \frac{1393}{972}$. Zauważmy, że $P_4Q_5 - Q_5P_4 = (-1)^5$, więc $225 \cdot 972 - 157 \cdot 1393 = -1$, skąd $1393 \cdot 157 - 972 \cdot 225 = 1$. Stąd para $(157, -225)$ jest rozwiązaniem szczególnym diofantycznego równania liniowego $1393x + 972y = 1$.

Zauważmy też, że z lematu 18.2 uzyskujemy od razu następujący

Lemat 18.13. *Część całkowita dowolnego skończonego ułamka łańcuchowego $\langle a_0, \ldots, a_n\rangle$ jest równa a_0.* □

Twierdzenie 18.14. *Skończone ułamki łańcuchowe $\langle a_0, \ldots, a_n\rangle$ oraz $\langle b_0, \ldots, b_m\rangle$ są równe wtedy i tylko wtedy, gdy $n = m$ oraz $a_k = b_k$ dla każdego $k = 0, 1, \ldots, n$.*

Dowód. $\Rightarrow$. Załóżmy, że skończone ułamki łańcuchowe $\langle b_0, b_1, \ldots, b_m\rangle$ i $\langle a_0\rangle$ są równe. Wtedy ich części całkowite też są równe. Zatem na mocy lematu 18.13, $a_0 = b_0$. Jeśli $m > 0$, to $b_0 = b_0 + \frac{1}{\langle b_1, \ldots, b_m\rangle}$, co prowadzi do sprzeczności, bo $\langle b_1, \ldots, b_m\rangle \geqslant 1$. Zatem $m = 0$ i teza zachodzi dla $n = 0$.

Przypuśćmy, że teza zachodzi dla pewnego $n \in \mathbb{N}_0$ i niech skończone ułamki łańcuchowe $\langle a_0, a_1, \ldots, a_{n+1}\rangle$ i $\langle b_0, b_1, \ldots, b_m\rangle$ będą równe. Wtedy ich części całkowite też są równe, więc z lematu 18.13, $a_0 = b_0$. Ponieważ $n > 0$, więc z pierwszej części dowodu $m > 0$. Stąd na mocy (18.1), $a_0 + \frac{1}{\langle a_1, \ldots, a_{n+1}\rangle} = a_0 + \frac{1}{\langle b_1, \ldots, b_m\rangle}$. Zatem $\langle a_1, \ldots, a_{n+1}\rangle = \langle b_1, \ldots, b_m\rangle$ i z założenia indukcyjnego $n = m - 1$ oraz $a_k = b_k$ dla każdego $k = 1, 2, \ldots, n+1$. Wobec tego $n + 1 = m$ i $a_k = b_k$ dla każdego $k = 0, 1, \ldots, n+1$. Stąd na mocy zasady indukcji matematycznej mamy tezę.

Implikacja $\Leftarrow$ jest oczywista. □

Twierdzenie 18.15. *Każda liczba wymierna jest równa dokładnie jednemu skończonemu ułamkowi łańcuchowemu. Dokładniej, jeśli $a \in$*

$\in \mathbb{Z}$ *i* $b \in \mathbb{N}$ *oraz* $q_0, q_1, \ldots, q_n$ *są wszystkimi niepełnymi ilorazami w algorytmie Euklidesa wyznaczania* $\mathrm{NWD}(a, b)$*, przy czym* $a = q_0 b + r_0$*, gdzie* $r_0 \in \{0, 1, \ldots, b-1\}$*, to* $\frac{a}{b} = \langle q_0, q_1, \ldots, q_n \rangle$.

Dowód. Jednoznaczność zapisu liczby wymiernej w postaci skończonego ułamka łańcuchowego wynika z twierdzenia 18.14. Wzór $\frac{a}{b} = \langle q_0, q_1, \ldots, q_n \rangle$ udowodnimy przez indukcję ze względu na n. Zauważmy najpierw, że jeśli $n \geqslant 1$, to $q_n > 1$, bo w algorytmie Euklidesa q_n jest ilorazem większej liczby naturalnej przez mniejszą od niej liczbę naturalną (która jest ostatnią niezerową resztą). Dla $n = 0$, $r_0 = 0$, więc $\frac{a}{b} = q_0 = \langle q_0 \rangle$. Przypuśćmy, że teza zachodzi dla pewnego całkowitego $n \geqslant 0$ (przy dowolnych a i b). Weźmy dowolne $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ takie, że $q_0, q_1, \ldots, q_n, q_{n+1}$ są wszystkimi niepełnymi ilorazami w algorytmie Euklidesa wyznaczania $\mathrm{NWD}(a, b)$, przy czym $a = q_0 b + r_0$, gdzie $r_0 \in \{0, 1, \ldots, b-1\}$. Wtedy $r_0 > 0$ oraz $\frac{a}{b} = q_0 + \frac{r_0}{b} = q_0 + \frac{1}{\frac{b}{r_0}}$. Ponadto $q_1, \ldots, q_n, q_{n+1}$ są wszystkimi niepełnymi ilorazami w algorytmie Euklidesa obliczania $\mathrm{NWD}(b, r_0)$ oraz $b = q_1 r_0 + r_1$ dla pewnego $r_1 \in \{0, 1, \ldots, r_0 - 1\}$, więc z założenia indukcyjnego $\frac{b}{r_0} = \langle q_1, \ldots, q_n, q_{n+1} \rangle$. Stąd na mocy (18.1), $\frac{a}{b} = \langle q_0, q_1, \ldots, q_n, q_{n+1} \rangle$. □

Wniosek 18.16. *Dla każdej liczby wymiernej* q *istnieją: nieparzysta liczba naturalna* m*, parzysta nieujemna liczba całkowita* n*, liczby całkowite* a_0, b_0*, oraz liczby naturalne* $a_1, \ldots, a_n, b_1, \ldots, b_m$ *takie, że* $q = \langle a_0, \ldots, a_n \rangle$ *i* $q = \langle b_0, b_1, \ldots, b_m \rangle$.

Dowód. Jeżeli $q \in \mathbb{Z}$, to $q = \langle q \rangle$ i $q = \langle q - 1, 1 \rangle$. Niech dalej $q \notin \mathbb{Z}$. Wtedy na mocy twierdzenia 18.15 istnieje skończony ułamek łańcuchowy $\langle c_0, c_1, \ldots, c_p \rangle$ taki, że $q = \langle c_0, c_1, \ldots, c_p \rangle$, przy czym $p \in \mathbb{N}$. Stąd $c_0 \in \mathbb{Z}$ oraz $c_1, \ldots, c_p \in \mathbb{N}$ i $c_p > 1$. Zatem $c_p - 1 \in \mathbb{N}$ i ze wzoru (18.3), $q = \langle c_0, c_1, \ldots, c_p - 1, 1 \rangle$. Ponadto, $p \in \mathbb{N}$, więc p i $p + 1$ jako kolejne liczby naturalne są różnej parzystości, co kończy dowód. □

Przykład 18.17. Zapiszemy $\frac{41}{18}$ w postaci skończonego ułamka łańcuchowego. W tym celu wyznaczamy najpierw kolejne dzielenia z resztą

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

w algorytmie Euklidesa obliczania NWD$(41, 18)$:

$$\begin{aligned} 41 &= 2 \cdot 18 + 5 \\ 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned} \quad . \tag{18.9}$$

Zatem na mocy twierdzenia 18.15, $\frac{41}{18} = \langle 2, 3, 1, 1, 2\rangle$. Ponadto mamy, że $18 = 0 \cdot 41 + 18$, więc stąd $\frac{18}{41} = \langle 0, 2, 3, 1, 1, 2\rangle$.

Zauważmy, że twierdzenie 18.11 możemy zastosować do znalezienia rozwiązania w liczbach całkowitych x i y równania $41x + 18y = 1$. Mamy tutaj $n = 4$. Budujemy tabelkę:

k	0	1	2	3	4
a_k	2	3	1	1	2
P_k	2	7	9	16	41
Q_k	1	3	4	7	18

,

z której odczytujemy, że $P_3 = 16$, $P_4 = 41$, $Q_3 = 7$ i $Q_4 = 18$. Dodatkowo $P_3Q_4 - Q_3P_4 = (-1)^4 = 1$, więc $41 \cdot (-7) + 18 \cdot 16 = 1$. Zatem para $(-7, 16)$ jest szczególnym rozwiązaniem diofantycznego równania liniowego $41x + 18y = 1$.

Przykład 18.18. Twierdzenie 18.11 można też stosować do skracania ułamków. Pokażemy to na przykładzie ułamka $\frac{84281}{86147}$. Wyznaczamy najpierw kolejne dzielenia z resztą w algorytmie Euklidesa obliczania NWD$(84281, 86147)$:

$$\begin{aligned} 84281 &= 0 \cdot 86147 + 84281 \\ 86147 &= 1 \cdot 84281 + 1866 \\ 84281 &= 45 \cdot 1866 + 311 \\ 1866 &= 6 \cdot 311 \end{aligned} \quad . \tag{18.10}$$

Zatem na mocy twierdzenia 18.15, $\frac{84281}{86147} = \langle 0, 1, 45, 6\rangle$. Budujemy tabelkę:

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

k	0	1	2	3
a_k	0	1	45	6
P_k	0	1	45	271
Q_k	1	1	46	277

,

z której wynika, że $\frac{84281}{86147} = \frac{271}{277}$ i na mocy twierdzenia 18.15 ułamek $\frac{271}{277}$ jest nieskracalny.

18.3 Nieskończone ułamki łańcuchowe

Z twierdzenia 18.7 wynika od razu, że jeżeli $(a_n)_{n=0}^{\infty}$ jest dowolnym ciągiem liczb całkowitych takim, że $a_k \geqslant 1$ dla wszystkich $k \in \mathbb{N}$, to ciąg $(\langle a_0, a_1, \ldots, a_n\rangle)_{n=0}^{\infty}$ jest zbieżny. Ma zatem sens następujące określenie.

Definicja 18.19. Niech $(a_n)_{n=0}^{\infty}$ będzie ciągiem liczb całkowitych takim, że $a_k \geqslant 1$ dla wszystkich $k \in \mathbb{N}$. Granicę ciągu

$$(\langle a_0, a_1, \ldots, a_n\rangle)_{n=0}^{\infty}$$

nazywamy **nieskończonym ułamkiem łańcuchowym** i oznaczamy symbolem $\langle a_0, a_1, a_2, \ldots\rangle$.

Z twierdzenia 18.7 i ze stwierdzenia 18.4 otrzymujemy od razu następujące

Twierdzenie 18.20. *Niech $\alpha = \langle a_0, a_1, \ldots\rangle$ będzie nieskończonym ułamkiem łańcuchowym, $P_k = p_k(a_0, \ldots, a_k)$ i $Q_k = q_k(a_0, \ldots, a_k)$ oraz $R_k = \frac{P_k}{Q_k}$ dla każdego $k = 0, 1, \ldots$. Wówczas:*
(i) $P_k \in \mathbb{Z}$, $Q_k \in \mathbb{N}$ i $\mathrm{NWD}(P_k, Q_k) = 1$ dla każdego $k = 0, 1, \ldots$,
(ii) $P_0 = a_0$, $P_1 = a_0a_1 + 1$, $Q_0 = 1$ oraz $Q_1 = a_1$,
(iii) $P_{k+1} = P_k a_{k+1} + P_{k-1}$ i $Q_{k+1} = Q_k a_{k+1} + Q_{k-1}$ dla $k \in \mathbb{N}$,
(iv) $P_{k-1}Q_k - Q_{k-1}P_k = (-1)^k$ dla każdego $k \in \mathbb{N}$,
(v) $\langle a_0, a_1, \ldots, a_k\rangle = \frac{P_k}{Q_k} = R_k$ dla $k = 0, 1, 2, \ldots$,
(vi) $Q_0 \leqslant Q_1 < Q_2 < Q_3 < \ldots$ i $Q_n \geqslant n$ dla $n = 1, 2, \ldots$,
(vii) $R_k - R_{k+1} = \frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{(-1)^{k+1}}{Q_kQ_{k+1}}$ dla każdego $k \in \mathbb{N}_0$,

(viii) $R_0 < R_2 < R_4 < \ldots$ *oraz* $R_1 > R_3 > R_5 > \ldots$,
(ix) $R_{2k} < R_{2l+1}$ *dla dowolnych* $k, l \in \mathbb{N}_0$,
(x) $\lim\limits_{n\to\infty} R_n = \alpha = \sup\{R_0, R_2, \ldots\} = \inf\{R_1, R_3, \ldots\}$.
W szczególności $R_{2k} < \alpha < R_{2l+1}$ *dla dowolnych* $k, l \in \mathbb{N}_0$.

Twierdzenie 18.21. *Niech* $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$ *będzie dowolnym nieskończonym ułamkiem łańcuchowym. Wtedy przy oznaczeniach twierdzenia 18.20:*
(i) $\lfloor\alpha\rfloor = a_0$,
(ii) $|\alpha - R_n| < \frac{1}{Q_n Q_{n+1}}$ *dla każdego* $n \in \mathbb{N}$,
(iii) α *jest liczbą niewymierną.*

Dowód. Na mocy twierdzenia 18.20, $a_0 = R_0 < \alpha < R_1 = a_0 + \frac{1}{a_1} \leqslant$ $\leqslant a_0 + 1$, skąd $\lfloor\alpha\rfloor = a_0$ oraz dla każdego $n \in \mathbb{N}$ liczba α leży w przedziale otwartym o końcach R_n i R_{n+1}. Stąd

$$|\alpha - R_n| < |R_n - R_{n+1}| = \frac{1}{Q_n Q_{n+1}}.$$

Pozostaje zatem udowodnić punkt *(iii)*. W tym celu załóżmy, że α jest liczbą wymierną. Wtedy istnieją względnie pierwsze liczby całkowite p i q takie, że $q > 0$ oraz $\alpha = \frac{p}{q}$. Z twierdzenia 18.20 *(vi)* istnieje liczba naturalna n taka, że $Q_n > q$. Ponadto $|\frac{p}{q} - \frac{P_n}{Q_n}| < \frac{1}{Q_n Q_{n+1}}$, więc po pomnożeniu przez qQ_n uzyskamy, że $|pQ_n - P_n q| < \frac{q}{Q_{n+1}} < 1$, bo $q < Q_n < Q_{n+1}$ na mocy twierdzenia 18.20 *(vi)*. Liczba $pQ_n - P_n q$ jest całkowita, więc stąd $pQ_n - P_n q = 0$, a zatem $\alpha = \frac{p}{q} = \frac{P_n}{Q_n} = R_n$, co przeczy twierdzeniu 18.20. Wobec tego liczba α jest niewymierna. □

Z twierdzeń 18.11 i 18.21 uzyskujemy od razu następujący

Wniosek 18.22. *Żaden nieskończony ułamek łańcuchowy nie jest równy żadnemu skończonemu ułamkowi łańcuchowemu.*

Stwierdzenie 18.23. *Dla każdego nieskończonego ułamka łańcuchowego* $\langle a_0, a_1, a_2, \ldots\rangle$ *i dla dowolnego* $n \in \mathbb{N}_0$ *zachodzi wzór:*

$$\langle a_0, a_1, a_2, \ldots\rangle = \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, a_{n+2}, \ldots\rangle\rangle. \tag{18.11}$$

Dowód. Weźmy dowolne $m \in \mathbb{N}$. Wtedy na mocy wzoru (18.2),

$$\langle a_0, a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+m}\rangle = \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+m}\rangle\rangle.$$

Z twierdzenia 18.20 mamy, że

$$\langle a_0, a_1, a_2, \ldots\rangle = \lim_{m\to\infty} \langle a_0, a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+m}\rangle$$

oraz

$$\langle a_{n+1}, a_{n+2}, a_{n+3}, \ldots\rangle = \lim_{m\to\infty} \langle a_{n+1}, a_{n+2}, \ldots, a_{n+m}\rangle.$$

Stąd i na mocy lematu 18.3 uzyskujemy, że

$$\langle a_0, a_1, a_2, \ldots\rangle = \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, a_{n+2}, \ldots\rangle\rangle.$$

□

Twierdzenie 18.24. *Nieskończone ułamki łańcuchowe* $\langle a_0, a_1 \ldots\rangle$ *i* $\langle b_0, b_1 \ldots\rangle$ *są równe wtedy i tylko wtedy, gdy* $a_i = b_i$ *dla każdego* $i \in \mathbb{N}_0$.

Dowód. Implikacja $\Leftarrow$ jest oczywista. Dla dowodu implikacji $\Rightarrow$ załóżmy, że nieskończone ułamki łańcuchowe $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$ i $\beta = \langle b_0, b_1, b_2, \ldots\rangle$ są równe. Wtedy $\lfloor\alpha\rfloor = \lfloor\beta\rfloor$, więc z twierdzenia 18.21 otrzymujemy, że $a_0 = b_0$. Przypuśćmy, że $i \in \mathbb{N}_0$ jest takie, że $a_j = b_j$ dla każdego $j = 0, 1, \ldots, i$. Uwzględniając też stwierdzenie 18.23 mamy stąd, że

$$\langle a_0, a_1, \ldots, a_i, \langle a_{i+1}, a_{i+2}, \ldots\rangle\rangle = \langle a_0, a_1, \ldots, a_i, \langle b_{i+1}, b_{i+2}, \ldots\rangle\rangle.$$

Oznaczmy $\gamma = \langle a_{i+1}, a_{i+2}, \ldots\rangle$ i $\delta = \langle b_{i+1}, b_{i+2}, \ldots\rangle$. Wtedy z twierdzenia 18.21 uzyskujemy, że $\gamma > a_{i+1} \geqslant 1$ i $\delta > b_{i+1} \geqslant 1$ oraz

$$\langle a_0, a_1, \ldots, a_i, \gamma\rangle = \langle a_0, a_1, \ldots, a_i, \delta\rangle.$$

Jeśli $i = 0$, to stąd $a_0 + \frac{1}{\gamma} = a_0 + \frac{1}{\delta}$, skąd $\gamma = \delta$, więc z pierwszego kroku dowodu $a_{i+1} = b_{i+1}$. Niech dalej $i \geqslant 1$. Wtedy z twierdzenia

18.7 mamy, że $\langle a_0, a_1, \ldots, a_i, \gamma\rangle = \frac{P_i\gamma+P_{i-1}}{Q_i\gamma+Q_{i-1}}$ oraz $\langle a_0, a_1, \ldots, a_i, \delta\rangle = \frac{P_i\delta+P_{i-1}}{Q_i\delta+Q_{i-1}}$. Zatem $\frac{P_i\gamma+P_{i-1}}{Q_i\gamma+Q_{i-1}} = \frac{P_i\delta+P_{i-1}}{Q_i\delta+Q_{i-1}}$, czyli

$$(P_i\gamma + P_{i-1})(Q_i\delta + Q_{i-1}) = (Q_i\gamma + Q_{i-1})(P_i\delta + P_{i-1}).$$

Stąd $(P_{i-1}Q_i - Q_{i-1}P_i)\delta = (P_{i-1}Q_i - Q_{i-1}P_i)\gamma$. Zatem na mocy twierdzenia 18.7, $(-1)^i\delta = (-1)^i\gamma$, czyli $\delta = \gamma$, więc z pierwszego kroku dowodu $a_{i+1} = b_{i+1}$.

Wobec tego przez indukcję wykazaliśmy, że $a_i = b_i$ dla każdego $i \in \mathbb{N}_0$. □

18.4 Rozwijanie liczby niewymiernej na ułamek łańcuchowy

Niech x będzie dowolną rzeczywistą liczbą niewymierną. Wtedy $\lfloor x\rfloor \leqslant \leqslant x < \lfloor x\rfloor + 1$ i $\lfloor x\rfloor \neq x$, więc $0 < x - \lfloor x\rfloor < 1$. Zatem $x_1 = \frac{1}{x-\lfloor x\rfloor} > 1$ i x_1 jest liczbą niewymierną oraz $x = \lfloor x\rfloor + \frac{1}{x_1}$, czyli $x = \langle\lfloor x\rfloor, x_1\rangle$. Analogicznie dalej, $x_2 = \frac{1}{x_1-\lfloor x_1\rfloor} > 1$ i x_2 jest liczbą niewymierną oraz $x_1 = \langle\lfloor x_1\rfloor, x_2\rangle$. Wobec tego na mocy (18.2), $x = \langle\lfloor x\rfloor, \lfloor x_1\rfloor, x_2\rangle$, przy czym $\lfloor x_1\rfloor \in \mathbb{N}$, bo $x_1 > 1$. Kontynuując ten proces widzimy, że istnieje ciąg $(x_n)_{n=0}^{\infty}$ liczb niewymiernych taki, że $x_0 = x$ oraz:

$$x_k > 1 \ \text{ i } \ x_{k+1} = \frac{1}{x_k - \lfloor x_k\rfloor} \quad \text{dla każdego } \ k \in \mathbb{N}, \tag{18.12}$$

przy czym na mocy (18.2) i prostej indukcji:

$$x = \langle\lfloor x\rfloor, \lfloor x_1\rfloor, \ldots, \lfloor x_n\rfloor, x_{n+1}\rangle \quad \text{dla każdego } \ n \in \mathbb{N}_0. \tag{18.13}$$

W szczególności

$$a_0 = \lfloor x\rfloor \in \mathbb{Z} \ \text{ oraz } \ a_n = \lfloor x_n\rfloor \in \mathbb{N} \ \text{ dla każdego } \ n \in \mathbb{N}. \tag{18.14}$$

Udowodnimy, że

$$x = \langle a_0, a_1, a_2, \ldots\rangle. \tag{18.15}$$

Niech $n \in \mathbb{N}$. Wtedy z (18.13) i (18.14) mamy, że $x = \langle a_0, \ldots, a_n, x_{n+1}\rangle$. Zatem na mocy twierdzenia 18.7 uzyskujemy, że

$$x = \frac{P_n x_{n+1} + P_{n-1}}{Q_n x_{n+1} + Q_{n-1}} \quad \text{oraz} \quad R_{n+1} = \frac{P_{n+1}}{Q_{n+1}} = \frac{P_n a_{n+1} + P_{n-1}}{Q_n a_{n+1} + Q_{n-1}}.$$

Wobec tego

$$x - R_{n+1} = \frac{P_n x_{n+1} + P_{n-1}}{Q_n x_{n+1} + Q_{n-1}} - \frac{P_n a_{n+1} + P_{n-1}}{Q_n a_{n+1} + Q_{n-1}} =$$

$$= \frac{(P_n x_{n+1} + P_{n-1})(Q_n a_{n+1} + Q_{n-1}) - (Q_n x_{n+1} + Q_{n-1})(P_n a_{n+1} + P_{n-1})}{(Q_n x_{n+1} + Q_{n-1})(Q_n a_{n+1} + Q_{n-1})}$$

i po uproszczeniach uwzględniających twierdzenie 18.7 (*iii*),

$$x - R_{n+1} = (-1)^n \cdot \frac{a_{n+1} - x_{n+1}}{(Q_n x_{n+1} + Q_{n-1})(Q_n a_{n+1} + Q_{n-1})}.$$

Ponadto $a_{n+1} = \lfloor x_{n+1} \rfloor$, więc $0 < x_{n+1} - a_{n+1} < 1$. Ponadto $a_{n+1} \geqslant 1$ oraz $x_{n+1} > 1$, więc

$$|x - R_{n+1}| < \frac{1}{(Q_n + Q_{n-1})^2} < \frac{1}{Q_n^2} \leqslant \frac{1}{n^2} \leqslant \frac{1}{n},$$

na mocy twierdzenia 18.7. Wynika stąd, że $x = \lim\limits_{n\to\infty} R_n$. Jak wiemy, $\lim\limits_{n\to\infty} R_n = \langle a_0, a_1, \ldots\rangle$, więc $x = \langle a_0, a_1, a_2, \ldots\rangle$.

Stąd i z twierdzenia 18.24 wynika od razu następujące

Twierdzenie 18.25. *Każda rzeczywista liczba niewymierna jest dokładnie jednym nieskończonym ułamkiem łańcuchowym.*

Przykład 18.26. Przedstawimy $\sqrt{21}$ w postaci nieskończonego ułamka łańcuchowego. Tutaj $x = \sqrt{21}$, więc $4 < \sqrt{21} < 5$, skąd $a_0 = \lfloor x \rfloor = 4$. Zatem $x_1 = \frac{1}{\sqrt{21}-4} = \frac{\sqrt{21}+4}{21-4^2} = \frac{\sqrt{21}+4}{5}$. Stąd na mocy stwierdzenia 9.46, $a_1 = \lfloor x_1 \rfloor = \lfloor \frac{4+4}{5} \rfloor = 1$. Dalej, $x_2 = \frac{1}{x_1 - a_1} = \frac{1}{\frac{\sqrt{21}+4}{5}-1} =$ $= \frac{5}{\sqrt{21}-1} = \frac{5(\sqrt{21}+1)}{21-12} = \frac{\sqrt{21}+1}{4}$, więc na mocy stwierdzenia 9.46, $a_2 =$ $= \lfloor \frac{4+1}{4} \rfloor = 1$. Wobec tego $x_3 = \frac{1}{\frac{\sqrt{21}+1}{4}-1} = \frac{4}{\sqrt{21}-3} = \frac{4(\sqrt{21}+3)}{21-3^2} =$

$\frac{\sqrt{21}+3}{3}$, więc na mocy stwierdzenia 9.46, $a_3 = \lfloor \frac{4+3}{3} \rfloor = 2$. Dalej, $x_4 = \frac{1}{\frac{\sqrt{21}+3}{3}-2} = \frac{3}{\sqrt{21}-3} = \frac{3(\sqrt{21}+3)}{21-3^2} = \frac{\sqrt{21}+3}{4}$, więc na mocy stwierdzenia 9.46, $a_4 = \lfloor \frac{4+3}{4} \rfloor = 1$. Stąd $x_5 = \frac{1}{\frac{\sqrt{21}+3}{4}-1} = \frac{4}{\sqrt{21}-1} = \frac{4(\sqrt{21}+1)}{21-1} = \frac{\sqrt{21}+1}{5}$, więc na mocy stwierdzenia 9.46, $a_5 = \lfloor \frac{4+1}{5} \rfloor = 1$. Dalej, $x_6 = \frac{1}{\frac{\sqrt{21}+1}{5}-1} = \frac{5}{\sqrt{21}-4} = \frac{5(\sqrt{21}+4)}{21-4^2} = \sqrt{21}+4$, więc na mocy stwierdzenia 9.46, $a_6 = 4+4 = 8$. Stąd $x_7 = \frac{1}{\sqrt{21}+4-8} = \frac{1}{\sqrt{21}-4} = x_1$. Zatem $a_7 = a_1$, skąd $x_8 = x_2$, i tak dalej. Wobec tego

$$\sqrt{21} = \langle 4, 1, 1, 2, 1, 1, 8, 1, 1, 2, 1, 1, 8, \ldots \rangle,$$

co będziemy zapisywać w postaci $\sqrt{21} = \langle 4, \overline{1, 1, 2, 1, 1, 8} \rangle$.

Twierdzenie 18.27. *Niech α będzie liczbą rzeczywistą i niech a oraz b będą względnie pierwszymi liczbami całkowitymi takimi, że $b > 0$ oraz $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$. Wówczas $a = P_m$ i $b = Q_m$ dla pewnego $m \in \mathbb{N}_0$, gdzie ciągi $(P_n)_{n=0}^{\infty}$ i $(Q_n)_{n=0}^{\infty}$ są wyznaczone przez rozwinięcie liczby α na ułamek łańcuchowy.*

Dowód. Rozważmy najpierw przypadek $\alpha = \frac{a}{b}$. Wtedy z twierdzenia 18.15 wynika, że α jest skończonym ułamkiem łańcuchowym, czyli $\alpha = \langle a_0, a_1, \ldots, a_m \rangle$. Na mocy twierdzenia 18.11 mamy, że $\alpha = \frac{P_m}{Q_m}$, przy czym $P_m \in \mathbb{Z}$, $Q_m \in \mathbb{N}$ i $\mathrm{NWD}(P_m, Q_m) = 1$. Zatem $\frac{a}{b} = \frac{P_m}{Q_m}$, skąd $aQ_m = bP_m$. Dodatkowo $\mathrm{NWD}(a, b) = 1$, więc z zasadniczego twierdzenia arytmetyki, $b \mid Q_m$ i $Q_m \mid b$, skąd $b = Q_m$, bo $b, Q_m \in \mathbb{N}$. Po skróceniu przez b, $a = P_m$.

Niech dalej $\alpha \neq \frac{a}{b}$. Wtedy z wniosku 18.16 istnieje $m \in \mathbb{N}_0$ i istnieją $c_0 \in \mathbb{Z}$ oraz $c_1, c_2, \ldots, c_m \in \mathbb{N}$ takie, że

$$\frac{a}{b} = \langle c_0, c_1, \ldots, c_m \rangle \text{ oraz } (-1)^m = \operatorname{sgn}\left(\alpha - \frac{a}{b}\right). \tag{18.16}$$

Jeśli $m = 0$, to $\frac{a}{b} = c_0$ i $\alpha > \frac{a}{b}$, skąd $a = bc_0$. Dodatkowo $\mathrm{NWD}(a, b) = 1$, więc $b = 1$. Wobec tego $\alpha > a$. Ponadto $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$, więc $\alpha - \frac{a}{b} < \frac{1}{2}$, czyli $\alpha < a + \frac{1}{2}$. Zatem $a < \alpha < a + 1$, skąd $\lfloor \alpha \rfloor = a = P_0$ i $b = Q_0$.

Niech dalej $m > 0$. Podobnie jak w pierwszej części dowodu uzyskuje się, że $a = p_m(c_0, c_1, \ldots, c_m)$ i $b = q_m(c_0, c_1, \ldots, c_m)$. Oznaczmy $p_i(c_0, \ldots, c_i) = P'_i$ oraz $q_i(c_0, \ldots, c_i) = Q'_i$ dla $i = 0, 1, \ldots, m$. Ze wzorów (18.16) mamy, że $0 < (-1)^m(\alpha - \frac{a}{b}) < \frac{1}{2b^2}$, więc $0 < (-1)^m(\alpha b - +a) < \frac{1}{2b}$, bo $b > 0$. Wobec tego

$$0 < (-1)^m(\alpha Q'_m - P'_m) < \frac{1}{2Q'_m}. \tag{18.17}$$

Niech

$$\omega = \frac{P'_{m-1} - \alpha Q'_{m-1}}{\alpha Q'_m - P'_m}. \tag{18.18}$$

Wtedy $\omega\alpha Q'_m - \omega P'_m = P'_{m-1} - \alpha Q'_{m-1}$, czyli $\alpha(\omega Q'_m + Q'_{m-1}) = \omega P'_m + +P'_{m-1}$. Zatem

$$\alpha = \frac{\omega P'_m + P'_{m-1}}{\omega Q'_m + Q'_{m-1}}. \tag{18.19}$$

Z (18.18) i (18.17) mamy, że

$$\omega + \frac{Q'_{m-1}}{Q'_m} = \frac{Q'_m P'_{m-1} - \alpha Q'_{m-1} Q'_m + \alpha Q'_m Q'_{m-1} - P'_m Q'_{m-1}}{Q'_m(\alpha Q'_m - P'_m)} =$$

$$= \frac{P'_{m-1} Q'_m - Q'_{m-1} P'_m}{Q'_m(\alpha Q'_m - P'_m)} = \frac{(-1)^m}{Q'_m(\alpha Q'_m - P'_m)} =$$

$$= \frac{1}{(-1)^m Q'_m(\alpha Q'_m - P'_m)} > 2.$$

Ponadto $\frac{Q'_{m-1}}{Q'_m} \leqslant 1$ na mocy twierdzenia 18.7, więc $\omega > 1$, skąd $\lfloor \omega \rfloor > 1$. Zatem na mocy twierdzenia 18.6 i wzoru (18.19) dostajemy, że

$$\langle c_0, c_1, \ldots, c_m, \omega \rangle = \frac{\omega P'_m + P'_{m-1}}{\omega Q'_m + Q'_{m-1}} = \alpha.$$

Jeśli $\alpha \in \mathbb{Q}$, to z (18.18), $\omega \in \mathbb{Q}$ i na mocy twierdzenia 18.15 i lematu 18.13, $\omega = \langle c_{m+1}, c_{m+2}, \ldots, c_{m+n} \rangle$ dla pewnych liczb naturalnych $n, c_{m+1}, c_{m+2}, \ldots, c_{m+n}$, przy czym $c_{m+n} > 1$. Stąd i z (18.2) uzyskujemy, że $\alpha = \langle c_0, c_1, \ldots, c_m, c_{m+1}, \ldots, c_{m+n} \rangle$, więc na mocy twierdzenia 18.15, $P'_i = P_i$ oraz $Q'_i = Q_i$ dla $i = 0, 1, \ldots, m$, czyli $a = P_m$ i $b = Q_m$.

Jeśli liczba $\alpha \notin \mathbb{Q}$, to z (18.19), $\omega \notin \mathbb{Q}$ i z twierdzeń 18.25 i 18.21 istnieją liczby naturalne $c_{m+1}, c_{m+2}, \ldots$ takie, że $\omega = \langle c_{m+1}, c_{m+2}, \ldots \rangle$. Stąd i z (18.11) uzyskujemy, że $\alpha = \langle c_0, c_1, \ldots, c_m, c_{m+1}, c_{m+2}, \ldots \rangle$. Zatem na mocy twierdzenia 18.20 otrzymujemy, że $P_i' = P_i$ oraz $Q_i' = Q_i$ dla $i = 0, 1, \ldots, m$, czyli $a = P_m$ i $b = Q_m$. □

Ćwiczenie 18.28. Przedstaw w postaci ułamka łańcuchowego następujące liczby rzeczywiste:
(a) $\frac{1+\sqrt{5}}{2}$, (b) $\frac{1+\sqrt{5}}{3}$, (c) $\frac{2+\sqrt{5}}{4}$.

Przykład 18.29. Niech ciągi $(P_n)_{n=0}^{\infty}$ i $(Q_n)_{n=0}^{\infty}$ będą wyznaczone przez rozwinięcie liczby niewymiernej α na ułamek łańcuchowy. Udowodnimy, że $|\alpha - \frac{P_n}{Q_n}| < \frac{1}{2Q_n^2}$ lub $|\alpha - \frac{P_{n+1}}{Q_{n+1}}| < \frac{1}{2Q_{n+1}^2}$ dla każdego $n \in \mathbb{N}$. Ponieważ liczba α leży w przedziale otwartym o końcach $\frac{P_n}{Q_n}$ i $\frac{P_{n+1}}{Q_{n+1}}$, więc na mocy twierdzeń 18.20 i 18.25 mamy, że $|\alpha - \frac{P_n}{Q_n}| + |\alpha - \frac{P_{n+1}}{Q_{n+1}}| = |\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}}| = \frac{1}{Q_n Q_{n+1}}$. Przypuśćmy, że $|\alpha - \frac{P_n}{Q_n}| \geqslant \frac{1}{2Q_n^2}$ i $|\alpha - \frac{P_{n+1}}{Q_{n+1}}| \geqslant \frac{1}{2Q_{n+1}^2}$. Wtedy $\frac{1}{2Q_n^2} + \frac{1}{2Q_{n+1}^2} \leqslant \frac{1}{Q_n Q_{n+1}}$, skąd $2Q_n Q_{n+1} \geqslant Q_n^2 + Q_{n+1}^2$, czyli $(Q_{n+1} - Q_n)^2 \leqslant 0$. Wobec tego $Q_{n+1} = Q_n$, co przeczy twierdzeniu 18.20. Wobec tego $|\alpha - \frac{P_n}{Q_n}| < \frac{1}{2Q_n^2}$ lub $|\alpha - \frac{P_{n+1}}{Q_{n+1}}| < \frac{1}{2Q_{n+1}^2}$ dla każdego $n \in \mathbb{N}$.

Załóżmy, że $m \in \mathbb{N}$ i $|\alpha - \frac{P_m}{Q_m}| < \frac{1}{2Q_m^2}$. Wtedy z pierwszej części naszego rozumowania mamy, że $|\alpha - \frac{P_{m+1}}{Q_{m+1}}| < \frac{1}{2Q_{m+1}^2}$ lub $|\alpha - \frac{P_{m+2}}{Q_{m+2}}| < \frac{1}{2Q_{m+2}^2}$. Wynika stąd, że $|\alpha - \frac{P_n}{Q_n}| < \frac{1}{2Q_n^2}$ dla nieskończenie wielu $n \in \mathbb{N}$.

Przykład 18.30. Niech $D > 4$ będzie liczbą naturalną, która nie jest kwadratem liczby naturalnej. Niech ciągi $(P_n)_{n=0}^{\infty}$ i $(Q_n)_{n=0}^{\infty}$ będą wyznaczone przez rozwinięcie liczby $\sqrt{D}$ na ułamek łańcuchowy. Udowodnimy, że jeżeli $x, y \in \mathbb{N}$ i $x^2 - Dy^2 = \pm 2$, to $x = P_m$ i $y = Q_m$ dla pewnego $m \in \mathbb{N}_0$. Zauważmy najpierw, że $d > 5$, bo inaczej (to znaczy dla $d = 5$) mielibyśmy, że $x^2 \equiv \pm 1 \pmod 5$, co wobec przykładu 12.13 prowadzi do sprzeczności. Wobec tego $D \geqslant 6$, skąd $\sqrt{D-2} + \sqrt{D} > 4$. Jeśli $k = \mathrm{NWD}(x, y)$, to $k^2 \mid 2$, skąd $k = 1$, czyli liczby x i y są względnie pierwsze. Ponadto $x^2 = Dy^2 \pm 2 \geqslant Dy^2 - 2$, skąd $\frac{x^2}{y^2} \geqslant D - 2$,

a więc $\frac{x}{y} \geqslant \sqrt{D-2}$ oraz $\frac{x}{y} + \sqrt{D} > 4$. Ponadto $|x^2 - Dy^2| = 2$, więc $|\frac{x}{y} - \sqrt{D}| = \frac{2}{(\frac{x}{y}+\sqrt{D})y^2} < \frac{2}{4y^2} = \frac{1}{2y^2}$. Zatem na mocy twierdzenia 18.27 mamy, że $x = P_m$ i $y = Q_m$ dla pewnego $m \in \mathbb{N}_0$.

Bardzo ciekawe jest przedstawienie stałej Eulera e w postaci ułamka łańcuchowego. Mianowicie na mocy twierdzenia 240 w [7] zachodzi wzór:

$$e = \langle 2, a_1, a_2, a_3, \ldots \rangle,$$

gdzie $a_{3n} = a_{3n+1} = 1$ i $a_{3n-1} = 2n$ dla każdego $n \in \mathbb{N}$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 19

Niewymierności kwadratowe

19.1 Określenie niewymierności kwadratowych

Niech D będzie liczbą naturalną, która nie jest kwadratem liczby naturalnej. Wówczas dodatnia liczba rzeczywista $\sqrt{D}$ jest niewymierna na mocy twierdzenia 8.53. Wynika stąd, że dla dowolnych $a, b \in \mathbb{Q}$ takich, że $b \neq 0$ liczby $a + b\sqrt{D}$ i $a - b\sqrt{D}$ są niewymierne oraz różne. Ponadto, dla dowolnych liczb wymiernych a_1, a_2, b_1, b_2:

$$a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D} \iff [a_1 = a_2 \text{ i } b_1 = b_2]. \tag{19.1}$$

Oznacza to, że przy ustalonym D zapis liczby rzeczywistej w postaci $a + b\sqrt{D}$, gdzie $a, b \in \mathbb{Q}$ jest jednoznaczny.

Przyjrzymy się teraz zbiorowi:

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}. \tag{19.2}$$

Jest jasne, że $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D})$ i $\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. Standardowe sprawdzenie pokazuje też, że $-\alpha, \alpha+\beta, \alpha\cdot\beta \in \mathbb{Q}(\sqrt{D})$ dla dowolnych $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$. Weźmy dowolne niezerowe $\alpha \in \mathbb{Q}(\sqrt{D})$. Wtedy na mocy (19.1) istnieją $a, b \in \mathbb{Q}$ takie, że $b \neq 0$ i $\alpha = a + b\sqrt{D}$, przy czym $\beta = a - b\sqrt{D} \neq 0$. Zatem $0 \neq \alpha \cdot \beta = a^2 - b^2 D \in \mathbb{Q}$ oraz $\frac{1}{\alpha} = \frac{\beta}{\alpha\cdot\beta} = \frac{a-b\sqrt{D}}{a^2-b^2D} = \frac{a}{a^2-B^2D} + + \frac{-b}{a^2-b^2D}\sqrt{D}$, skąd $\frac{1}{\alpha} \in \mathbb{Q}(\sqrt{D})$. W ten sposób wykazaliśmy, że **zbiór**

$\mathbb{Q}(\sqrt{D})$ **z naturalnym dodawaniem i mnożeniem liczb rzeczywistych tworzy ciało**, gdyż jest podciałem ciała $\mathbb{R}$.

W dalszych naszych rozważaniach będziemy używali funkcji ze zbioru $\mathbb{Q}(\sqrt{D})$ w zbiór $\mathbb{Q}(\sqrt{D})$ danej dla dowolnych $a, b \in \mathbb{Q}$ wzorem:

$$a + b\sqrt{D} \mapsto \overline{a + b\sqrt{D}} = a - b\sqrt{D} \tag{19.3}$$

i nazywanej przez nas **sprzęganiem** w ciele $\mathbb{Q}(\sqrt{D})$. Własności tej funkcji grupuje następujące stwierdzenie.

Stwierdzenie 19.1. *Załóżmy, że liczba naturalna D nie jest kwadratem liczby naturalnej. Wówczas dla dowolnych $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$:*

(i) $\alpha \notin \mathbb{Q} \iff \overline{\alpha} \notin \mathbb{Q}$,
(ii) $\alpha = \overline{\alpha} \iff \alpha \in \mathbb{Q}$,
(iii) $\overline{\alpha} = \overline{\beta} \iff \alpha = \beta$,
(iv) $\overline{(\overline{\alpha})} = \alpha$,
(v) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ *i* $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$,
(vi) $\overline{(\frac{\alpha}{\beta})} = \frac{\overline{\alpha}}{\overline{\beta}}$, *gdy* $\beta \neq 0$.

W szczególności sprzęganie w ciele $\mathbb{Q}(\sqrt{D})$ jest bijekcją.

Dowód. Oczywiście $\alpha = a_1 + b_1\sqrt{D}$ i $\beta = a_2 + b_2\sqrt{D}$ dla pewnych $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Z niewymierności liczby $\sqrt{D}$ wynika, że $\alpha \notin \mathbb{Q}$ wtedy i tylko wtedy, gdy $b_1 \neq 0$ oraz $\overline{\alpha} = a_1 - b_1\sqrt{D} \notin \mathbb{Q}$ wtedy i tylko wtedy, gdy $-b_1 \neq 0$. Stąd wynika (i).

(ii). Jeśli $\alpha = \overline{\alpha}$, to na mocy (19.1), $b_1 = -b_1$, skąd $b_1 = 0$ i $\alpha = a_1 \in \mathbb{Q}$. Na odwrót, niech $\alpha \in \mathbb{Q}$. Wtedy $\alpha = \alpha + 0 \cdot \sqrt{D}$, więc $\overline{\alpha} = a_1 - 0 \cdot \sqrt{D} = a_1 = \alpha$.

(iii). Wynika od razu z (19.1) i (19.3).

(iv). Ze wzoru (19.3), $\overline{(\overline{\alpha})} = \overline{a_1 - b_1\sqrt{D}} = a_1 - (-b_1)\sqrt{D} = \alpha$.

(v). Ze wzoru (19.3) mamy, $\overline{\alpha + \beta} = \overline{(a_1 + a_2) + (b_1 + b_2)\sqrt{D}} = (a_1 + a_2) - (b_1 + b_2)\sqrt{D} = (a_1 - b_1\sqrt{D}) + (a_2 - b_2\sqrt{D}) = \overline{\alpha} + \overline{\beta}$ oraz $\alpha \cdot \beta = (a_1 + b_1\sqrt{D}) \cdot (a_2 + b_2\sqrt{D}) = (a_1a_2 + b_1b_2D) + (a_1b_2 + a_2b_1)\sqrt{D}$, więc $\overline{\alpha \cdot \beta} = (a_1a_2 + b_1b_2D) - (a_1b_2 + a_2b_1)\sqrt{D}$. Ponadto mamy, że $\overline{\alpha} \cdot \overline{\beta} = (a_1 - b_1\sqrt{D}) \cdot (a_2 - b_2\sqrt{D}) = (a_1a_2 + b_1b_2D) - (a_1b_2 + a_2b_1)\sqrt{D}$. Zatem $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$.

(vi). Ponieważ $\beta \neq 0$, więc z (iii), $\overline{\beta} \neq \overline{0} = 0$. Ponadto $\alpha = \frac{\alpha}{\beta} \cdot \beta$, więc na mocy (v), $\overline{\alpha} = \overline{(\frac{\alpha}{\beta})} \cdot \overline{\beta}$. Zatem po podzieleniu obu stron przez $\overline{\beta} \neq 0$ uzyskamy tezę. □

Przez prostą indukcję ze stwierdzenia 19.1 można wyprowadzić następujący

Wniosek 19.2. *Załóżmy, że liczba naturalna D nie jest kwadratem liczby naturalnej. Wówczas dla dowolnego $n \in \mathbb{N}$ i dla dowolnych $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}(\sqrt{D})$:*
(i) $\overline{\alpha_1 + \alpha_2 + \ldots + \alpha_n} = \overline{\alpha_1} + \overline{\alpha_2} + \ldots + \overline{\alpha_n}$,
(ii) $\overline{\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n} = \overline{\alpha_1} \cdot \overline{\alpha_2} \cdot \ldots \cdot \overline{\alpha_n}$,
(iii) $\overline{(\alpha^n)} = \overline{\alpha}^n$.

Definicja 19.3. Niewymiernością kwadratową nazywamy każdą liczbę niewymierną należącą do ciała postaci $\mathbb{Q}(\sqrt{D})$, gdzie D jest liczbą naturalną nie będącą kwadratem liczby naturalnej. **Niewymiernością kwadratową sprzężoną** do niewymierności kwadratowej $\alpha = a + b\sqrt{D}$ dla $a, b \in \mathbb{Q}$, $b \neq 0$, nazywamy liczbę $\overline{\alpha} = a - b\sqrt{D}$.

Następujące stwierdzenie pokazuje, że określenie niewymierności kwadratowej sprzężonej nie zależy od liczby D, ale od ciała $\mathbb{Q}(\sqrt{D})$.

Stwierdzenie 19.4. *Niech D_1 i D_2 będą liczbami naturalnymi, które nie są kwadratami liczb naturalnych i niech $x_1, x_2, y_1, y_2 \in \mathbb{Q}$. Jeżeli $x_1 + y_1\sqrt{D_1} = x_2 + y_2\sqrt{D_2}$, to $x_1 - y_1\sqrt{D_1} = x_2 - y_2\sqrt{D_2}$.*

Dowód. Jeśli $y_1 = 0$, to $x_1 - x_2 = y_2\sqrt{D_2}$, więc z niewymierności $\sqrt{D_2}$, $y_2 = 0$ oraz $x_1 = x_2$. Zatem $x_1 - y_1\sqrt{D_1} = x_2 - y_2\sqrt{D_2}$. Podobnie jest, gdy $y_2 = 0$. Niech dalej $y_1 \neq 0$ i $y_2 \neq 0$. Wtedy $\sqrt{D_2} = \frac{x_1 - x_2}{y_2} + \frac{y_1}{y_2}\sqrt{D_1}$, skąd $D_2 = (\frac{x_1 - x_2}{y_2})^2 + \frac{y_1^2}{y_2^2}D_1 + 2\frac{x_1 - x_2}{y_2}\frac{y_1}{y_2}\sqrt{D_1}$, więc z niewymierności $\sqrt{D_1}$ i tego, że $y_1 \neq 0$, $x_1 - x_2 = 0$, czyli $x_1 = x_2$. Zatem $y_1\sqrt{D_1} = y_2\sqrt{D_2}$ i stąd $x_1 - y_1\sqrt{D_1} = x_2 - y_2\sqrt{D_2}$. □

Stwierdzenie 19.5. *Liczba rzeczywista α jest niewymiernością kwadratową wtedy i tylko wtedy, gdy α jest pierwiastkiem trójmianu*

kwadratowego $f(x) = Ax^2 + Bx + C$ *o współczynnikach całkowitych i o dodatnim wyróżniku* $\Delta = B^2 - 4AC$*, który nie jest kwadratem liczby naturalnej. Ponadto, jeśli* $f(\alpha) = 0$*, to* $f(\overline{\alpha}) = 0$*.*

Dowód. Niech $\alpha = a + b\sqrt{D}$, gdzie $a, b \in \mathbb{Q}$, $b \neq 0$ i liczba naturalna D nie jest kwadratem liczby naturalnej. Wtedy istnieje liczba naturalna n taka, że $k = na \in \mathbb{Z}$ i $l = nb \in \mathbb{Z} \setminus \{0\}$. Stąd $n\alpha = k + l\sqrt{D}$, czyli $(n\alpha - k)^2 = l^2 D$. Wobec tego $n^2\alpha^2 - 2nk\alpha + k^2 - l^2 D = 0$. Zatem dla $A = n^2$, $B = -2nk$ i $C = k^2 - l^2 D$ mamy, że $A, B, C \in \mathbb{Z}$, $A > 0$ oraz α jest pierwiastkiem trójmianu kwadratowego $Ax^2 + Bx + C$ o wyróżniku $\Delta = B^2 - 4AC = 4n^2k^2 - 4n^2(k^2 - l^2 D) = 4n^2 l^2 D \in \mathbb{N}$, który nie jest kwadratem liczby naturalnej, gdyż D nie jest kwadratem liczby naturalnej.

Na odwrót, niech α będzie pierwiastkiem trójmianu kwadratowego $f(x) = Ax^2 + Bx + C$ o współczynnikach całkowitych i o dodatnim wyróżniku $\Delta = B^2 - 4AC$, który nie jest kwadratem liczby naturalnej. Wtedy $\alpha \in \mathbb{R}$ oraz $\alpha = \frac{-B+\sqrt{\Delta}}{2A}$ lub $\alpha = \frac{-B-\sqrt{\Delta}}{2A}$, skąd wynika, że $\alpha \in \mathbb{Q}(\sqrt{\Delta})$. Jednak $\sqrt{\Delta}$ jest liczbą niewymierną, więc też α jest liczbą niewymierną. Wobec tego α jest niewymiernością kwadratową. Ponadto $A\alpha^2 + B\alpha + C = 0$, więc na mocy wniosku 19.2 mamy, że $\overline{A}(\overline{\alpha})^2 + \overline{B}\overline{\alpha} + \overline{C} = \overline{0}$. Dodatkowo $\overline{q} = q$ dla każdego $q \in \mathbb{Q}$, więc $A(\overline{\alpha})^2 + B\overline{\alpha} + C = 0$, czyli $f(\overline{\alpha}) = 0$. □

Stwierdzenie 19.6. *Niech* α *będzie niewymiernością kwadratową i niech* $\beta \in \mathbb{R}$*. Wówczas:* $\beta = \overline{\alpha}$ *wtedy i tylko wtedy, gdy* $\alpha + \beta \in \mathbb{Q}$ *oraz* $\alpha \cdot \beta \in \mathbb{Q}$*.*

Dowód. Z założenia wynika, że istnieje liczba naturalna D, która nie jest kwadratem liczby naturalnej i istnieją $a, b \in \mathbb{Q}$ takie, że $b \neq 0$ oraz $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$.

Jeżeli $\beta = \overline{\alpha}$, to $\beta = a - b\sqrt{D}$, więc $\alpha + \beta = 2a \in \mathbb{Q}$ i $\alpha \cdot \beta = a^2 - b^2 D \in \mathbb{Q}$.

Na odwrót, niech $\alpha + \beta, \alpha \cdot \beta \in \mathbb{Q}$. Wtedy $\alpha + \beta = q$ dla pewnego $q \in \mathbb{Q}$, skąd $\beta = q - \alpha \in \mathbb{Q}(\sqrt{D})$. Zatem $\beta = x + y\sqrt{D}$ dla pewnych $x, y \in \mathbb{Q}$. Stąd $(a+x)+(b+y)\sqrt{D} = \alpha+\beta \in \mathbb{Q}$, więc z (19.1), $b+y = 0$, czyli $\beta = x - b\sqrt{D} = \overline{\alpha} + (x - a)$. Uwzględniając to, że $\alpha \cdot \overline{\alpha}, \alpha \cdot \beta \in \mathbb{Q}$,

uzyskujemy stąd, że $(x-a)\cdot\alpha \in \mathbb{Q}$, czyli $(x-a)a+(x-a)b\sqrt{D} \in \mathbb{Q}$. Stąd na mocy (19.1), $(x-a)b = 0$. Ponadto $b \neq 0$, więc $x-a = 0$ i $\beta = \overline{\alpha}$. □

Niewymierność kwadratowa $\alpha \in \mathbb{Q}(\sqrt{D})$, jako liczba niewymierna, może być zapisana jednoznacznie w postaci nieskończonego ułamka łańcuchowego $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$, gdzie $a_0 = \lfloor\alpha\rfloor$, $\alpha_0 = \alpha$ oraz $\alpha_{k+1} = \frac{1}{\alpha_k - \lfloor\alpha_k\rfloor}$ dla $k \in \mathbb{N}_0$, przy czym $a_k = \lfloor\alpha_k\rfloor$ dla $k \in \mathbb{N}_0$. Stąd na mocy tego, że $\mathbb{Q}(\sqrt{D})$ jest ciałem, przez prostą indukcję wynika, że $\alpha_k \in \mathbb{Q}(\sqrt{D})$ i α_k jest liczbą niewymierną, czyli α_k jest niewymiernością kwadratową dla każdego $k \in \mathbb{N}_0$. Ze wzoru (18.13) mamy, że dla każdego $k \in \mathbb{N}$:

$$\alpha = \langle a_0, a_1, \ldots, a_{k-1}, \alpha_k\rangle. \tag{19.4}$$

Na mocy stwierdzenia 19.5 mamy, że istnieje trójmian kwadratowy $f(x) = Ax^2 + Bx + C$ o współczynnikach całkowitych i dodatnim wyróżniku $\Delta = B^2 - 4AC$ nie będącym kwadratem liczby naturalnej taki, że $f(\alpha) = 0$.

Ponieważ $\alpha = a_0 + \frac{1}{\alpha_1}$, więc $A(a_0 + \frac{1}{\alpha_1})^2 + B(a_0 + \frac{1}{\alpha_1}) + C = 0$, skąd po standardowych rachunkach: $A_1\alpha_1^2 + B_1^2\alpha_1 + C_1 = 0$ dla

$$A_1 = f(a_0),\ B_1 = 2a_0A + B,\ C_1 = A, \tag{19.5}$$

przy czym $B_1^2 - 4A_1C_1 = B^2 - 4AC$. Udowodnimy, że przy tych oznaczeniach zachodzi też następujący

Lemat 19.7. *Dla każdego naturalnego k liczba α_{k+1} jest pierwiastkiem trójmianu kwadratowego $f_k(x) = A_kx^2 + B_kx + C_k$ o współczynnikach całkowitych i wyróżniku $\Delta_k = B_k^2 - 4A_kC_k = B^2 - 4AC$, przy czym*
$A_k = AP_k^2 + BP_kQ_k + CQ_k^2 = Q_k^2 f(\frac{P_k}{Q_k})$,
$B_k = 2AP_kP_{k-1} + B(P_kQ_{k-1} + Q_kP_{k-1}) + 2CQ_kQ_{k-1}$,
$C_k = AP_{k-1}^2 + BP_{k-1}Q_{k-1} + CQ_{k-1}^2 = Q_{k-1}^2 f(\frac{P_{k-1}}{Q_{k-1}})$.

Dowód. Jest jasne, że $A_k, B_k, C_k \in \mathbb{Z}$ dla każdego $k \in \mathbb{N}$. Trójmian kwadratowy f ma dodatni wyróżnik, który nie jest kwadratem liczby naturalnej, więc f nie posiada pierwiastka wymiernego. Zatem $A_k \neq 0$

i $C_k \neq 0$ dla każdego $k \in \mathbb{N}$, skąd wynika, że f_k jest trójmianem kwadratowym o współczynnikach całkowitych dla każdego $k \in \mathbb{N}$.

Ustalmy teraz $k \in \mathbb{N}$. Zauważmy, że $\Delta_k = n_1A^2 + n_2AB + n_3AC + n_4B^2 + n_5BC + n_6C^2$ dla pewnych liczb całkowitych $n_1, \ldots, n_6$. Stosując wzory skróconego mnożenia obliczamy kolejno:
$n_1 = 4P_k^2P_{k-1}^2 - 4P_k^2P_{k-1}^2 = 0$,
$n_2 = 4P_kP_{k-1}(P_kQ_{k-1} + Q_kP_{k-1}) - 4(P_k^2P_{k-1}Q_{k-1} + P_kQ_kP_{k-1}^2) = 0$,
$n_3 = 8P_kP_{k-1}Q_kQ_{k-1} - 4(P_k^2Q_{k-1}^2 + Q_k^2P_{k-1}^2) =$
$= -4(P_{k-1}Q_k - Q_{k-1}P_k)^2 = -4 \cdot ((-1)^k)^2 = -4$, na mocy twierdzenia 18.20;
$n_4 = (P_kQ_{k-1} + Q_kP_{k-1})^2 - 4P_kQ_kP_{k-1}Q_{k-1} = (P_{k-1}Q_k - Q_{k-1}P_k)^2 =$
$= ((-1)^k)^2 = 1$, na mocy twierdzenia 18.20 oraz
$n_5 = 4(P_kQ_{k-1} + Q_kP_{k-1})Q_kQ_{k-1} - 4(P_kQ_kQ_{k-1}^2 + Q_k^2P_{k-1}Q_{k-1}) =$
$= 0$ i w końcu, $n_6 = 4Q_k^2Q_{k-1}^2 - 4Q_k^2Q_{k-1}^2 = 0$. Wobec tego $\Delta_k = B^2 - 4AC$. Teraz ze wzorów (19.4) i (18.8), $\alpha = \frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}}$, więc ponieważ $A\alpha^2 + B\alpha + C = 0$, to $A(\frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}})^2 + B\frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}} + C =$
$= 0$, skąd $A(P_k\alpha_{k+1} + P_{k-1})^2 + B(P_k\alpha_{k+1} + P_{k-1})(Q_k\alpha_{k+1} + Q_{k-1}) +$
$+C(Q_k\alpha_{k+1} + Q_{k-1})^2 = 0$. Wobec tego $A_k\alpha_{k+1}^2 + B_k\alpha_{k+1} + C_k = 0$. □

19.2 Okresowe ułamki łańcuchowe

Mówimy, że nieskończony ułamek łańcuchowy $\langle a_0, a_1, a_2, \ldots\rangle$ jest **okresowy**, jeżeli ciąg (a_n) jest okresowy, to znaczy istnieją $s \in \mathbb{N}_0$ i $k \in \mathbb{N}$ takie, że $a_{n+k} = a_n$ dla wszystkich $n \geqslant s$, przy czym jeśli $s = 0$, to mówimy, że ten ułamek łańcuchowy jest **czysto okresowy**. Oznaczamy to symbolicznie wzorem:

$$\langle a_0, a_1, a_2, \ldots\rangle = \langle a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}}\rangle. \tag{19.6}$$

Z twierdzenia 18.24 otrzymujemy od razu następujące

Stwierdzenie 19.8. *Niech $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$, $s \in \mathbb{N}_0$ i $k \in \mathbb{N}$. Wówczas równoważne są warunki:*
(i) $\alpha = \langle a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}}\rangle$,
(ii) $\alpha_s = \alpha_{s+k}$, gdzie $\alpha_m = \langle a_m, a_{m+1}, \ldots\rangle$ dla $m \in \mathbb{N}_0$.

Stwierdzenie 19.9. *Niech $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$ będzie ułamkiem łańcuchowym czysto okresowym o najkrótszym okresie długości $k \in \mathbb{N}$. Wówczas $\alpha_m = \langle a_m, a_{m+1}, \ldots\rangle$ dla $m \in \mathbb{N}_0$ też jest ułamkiem łańcuchowym czysto okresowym o najkrótszym okresie k oraz dla każdego $l \in \mathbb{N}_0$: $\alpha_0 = \alpha_l$ wtedy i tylko wtedy, gdy $k \mid l$.*

Dowód. Ponieważ $\alpha = \langle \overline{a_0, a_1, \ldots, a_{k-1}}\rangle$, więc $\alpha_0 = \alpha_{kn}$ dla wszystkich $n \in \mathbb{N}_0$. Na mocy twierdzenia 18.24 mamy stąd, że $a_m = a_{kn+m}$ dla wszystkich $m, n \in \mathbb{N}_0$, a to oznacza, że α_m jest ułamkiem łańcuchowym czysto okresowym o okresie długości k oraz $\alpha_m = \alpha_{m+k}$ dla każdego $m \in \mathbb{N}_0$.

Na mocy stwierdzenia 19.8 wystarczy teraz pokazać, że dla każdego $l \in \mathbb{N}$: jeśli $\alpha_0 = \alpha_l$, to $k \mid l$. Weźmy zatem dowolne $l \in \mathbb{N}$ takie, że $\alpha_0 = \alpha_l$. Wtedy $l = qk + r$ dla pewnych $q, r \in \mathbb{N}_0$ takich, że $r < k$. Zatem $\alpha_r = \alpha_{qk+r} = \alpha_l = \alpha_0$. Stąd na mocy stwierdzenia 19.8, gdy $r > 0$, to r jest długością pewnego okresu ułamka łańcuchowego α_0. Ponadto $r < k$, więc przeczy to minimalności k. Zatem $r = 0$, a więc $k \mid l$. □

Przykład 19.10. Dla $a \in \mathbb{N}$ obliczymy wartość ułamka łańcuchowego $\alpha = \langle\overline{a}\rangle = \langle a, a, a, \ldots\rangle$. Ze stwierdzenia 18.23 mamy, że $\alpha = \langle a, \alpha\rangle$, a z twierdzenia 18.21 uzyskujemy, że $\lfloor\alpha\rfloor = a$ i α jest liczbą niewymierną, więc $\alpha > a > 0$. Zatem $\alpha = a + \frac{1}{\alpha}$, skąd $\alpha^2 - a\alpha - 1 = 0$, skąd $\alpha = \frac{a+\sqrt{a^2+4}}{2}$ lub $\alpha = \frac{a-\sqrt{a^2+4}}{2}$, ale $a^2 + 4 > a^2$, więc $a - \sqrt{a^2+4} < 0$. Wobec tego $\alpha = \frac{a+\sqrt{a^2+4}}{2}$. Mamy zatem wzór:

$$\langle a, a, a, \ldots\rangle = \frac{a + \sqrt{a^2+4}}{2}, \tag{19.7}$$

z którego wynika, że $\langle\overline{a}\rangle$ jest niewymiernością kwadratową dla każdego $a \in \mathbb{N}$. Zauważmy jeszcze, że $\langle\overline{a}\rangle = a + \frac{1}{\alpha} > a$, skąd $\langle\overline{a}\rangle > 1$. Natomiast niewymierność kwadratowa sprzężona z $\langle\overline{a}\rangle$ jest równa $\overline{\alpha} = \frac{a-\sqrt{a^2+4}}{2} <$ < 0 oraz $\sqrt{a^2+4} < a + 2$, skąd $\overline{\alpha} > \frac{a-(a+2)}{2} = -1$. Zatem $\alpha > 1$ oraz $-1 < \overline{\alpha} < 0$.

Przykład 19.11. Dla $a, b \in \mathbb{N}$ obliczymy wartość ułamka łańcuchowego $\alpha = \langle \overline{a, b} \rangle$. Ze stwierdzenia 18.23 mamy, że $\alpha = \langle a, b, \alpha \rangle$, natomiast z twierdzenia 18.21 mamy, że $\lfloor \alpha \rfloor = a$ i α jest liczbą niewymierną, więc $\alpha > a > 0$. Zatem $\alpha = a + \frac{1}{b+\frac{1}{\alpha}}$. Stąd $\alpha = a + \frac{\alpha}{b\alpha+1} > 1$, czyli $b\alpha^2 - ab\alpha - a = 0$. Zatem $\alpha = \frac{ab+\sqrt{a^2b^2+4ab}}{2b}$ lub $\alpha = \frac{ab-\sqrt{a^2b^2+4ab}}{2b}$, ale $a^2b^2 + 4ab > a^2b^2$, więc $\frac{ab-\sqrt{a^2b^2+4ab}}{2b} < 0$ i wobec tego $\alpha = \frac{ab+\sqrt{a^2b^2+4ab}}{2b}$. Mamy zatem wzór:

$$\langle a, b, a, b, a, b, \ldots \rangle = \frac{ab + \sqrt{a^2b^2 + 4ab}}{2b}, \tag{19.8}$$

z którego wynika, że $\langle \overline{a, b} \rangle$ jest niewymiernością kwadratową dla wszystkich $a, b \in \mathbb{N}$. Ponieważ $\sqrt{a^2b^2 + 4ab} < ab + 2$, więc $\frac{ab-\sqrt{a^2b^2+4ab}}{2b} > \frac{ab-(ab+2)}{2} = -1$. Wobec tego w tym przypadku $-1 < \overline{\alpha} < 0$ oraz $\alpha > 1$.

Przykład 19.12. Uogólnijmy przykład 19.11 obliczając wartość ułamka łańcuchowego $\alpha = \langle \overline{a_0, a_1, \ldots, a_k} \rangle$ dla dowolnego naturalnego k. Z definicji ułamka łańcuchowego nieskończonego mamy, że $a_i \in \mathbb{N}$ dla każdego $i = 0, 1, \ldots, k$. Z twierdzenia 18.21 liczba α jest niewymierna i $\lfloor \alpha \rfloor = a_0 \in \mathbb{N}$, skąd wynika, że $\alpha > 1$. Ze stwierdzenia 18.23 mamy, że $\alpha = \langle a_0, a_1, \ldots, a_k, \alpha \rangle$. Zatem na mocy wzoru (18.8), $\alpha = \frac{P_k\alpha+P_{k-1}}{Q_k\alpha+Q_{k-1}}$. Stąd $Q_k\alpha^2 + (Q_{k-1} - P_k)\alpha - P_{k-1} = 0$ i na mocy stwierdzenia 19.5, α jest niewymiernością kwadratową. Ponadto $\alpha = \frac{P_k-Q_{k-1}+\sqrt{(Q_{k-1}-P_k)^2+4Q_kP_{k-1}}}{2Q_k}$ lub $\alpha = \frac{P_k-Q_{k-1}-\sqrt{(Q_{k-1}-P_k)^2+4Q_kP_{k-1}}}{2Q_k}$, więc liczba naturalna $(Q_{k-1}-P_k)^2+4Q_kP_{k-1}$ nie jest kwadratem liczby naturalnej. Dalej, $a_n \in \mathbb{N}$ dla wszystkich $n \in \mathbb{N}_0$, więc z określenia ciągu (P_n) wynika, że $P_n \in \mathbb{N}$ dla wszystkich $n \in \mathbb{N}_0$. Ponadto, jak wiemy, $Q_n \in \mathbb{N}$ dla każdego $n \in \mathbb{N}_0$, więc stąd $\sqrt{(Q_{k-1} - P_k)^2 + 4Q_kP_{k-1}} > |Q_{k-1} - P_k| \geqslant P_k - Q_{k-1}$, czyli $\frac{P_k-Q_{k-1}-\sqrt{(Q_{k-1}-P_k)^2+4Q_kP_{k-1}}}{2Q_k} < 0$. A zatem $\alpha = \frac{P_k-Q_{k-1}+\sqrt{(Q_{k-1}-P_k)^2+4Q_kP_{k-1}}}{2Q_k}$. Wobec tego mamy wzór:

$$\langle \overline{a_0, a_1, \ldots, a_k} \rangle = \frac{P_k - Q_{k-1} + \sqrt{(Q_{k-1} - P_k)^2 + 4Q_kP_{k-1}}}{2Q_k}, \tag{19.9}$$

z którego wynika, że $\alpha = \langle \overline{a_0, a_1, \ldots, a_k} \rangle$ jest niewymiernością kwadratową. Ponadto, jak pokazaliśmy, $\alpha > 1$ oraz

$$\overline{\alpha} = \frac{P_k - Q_{k-1} - \sqrt{(Q_{k-1} - P_k)^2 + 4Q_k P_{k-1}}}{2Q_k} < 0.$$

Ze stwierdzenia 19.1 wynika, że α i $\overline{\alpha}$ są pierwiastkami trójmianu kwadratowego $f(x) = Q_k x^2 + (Q_{k-1} - P_k)x - P_{k-1}$. Dodatkowo $f(0) = -P_{k-1} < 0$ i $f(-1) = (Q_k - Q_{k-1}) + (P_k - P_{k-1}) > 0$, bo z twierdzenia 18.20 wynika, że $Q_k - Q_{k-1} \geqslant 0$ oraz $P_1 = a_0 a_1 + 1 > a_0 = P_0$ i dla $k \geqslant 2$, $P_k = P_{k-1} a_k + P_{k-2} > P_{k-1} a_k \geqslant P_{k-1}$, więc ponieważ $\alpha > 1$ i $\overline{\alpha} < 0$, to z własności trójmianu kwadratowego $\overline{\alpha} > -1$, gdyż $Q_k > 0$. Zatem $\alpha > 1$ i $-1 < \overline{\alpha} < 0$.

Twierdzenie 19.13. (Lagrange). *Liczba rzeczywista α jest nieskończonym ułamkiem łańcuchowym okresowym wtedy i tylko wtedy, gdy α jest niewymiernością kwadratową.*

Dowód. $\Rightarrow$. Załóżmy, że $\alpha = \langle a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}} \rangle$ i oznaczmy $\beta = \langle \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}} \rangle$. Wówczas $\alpha = \langle a_0, \ldots, a_{s-1}, \beta \rangle$ i z przykładów 19.10 i 19.12, β jest niewymiernością kwadratową. Zatem $\beta \in \mathbb{Q}(\sqrt{D})$ dla pewnej liczby naturalnej D, która nie jest kwadratem liczby naturalnej. Jeśli $s = 0$, to $\alpha = \beta$. Jeśli $s = 1$, to $\alpha = \langle a_0, \beta \rangle = a_0 + \frac{1}{\beta}$. Ponadto dla $s \geqslant 2$, z twierdzenia 18.20 uzyskujemy, że $\alpha = \frac{P_{s-1}\beta + P_{s-2}}{Q_{s-1}\beta + Q_{s-2}}$. Stąd we wszystkich przypadkach $\alpha \in \mathbb{Q}(\sqrt{D})$, przy czym na mocy twierdzenia 18.20 liczba α jest niewymierna. Zatem α jest niewymiernością kwadratową.

$\Leftarrow$. Ze stwierdzenia 19.5 wynika, że $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$ jest pierwiastkiem trójmianu kwadratowego $f(x) = Ax^2 + Bx + C$ o współczynnikach całkowitych i dodatnim wyróżniku $\Delta = B^2 - 4AC$, który nie jest kwadratem liczby naturalnej, przy czym można zakładać, że $A > 0$. Ze stwierdzenia 19.1 otrzymujemy, że $A\overline{\alpha}^2 + B\overline{\alpha} + C = 0$, przy czym, jak wiemy, $\alpha \neq \overline{\alpha}$. Zatem α i $\overline{\alpha}$ są jedynymi pierwiastkami trójmianu f oraz $f(x) = A(x - \alpha)(x - \overline{\alpha})$ dla $x \in \mathbb{R}$. W szczególności f nie posiada pierwiastka wymiernego, skąd $f(\frac{P_m}{Q_m}) \neq 0$ dla wszystkich $m \in \mathbb{N}_0$. Ponieważ $\lim\limits_{m \to \infty} \dfrac{P_m}{Q_m} = \alpha$ na mocy twierdzenia 18.20, więc istnieje $n_0 \in \mathbb{N}$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

takie, że $|\alpha - \frac{P_m}{Q_m}| < |\alpha - \overline{\alpha}|$ dla wszystkich $m \geqslant n_0$. Weźmy dowolne naturalne $k \geqslant n_0 + 1$. Wtedy $|\alpha - \frac{P_k}{Q_k}| < |\alpha - \overline{\alpha}|$ i $|\alpha - \frac{P_{k-1}}{Q_{k-1}}| < |\alpha - \overline{\alpha}|$ oraz na mocy twierdzenia 18.20 liczby $\frac{P_k}{Q_k}$ i $\frac{P_{k-1}}{Q_{k-1}}$ leżą po różnych stronach liczby α. Oznacza to, że liczby $f(\frac{P_k}{Q_k})$ i $f(\frac{P_{k-1}}{Q_{k-1}})$ mają różne znaki. Niech $\alpha_{k+1} = \langle a_{k+1}, a_{k+2}, \ldots \rangle$. Wtedy $\alpha = \langle a_0, a_1, \ldots, a_k, \alpha_{k+1} \rangle$ oraz na mocy lematu 19.7, α_{k+1} jest pierwiastkiem trójmianu kwadratowego $f_k(x) = A_k x^2 + B_k x + C_k$ o współczynnikach całkowitych i wyróżniku $B_k^2 - 4A_kC_k = B^2 - 4AC$, przy czym $A_k = Q_k^2 f(\frac{P_k}{Q_k})$ i $C_k = Q_{k-1}^2 f(\frac{P_{k-1}}{Q_{k-1}})$. Ponadto na mocy twierdzenia 18.20 mamy, że $Q_k, Q_{k-1} \in \mathbb{N}$, więc dla wszystkich $k \geqslant n_0+1$ uzyskujemy, że $-A_kC_k = |A_k| \cdot |C_k|$ oraz

$$|B_k|^2 + 4|A_k| \cdot |C_k| = \Delta,$$

gdzie $\Delta = B^2 - 4AC \in \mathbb{N}$. Stąd wynika, że $|A_k|, |B_k|, |C_k| \leqslant \Delta$ dla wszystkich $k \geqslant n_0 + 1$. Ponieważ $A_k, B_k, C_k \in \mathbb{Z}$ dla $k \geqslant n_0 + 1$, więc ciąg

$$(A_{n_0+1}, B_{n_0+1}, C_{n_0+1}), (A_{n_0+2}, B_{n_0+2}, C_{n_0+2}), \ldots$$

posiada jedynie skończenie wiele różnych wyrazów. Zatem pewien jego wyraz powtarza się nieskończenie wiele razy, a więc istnieją liczby naturalne k, p, q takie, że $k \geqslant n_0+1$ i $(A_k, B_k, C_k) = (A_{k+p}, B_{k+p}, C_{k+p}) = (A_{k+p+q}, B_{k+p+q}, C_{k+p+q})$, czyli $A_k = A_{k+p} = A_{k+p+q}$, $B_k = B_{k+p} = B_{k+p+q}$, $C_k = C_{k+p} = C_{k+p+q}$. Wobec tego $f_k = f_{k+p} = f_{k+p+q}$, czyli $f_k(\alpha_k) = f_k(\alpha_{k+p}) = f_k(\alpha_{k+p+q}) = 0$ i trójmian kwadratowy f_k ma dokładnie dwa pierwiastki, więc stąd $\alpha_k = \alpha_{k+p}$ lub $\alpha_k = \alpha_{k+p+q}$ lub $\alpha_{k+p} = \alpha_{k+p+q}$.

W ten sposób pokazaliśmy, że istnieją liczby naturalne k i s takie, że $\alpha_s = \alpha_{s+k}$. Wobec tego na mocy stwierdzenia 19.8 dostajemy, że

$$\alpha = \langle a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}} \rangle.$$

□

Twierdzenie 19.14. (Galois). *Niewymierność kwadratowa α jest nieskończonym ułamkiem czysto okresowym wtedy i tylko wtedy, gdy $\alpha > 1$ i $-1 < \overline{\alpha} < 0$. Ponadto, jeśli $\alpha = \langle \overline{a_0, a_1, \ldots, a_{r-1}} \rangle$, to $\frac{1}{-\overline{\alpha}} = \langle \overline{a_{r-1}, a_{r-2}, \ldots, a_1, a_0} \rangle$.*

Dowód. $\Rightarrow$. Wynika od razu z przykładów 19.10 i 19.12.

$\Leftarrow$. Niech α będzie niewymiernością kwadratową taką, że $\alpha > 1$ i $-1 < \overline{\alpha} < 0$. Z twierdzenia 19.13 liczbę α można zapisać w postaci

$$\alpha = \langle a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}} \rangle.$$

Niech $\alpha_n = \langle a_n, a_{n+1}, \ldots \rangle$ dla $n \in \mathbb{N}_0$. Wtedy $\alpha_0 = \alpha$ i $\alpha_s = \alpha_{s+k}$. Ponieważ $\alpha > 1$, więc $\lfloor \alpha \rfloor \geqslant 1$. Stąd na mocy twierdzenia 18.21, $a_0 = \lfloor \alpha \rfloor \geqslant 1$, czyli $a_0 \in \mathbb{N}$. Wobec tego $a_n \in \mathbb{N}$ dla wszystkich $n \in \mathbb{N}_0$, ale $\alpha_n = a_n + \frac{1}{\alpha_{n+1}} > a_n \geqslant 1$, więc

$$\alpha_n > 1 \quad \text{dla każdego} \quad n \in \mathbb{N}_0. \tag{19.10}$$

Na mocy założeń, $-1 < \overline{\alpha_0} < 0$. Przypuśćmy, że $-1 < \overline{\alpha_n} < 0$ dla pewnego $n \in \mathbb{N}_0$. Wtedy $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$, więc na mocy stwierdzenia 19.1, $\overline{\alpha_n} = a_n + \frac{1}{\overline{\alpha_{n+1}}}$, czyli $-1 < a_n + \frac{1}{\overline{\alpha_{n+1}}} < 0$. Stąd $\overline{\alpha_{n+1}} < 0$ i $\frac{1}{\overline{\alpha_{n+1}}} < -a_n \leqslant -1$, a więc $\frac{1}{\overline{\alpha_{n+1}}} < -1$, czyli $-1 < \overline{\alpha_{n+1}}$. Zatem na mocy zasady indukcji matematycznej

$$-1 < \overline{\alpha_n} < 0 \quad \text{dla każdego} \quad n \in \mathbb{N}_0. \tag{19.11}$$

Ponieważ $\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$ dla $n \in \mathbb{N}$, więc ze stwierdzenia 19.1 dostajemy, że $\overline{\alpha_{n-1}} = a_{n-1} + \frac{1}{\overline{\alpha_n}}$, czyli $-\frac{1}{\overline{\alpha_n}} = a_{n-1} - \overline{\alpha_{n-1}}$. Zatem na mocy (19.11),

$$-\frac{1}{\overline{\alpha_n}} = a_{n-1} - \overline{\alpha_{n-1}} \quad \text{oraz} \quad \left\lfloor -\frac{1}{\overline{\alpha_n}} \right\rfloor = a_{n-1} \quad \text{dla} \quad n \in \mathbb{N}. \tag{19.12}$$

Załóżmy, że $s \geqslant 1$. Wtedy z (19.12) i tego, że $\alpha_s = \alpha_{s+k}$, $a_{s-1} = \lfloor -\frac{1}{\overline{\alpha_s}} \rfloor = \lfloor -\frac{1}{\overline{\alpha_{s+k}}} \rfloor = a_{s+k-1}$. Wobec tego

$$\alpha_{s+k-1} = a_{s+k-1} + \frac{1}{\alpha_{s+k}} = a_{s-1} + \frac{1}{\alpha_s} = \alpha_{s-1}.$$

Zatem $\alpha_{s-1} = \alpha_{(s-1)+k}$. Kontynuując ten proces po skończonej liczbie kroków uzyskamy, że $\alpha_0 = \alpha_r$ dla pewnego $r \in \mathbb{N}$, a to oznacza na mocy stwierdzenia 19.8, że $\alpha = \langle \overline{a_0, a_1, \ldots, a_{r-1}} \rangle$.

Dalej, $\alpha_0 = \alpha_r$, więc z (19.12), $\frac{1}{-\overline{\alpha_0}} = a_{r-1} - \overline{\alpha_{r-1}}$, czyli $\frac{1}{-\overline{\alpha_0}} = \langle a_{r-1}, \frac{1}{-\overline{\alpha_{r-1}}}\rangle$. Załóżmy, że dla pewnego naturalnego $k < r$ zachodzi wzór:

$$\frac{1}{-\overline{\alpha_0}} = \left\langle a_{r-1}, a_{r-2}, \ldots, a_{r-k}, \frac{1}{-\overline{\alpha_{r-k}}} \right\rangle.$$

Wtedy z (19.12), $-\overline{\alpha_{r-k}} = a_{r-(k+1)} - \overline{\alpha_{r-(k+1)}} = \left\langle a_{r-(k+1)}, \frac{1}{-\overline{\alpha_{r-(k+1)}}} \right\rangle$. Stąd na mocy stwierdzenia 18.23,

$$\frac{1}{-\overline{\alpha_0}} = \left\langle a_{r-1}, a_{r-2}, \ldots, a_{r-k}, a_{r-(k+1)}, \frac{1}{-\overline{\alpha_{r-(k+1)}}} \right\rangle.$$

Zatem na mocy zasady indukcji, $\frac{1}{-\overline{\alpha_0}} = \langle a_{r-1}, a_{r-2}, \ldots, a_1, a_0, \frac{1}{-\overline{\alpha_0}}\rangle$, skąd $\frac{1}{-\overline{\alpha}} = \langle \overline{a_{r-1}, a_{r-2}, \ldots, a_1, a_0}\rangle$. □

Stwierdzenie 19.15. *Załóżmy, że liczba naturalna D nie jest kwadratem liczby naturalnej i niech $x, y \in \mathbb{Q}$, gdzie $y \neq 0$. Wówczas równoważne są warunki:*

(i) $x + y\sqrt{D}$ jest ułamkiem łańcuchowym czysto okresowym,

(ii) $x > 0$ i $y > 0$ oraz $\frac{\max\{x,1-x\}}{\sqrt{D}} < y < \frac{x+1}{\sqrt{D}}$.

W szczególności dla każdej liczby wymiernej $x > 0$ istnieje nieskończenie wiele liczb wymiernych $y > 0$ takich, że $x + y\sqrt{D}$ jest ułamkiem łańcuchowym czysto okresowym.

Dowód. $(i) \Rightarrow (ii)$. Na mocy twierdzenia Galois $x + y\sqrt{D} > 1$ oraz $0 > x - y\sqrt{D} > -1$, więc $2x = (x + y\sqrt{D}) + (x - y\sqrt{D}) > 1 + (-1) = 0$, skąd $x > 0$. Zatem $y\sqrt{D} > x > 0$, czyli $y > 0$. Ponadto $y\sqrt{D} > 1 - x$ i $y\sqrt{D} > x$, więc $y\sqrt{D} > \max\{x, 1 - x\}$, skąd $\frac{\max\{x,1-x\}}{\sqrt{D}} < y$, ale $-1 < x - y\sqrt{D}$, więc $y\sqrt{D} < x + 1$, skąd $y < \frac{x+1}{\sqrt{D}}$.

$(ii) \Rightarrow (i)$. Z naszych założeń wynika, że $\frac{x}{\sqrt{D}} < y$ i $\frac{1-x}{\sqrt{D}} < y$, skąd $x - y\sqrt{D} < 0$ i $1 < x + y\sqrt{D}$. Ponadto $y < \frac{x+1}{\sqrt{D}}$, więc $-1 < x - y\sqrt{D}$. Z twierdzenia Galois wynika zatem, że $x + y\sqrt{D}$ jest ułamkiem łańcuchowym czysto okresowym.

Niech x będzie dodatnią liczbą wymierną. Wtedy $x < x + 1$ i $1 - x < x + 1$, więc $\max\{x, 1 - x\} < x + 1$, skąd $0 < \frac{\max\{x,1-x\}}{\sqrt{D}} < \frac{x+1}{\sqrt{D}}$.

Między dowolnymi dwiema liczbami rzeczywistymi leży nieskończenie wiele liczb wymiernych, więc istnieje nieskończenie wiele dodatnich liczb wymiernych y takich, że $\frac{\max\{x,1-x\}}{\sqrt{D}} < y < \frac{x+1}{\sqrt{D}}$ i wtedy $x + y\sqrt{D}$ jest ułamkiem łańcuchowym czysto okresowym. □

Ćwiczenie 19.16. Dla jakich $x, y \in \mathbb{Z}$ liczba $x + y\sqrt{5}$ ma czysto okresowe rozwinięcie na nieskończony ułamek łańcuchowy?

Ćwiczenie 19.17. Wyznacz wszystkie $a, b \in \mathbb{N}$ takie, że $\frac{a+\sqrt{5}}{b}$ ma czysto okresowe rozwinięcie na nieskończony ułamek łańcuchowy.

19.3 Rozwijanie $\sqrt{D}$ na ułamek łańcuchowy

Twierdzenie 19.18. *Jeżeli liczba naturalna D nie jest kwadratem liczby naturalnej, to istnieją liczby naturalne $k, a_0, a_1, \ldots, a_{k-1}$ takie, że*

$$\sqrt{D} = \langle a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle,$$

przy czym dla $k > 1$ ciąg $(a_1, \ldots, a_{k-1})$ jest symetryczny i wszystkie jego wyrazy są nie większe niż a_0. Ponadto $P_{kn-1}^2 - DQ_{kn-1}^2 = (-1)^{kn}$ dla każdego $n \in \mathbb{N}$.

Dowód. Niech $a_0 = \lfloor\sqrt{D}\rfloor$. Wtedy $a_0 \in \mathbb{N}$ i $a_0 < \sqrt{D} < a_0 + 1$, bo $\sqrt{D}$ jest liczbą niewymierną. Stąd $\alpha = a_0 + \sqrt{D} > 1$ jest niewymiernością kwadratową i $\overline{\alpha} = a_0 - \sqrt{D} \in (-1, 0)$.

Na mocy twierdzenia 19.14 liczba α jest nieskończonym ułamkiem łańcuchowym czystym. Ponadto $\lfloor\alpha\rfloor = a_0 + \lfloor\sqrt{D}\rfloor = 2a_0$, więc stąd oraz na mocy twierdzenia 18.21, $a_0 + \sqrt{D} = \langle\overline{2a_0, a_1, \ldots, a_{k-1}}\rangle$ dla pewnych liczb naturalnych $k, a_1, \ldots, a_{k-1}$, przy czym k jest najmniejsze. Zatem

$$a_0 + \sqrt{D} = \langle 2a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle = a_0 + \langle a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle,$$

czyli $\sqrt{D} = \langle a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle$.

Dla $k > 1$ na mocy twierdzenia Galois mamy, że

$$\frac{1}{-(\overline{a_0 + \sqrt{D}})} = \langle\overline{a_{k-1}, \ldots, a_1, 2a_0}\rangle.$$

Ponadto

$$\frac{1}{-(\overline{a_0 + \sqrt{D}})} = \frac{1}{\sqrt{D} - a_0} = \langle\overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle,$$

bo $\sqrt{D} = \langle a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle$, więc

$$\langle\overline{a_1, \ldots, a_{k-1}, 2a_0}\rangle = \langle\overline{a_{k-1}, \ldots, a_1, 2a_0}\rangle.$$

Stąd na mocy twierdzenia 18.24,

$$(a_1, a_2, \ldots, a_{k-1}) = (a_{k-1}, \ldots, a_2, a_1),$$

czyli ciąg $(a_1, a_2, \ldots, a_{k-1})$ jest symetryczny. Niech dla $m \in \mathbb{N}_0$: $\alpha_m = \langle a_m, a_{m+1}, \ldots\rangle$. Wtedy $\alpha_0 = \sqrt{D}$ jest pierwiastkiem trójmianu kwadratowego $f(x) = x^2 - D$. Dla $n \in \mathbb{N}$ z lematu 19.7, liczba α_{n+1} jest pierwiastkiem trójmianu kwadratowego $g(x) = A_n x^2 + B_n x + C_n$ o współczynnikach całkowitych o wyróżniku równym $\Delta_n = 4D$, przy czym $B_n = 2l_n$, gdzie $l_n = P_n P_{n-1} - DQ_n Q_{n-1} \in \mathbb{Z}$ oraz $A_n = P_n^2 - DQ_n^2$. Stąd $\alpha_{n+1} = \frac{-l_n + \sqrt{D}}{A_n}$ lub $\alpha_{n+1} = \frac{-l_n - \sqrt{D}}{A_n}$.

Na mocy stwierdzenia 19.9, α_{n+1} ma rozwinięcie czysto okresowe na ułamek łańcuchowy, więc na mocy stwierdzenia 19.15 dla $A_n > 0$ jest $-l_n > 0$ i $\alpha_{n+1} = \frac{-l_n + \sqrt{D}}{A_n}$, a dla $A_n < 0$ jest $l_n > 0$ oraz $\alpha_{n+1} = \frac{-l_n - \sqrt{D}}{A_n} = \frac{l_n + \sqrt{D}}{-A_n}$. Zauważmy jednak, że A_n jest dodatnie wtedy i tylko wtedy, gdy $\frac{P_n}{Q_n} > \sqrt{D}$. Stąd na mocy twierdzenia 18.20 dla nieparzystych n mamy, że $A_n > 0$ oraz $-l_n > 0$ i $\alpha_{n+1} = \frac{-l_n + \sqrt{D}}{A_n}$, zaś dla parzystych n jest $A_n < 0$ oraz $l_n > 0$ i $\alpha_{n+1} = \frac{l_n + \sqrt{D}}{-A_n}$. Dodatkowo $\alpha_1 = \frac{1}{\sqrt{D} - a_0} = \frac{a_0 + \sqrt{D}}{D - a_0^2}$ i $D - a_0^2 = -A_0$, gdzie $A_0 = P_0^2 - DQ_0^2$. Wobec tego dla każdego $n \in \mathbb{N}$:

$$\alpha_n = \frac{b_n + \sqrt{D}}{c_n}, \quad \text{gdzie } b_n, c_n \in \mathbb{N}, \tag{19.13}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

przy czym

$$P_{n-1}^2 - DQ_{n-1}^2 = c_n \quad \text{dla parzystych } n \in \mathbb{N} \tag{19.14}$$

oraz

$$P_{n-1}^2 - DQ_{n-1}^2 = -c_n \quad \text{dla nieparzystych } n \in \mathbb{N}. \tag{19.15}$$

Niech $n \in \mathbb{N}$. Przypuśćmy, że $c_n = 1$. Wtedy $\lfloor \alpha_n \rfloor = \lfloor b_n + \sqrt{D} \rfloor = b_n + a_0$ na mocy stwierdzenia 9.46, więc

$$\alpha_{n+1} = \frac{1}{b_n + \sqrt{D} - (b_n + a_0)} = \frac{1}{\sqrt{D} - a_0} = \alpha_1 = \langle \overline{a_1, \ldots, a_{k-1}, 2a_0} \rangle.$$

Stąd na mocy stwierdzenia 19.9, $n = km$ dla pewnego $m \in \mathbb{N}$. Zatem dla liczb naturalnych $n < k$ jest $c_n \geqslant 2$, przy czym na mocy twierdzenia Galois $\frac{b_n - \sqrt{D}}{c_n} < 0$, skąd $b_n < \sqrt{D}$. Zatem dla $n = 1, 2, \ldots, k-1$: $\alpha_n < \frac{2\sqrt{D}}{2} = \sqrt{D}$, skąd $a_n = \lfloor \alpha_n \rfloor \leqslant \lfloor \sqrt{D} \rfloor = a_0$, czyli $a_n \leqslant a_0$.

Ustalmy dowolne $n \in \mathbb{N}$. Wtedy $\alpha_{kn} = \alpha_k = a_0 + \sqrt{D}$, więc na mocy (19.13) mamy, że, $c_{kn} = 1$. Jeśli liczba kn jest parzysta, to z (19.14), $P_{kn-1}^2 - DQ_{kn-1}^2 = 1$, a jeśli liczba kn jest nieparzysta, to z (19.15), $P_{kn-1}^2 - DQ_{kn-1}^2 = -1$. Wobec tego $P_{kn-1}^2 - DQ_{kn-1}^2 = (-1)^{kn}$.

Dowód naszego twierdzenia jest zatem zakończony. □

Z dowodu twierdzenia 19.18 i ze stwierdzenia 9.46 wynika następujący **algorytm przedstawiania $\sqrt{D}$ w postaci ułamka łańcuchowego:**

(I) Kładziemy: $b_0 = 0$, $c_0 = 1$ i $a_0 = \lfloor \sqrt{D} \rfloor$.

(II) Dopóki $a_i \neq 2a_0$ obliczamy kolejno dla $i \in \mathbb{N}_0$:
$b_{i+1} = a_i c_i - b_i$, $c_{i+1} = \frac{D - b_{i+1}^2}{c_i}$ oraz $a_{i+1} = \left\lfloor \frac{b_{i+1} + a_0}{c_{i+1}} \right\rfloor$.

(III) Jeżeli dojdziemy do najmniejszego $k \in \mathbb{N}$ takiego, że $a_k = 2a_0$, to $\sqrt{D} = \langle a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0} \rangle$.

Rzeczywiście, $\alpha_0 = \sqrt{D}$ i $a_0 = \lfloor \alpha_0 \rfloor = \lfloor \sqrt{D} \rfloor$, więc $\alpha_0 = \frac{b_0 + \sqrt{D}}{c_0}$. Dalej, $\alpha_1 = \frac{a_0 + \sqrt{D}}{D - a_0^2}$, więc $\alpha_1 = \frac{b_1 + \sqrt{D}}{c_1}$. Zatem na mocy stwierdzenia 9.46, $a_1 = \lfloor \alpha_1 \rfloor = \left\lfloor \frac{b_1 + a_0}{c_1} \right\rfloor$. Ponadto dla $i \in \mathbb{N}$ ze wzoru (19.13) mamy,

że $\alpha_i = \frac{b_i+\sqrt{D}}{c_i}$ oraz $\alpha_{i+1} = \frac{b_{i+1}+\sqrt{D}}{c_{i+1}}$ dla pewnych liczb naturalnych $b_i, b_{i+1}, c_i, c_{i+1}$. Dodatkowo $\alpha_{i+1} = \frac{1}{\alpha_i - a_i}$, więc $\alpha_{i+1} = \frac{1}{\frac{b_i+\sqrt{D}}{c_i} - a_i}$, skąd po usunięciu niewymierności z mianownika ułamka $\alpha_{i+1} = \frac{(a_i c_i - b_i)+\sqrt{D}}{\frac{D-(a_i c_i - b_i)^2}{c_i}}$. Wobec tego $\frac{b_{i+1}+\sqrt{D}}{c_{i+1}} = \frac{(a_i c_i - b_i)+\sqrt{D}}{\frac{D-(a_i c_i - b_i)^2}{c_i}}$. Stąd i z niewymierności $\sqrt{D}$ uzyskujemy, że $b_{i+1} = a_i c_i - b_i$ oraz $c_{i+1} = \frac{D - b_{i+1}^2}{c_i}$. Ponadto $a_{i+1} = \lfloor \alpha_{i+1} \rfloor$, więc na mocy stwierdzenia 9.46, $a_{i+1} = \left\lfloor \frac{b_{i+1}+a_0}{c_{i+1}} \right\rfloor$.

Przykład 19.19. Zastosujmy podany wyżej algorytm do przedstawienia $\sqrt{61}$ w postaci ułamka łańcuchowego. Ponieważ $49 < 61 < 64$, więc $7 < \sqrt{61} < 8$, skąd $\lfloor \sqrt{61} \rfloor = 7$. Wobec tego:

(0) $b_0 = 0$, $c_0 = 1$ i $a_0 = 7$.

Stosując (II) do $i = 0$ uzyskujemy, że $b_1 = 7 \cdot 1 - 0 = 7$, $c_1 = \frac{61-49}{1} = 12$, $a_1 = \lfloor \frac{7+7}{12} \rfloor = 1$, czyli:

(1) $b_1 = 7$, $c_1 = 12$ i $a_1 = 1$.

Podobnie dalej, $b_2 = 1 \cdot 12 - 7 = 5$, $c_2 = \frac{61-25}{12} = \frac{36}{12} = 3$, $a_2 = \lfloor \frac{5+7}{3} \rfloor = 4$, czyli:

(2) $b_2 = 5$, $c_2 = 3$ i $a_2 = 4$.

Dalej, $b_3 = 4 \cdot 3 - 5 = 7$, $c_3 = \frac{61-49}{3} = \frac{12}{3} = 4$, $a_3 = \lfloor \frac{7+7}{4} \rfloor = 3$, czyli:

(3) $b_3 = 7$, $c_3 = 4$ i $a_3 = 3$.

Dalej, $b_4 = 3 \cdot 4 - 7 = 5$, $c_4 = \frac{61-25}{4} = \frac{36}{4} = 9$ i $a_4 = \lfloor \frac{5+7}{9} \rfloor = 1$, czyli:

(4) $b_4 = 5$, $c_4 = 9$ i $a_4 = 1$.

Dalej, $b_5 = 1 \cdot 9 - 5 = 4$, $c_5 = \frac{61-16}{9} = \frac{45}{9} = 5$ i $a_5 = \lfloor \frac{4+7}{5} \rfloor = 2$, czyli:

(5) $b_5 = 4$, $c_5 = 5$ i $a_5 = 2$.

Dalej, $b_6 = 2 \cdot 5 - 4 = 6$, $c_6 = \frac{61-36}{5} = \frac{25}{5} = 5$ i $a_6 = \lfloor \frac{6+7}{5} \rfloor = 2$, czyli:

(6) $b_6 = 6$, $c_6 = 5$ i $a_6 = 2$.

Dalej, $b_7 = 2 \cdot 5 - 6 = 4$, $c_7 = \frac{61-16}{5} = \frac{45}{5} = 9$ i $a_7 = \lfloor \frac{4+7}{9} \rfloor = 1$, czyli:

(7) $b_7 = 4$, $c_7 = 9$ i $a_7 = 1$.

Dalej, $b_8 = 1 \cdot 9 - 4 = 5$, $c_8 = \frac{61-25}{9} = \frac{36}{9} = 4$ i $a_8 = \lfloor \frac{5+7}{4} \rfloor = 3$, czyli:

(8) $b_8 = 5$, $c_8 = 4$ i $a_8 = 3$.

Dalej, $b_9 = 3 \cdot 4 - 5 = 7$, $c_9 = \frac{61-49}{4} = \frac{12}{4} = 3$ i $a_9 = \lfloor \frac{7+7}{3} \rfloor = 4$, czyli:

(9) $b_9 = 7$, $c_9 = 3$ i $a_9 = 4$.

Dalej, $b_{10} = 4 \cdot 3 - 7 = 5$, $c_{10} = \frac{61-25}{3} = \frac{36}{3} = 12$ i $a_{10} = \lfloor \frac{5+7}{12} \rfloor = 1$, czyli:

(10) $b_{10} = 5$, $c_{10} = 12$ i $a_{10} = 1$.

dalej, $b_{11} = 1 \cdot 12 - 5 = 7$, $c_{11} = \frac{61-49}{12} = 1$ i $a_{11} = \lfloor \frac{7+7}{1} \rfloor = 14 = 2a_0$, czyli:

(11) $b_{11} = 7$, $c_{11} = 1$ i $a_{11} = 14 = 2a_0$.

Wobec tego:

$$\sqrt{61} = \langle 7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14} \rangle.$$

Ćwiczenie 19.20. Stosując algorytm podany w tym rozdziale wyznacz rozwinięcie liczby $\sqrt{71}$ na ułamek łańcuchowy.

Ćwiczenie 19.21. Dla jakich liczb naturalnych k istnieją $a, D \in \mathbb{N}$ takie, że $\sqrt{D} = \langle a, \overline{\underbrace{1, \ldots, 1}_{k-1}, 2a} \rangle$?

Ćwiczenie 19.22. Udowodnij, że dla każdej liczby naturalnej k istnieją $a, D \in \mathbb{N}$ takie, że $a \geqslant 3$ i $\sqrt{D} = \langle a, \overline{\underbrace{2, \ldots, 2}_{k-1}, 2a} \rangle$.

19.4 Zastosowania do równań $x^2 - Dy^2 = C$

Lemat 19.23. *Jeżeli liczba naturalna D nie jest kwadratem liczby naturalnej i $\sqrt{D} = \langle a_0, a_1, a_2, \ldots \rangle$ oraz $x, y \in \mathbb{N}$ są takie, że $x^2 - Dy^2 = 1$ lub $x^2 - Dy^2 = -1$, to $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}_0$.*

Dowód. Jeśli $x < y$, to $x^2 - Dy^2 < y^2 - Dy^2 = (1 - D)y^2 \leqslant -1$, skąd $x^2 - Dy^2 < -1$. Wobec tego $x \geqslant y$, czyli $\frac{x}{y} \geqslant 1$. Ponadto $\mathrm{NWD}(x, y) \mid 1$, więc $\mathrm{NWD}(x, y) = 1$. Dalej, $1 = |x^2 - Dy^2| = |(x + y\sqrt{D})(x - y\sqrt{D})| =$

$= y^2(\frac{x}{y} + \sqrt{D})|\sqrt{D} - \frac{x}{y}| > 2y^2|\sqrt{D} - \frac{x}{y}|$, bo $\sqrt{D} > 1$ i $\frac{x}{y} \geqslant 1$. Wobec tego $|\sqrt{D} - \frac{x}{y}| < \frac{1}{2y^2}$. Zatem na mocy twierdzenia 18.27, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}_0$. □

Twierdzenie 19.24. *Niech liczba naturalna D nie będzie kwadratem liczby naturalnej i niech k będzie długością najkrótszego okresu ułamka łańcuchowego $\langle a_0, a_1, a_2, \ldots\rangle = \sqrt{D}$. Jeżeli liczba k jest parzysta, to wszystkimi rozwiązaniami równania Pella $x^2 - Dy^2 = 1$ są pary (P_{km-1}, Q_{km-1}) dla $m \in \mathbb{N}$ i para (P_{k-1}, Q_{k-1}) jest rozwiązaniem minimalnym. Jeżeli liczba k jest nieparzysta, to wszystkimi rozwiązaniami równania Pella $x^2 - Dy^2 = 1$ są pary (P_{2km-1}, Q_{2km-1}) dla $m \in \mathbb{N}$ i (P_{2k-1}, Q_{2k-1}) jest rozwiązaniem minimalnym.*

Dowód. Z twierdzenia 19.18 wiemy, że takie $k \in \mathbb{N}$ istnieje oraz $a_0 \in \in \mathbb{N}$. Wobec tego $P_n \in \mathbb{N}$ dla każdego $n \in \mathbb{N}_0$. Ponadto, jak wiemy $Q_n \in \mathbb{N}$ dla każdego $n \in \mathbb{N}_0$.

Niech liczba k będzie parzysta. Wtedy na mocy twierdzenia 19.18, $P_{km-1}^2 - DQ_{km-1}^2 = 1$ dla każdego $m \in \mathbb{N}$. Zatem (P_{km-1}, Q_{km-1}) jest rozwiązaniem równania Pella $x^2 - Dy^2 = 1$ dla każdego $m \in \mathbb{N}$. Na odwrót, załóżmy, że $x, y \in \mathbb{N}$ i $x^2 - Dy^2 = 1$. Wtedy z lematu 19.23, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}$. Stąd $P_n^2 - DQ_n^2 = 1$, więc na mocy (19.14) i (19.15), $c_{n+1} = 1$ i $n + 1$ jest parzyste, ale z dowodu twierdzenia 19.18, $k \mid n + 1$, więc $n + 1 = km$ dla pewnego $m \in \mathbb{N}$, czyli $n = km - 1$. Ponieważ, jak wiemy, $Q_1 < Q_2 < Q_3 < \ldots$, więc para (P_{k-1}, Q_{k-1}) jest rozwiązaniem minimalnym równania Pella $x^2 - Dy^2 = 1$.

Niech liczba k będzie nieparzysta. Wtedy na mocy twierdzenia 19.18 mamy, że $P_{2km-1}^2 - DQ_{2km-1}^2 = 1$ dla każdego $m \in \mathbb{N}$, czyli (P_{2km-1}, Q_{2km-1}) jest rozwiązaniem równania Pella $x^2 - Dy^2 = 1$. Na odwrót, załóżmy, że $x, y \in \mathbb{N}$ i $x^2 - Dy^2 = 1$. Wtedy z lematu 19.23, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}$. Stąd $P_n^2 - DQ_n^2 = 1$, więc na mocy (19.14) i (19.15), $c_{n+1} = 1$ i $n + 1$ jest parzyste, ale z dowodu twierdzenia 19.18, $k \mid n + 1$, więc $n + 1 = ks$ dla pewnego $s \in \mathbb{N}$ takiego, że liczba ks jest parzysta. Stąd mamy, że $s = 2m$ dla pewnego $m \in \mathbb{N}$ i $n = 2km - 1$. Ponieważ, jak wiemy, $Q_1 < Q_2 < Q_3 < \ldots$,

więc para (P_{2k-1}, Q_{2k-1}) jest rozwiązaniem minimalnym równania Pella $x^2 - Dy^2 = 1$. □

Twierdzenie 19.25. *Niech liczba naturalna D nie będzie kwadratem liczby naturalnej i niech k będzie długością najkrótszego okresu ułamka łańcuchowego $\langle a_0, a_1, a_2, \ldots\rangle = \sqrt{D}$. Równanie $x^2 - Dy^2 = -1$ posiada rozwiązanie w liczbach naturalnych wtedy i tylko wtedy, gdy liczba k jest nieparzysta. Ponadto, gdy liczba k jest nieparzysta, to wszystkimi rozwiązaniami równania $x^2 - Dy^2 = -1$ w liczbach naturalnych są pary $(P_{k(2m-1)-1}, Q_{k(2m-1)-1})$ dla $m \in \mathbb{N}$ i para (P_{k-1}, Q_{k-1}) jest rozwiązaniem minimalnym. W szczególności $P_{2k-1} = P_{k-1}^2 + DQ_{k-1}^2$ i $Q_{2k-1} = 2P_{k-1}Q_{k-1}$.*

Dowód. Z twierdzenia 19.18 wiemy, że takie $k \in \mathbb{N}$ istnieje oraz $a_0 \in$ $\in \mathbb{N}$. Wobec tego $P_n \in \mathbb{N}$ dla każdego $n \in \mathbb{N}_0$. Ponadto, jak wiemy $Q_n \in \mathbb{N}$ dla każdego $n \in \mathbb{N}_0$.

Załóżmy, że istnieją $x, y \in \mathbb{N}$ takie, że $x^2 - Dy^2 = -1$. Wtedy z lematu 19.23, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}$. Stąd $P_n^2 - DQ_n^2 = -1$, więc na mocy (19.14) i (19.15), $c_{n+1} = 1$ i $n+1$ jest nieparzyste. Ponadto z dowodu twierdzenia 19.18, $k \mid n+1$, więc liczba k jest nieparzysta i $n + 1 = ks$ dla pewnego $s \in \mathbb{N}$ takiego, że liczba ks jest nieparzysta. Stąd $s = 2m - 1$ dla pewnego $m \in \mathbb{N}$ i $n = k(2m-1) - 1$. Na odwrót, jeśli liczba k jest nieparzysta, to dla każdego $m \in \mathbb{N}$ liczba $k(2m-1)$ jest nieparzysta, więc na mocy twierdzenia 19.18, $P_{k(2m-1)-1}^2 - DQ_{k(2m-1)-1}^2 = -1$. Zatem para $(P_{k(2m-1)-1}, Q_{k(2m-1)-1})$ jest rozwiązaniem w liczbach naturalnych równania $x^2 - Dy^2 = -1$. Ponieważ, jak wiemy, $Q_1 < Q_2 < Q_3 < \ldots$, więc para (P_{k-1}, Q_{k-1}) jest rozwiązaniem minimalnym równania $x^2 - Dy^2 = -1$. Stąd i na mocy twierdzenia 17.27 para $(P_{k-1}^2 + DQ_{k-1}^2, 2P_{k-1}Q_{k-1})$ jest rozwiązaniem minimalnym równania Pella $x^2 - Dy^2 = 1$. Wobec tego na mocy twierdzenia 19.24, $P_{2k-1} = P_{k-1}^2 + DQ_{k-1}^2$ i $Q_{2k-1} = 2P_{k-1}Q_{k-1}$. □

Przykład 19.26. Zilustrujmy twierdzenia 19.24 i 19.25 dla liczby $D = 61$. Z przykładu 19.19 wiemy, że

$$\sqrt{61} = \langle 7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}\rangle.$$

Zatem $k = 11$ jest liczbą nieparzystą. Stąd para (P_{10}, Q_{10}) jest najmniejszym rozwiązaniem równania $x^2 - 61y^2 = -1$ w liczbach naturalnych oraz $(P_{10}^2 + 61Q_{10}^2, 2P_{10}Q_{10})$ jest najmniejszym rozwiązaniem równania Pella $x^2 - 61y^2 = 1$. Liczby P_{10} i Q_{10} wyznaczymy rekurencyjnie stosując obliczenia w tabelkach:

n	0	1	2	3	4	5	6	7
a_n	7	1	4	3	1	2	2	1
P_n	7	8	39	125	164	453	1070	1523
Q_n	1	1	5	16	21	58	137	195

,

n	8	9	10
a_n	3	4	1
P_n	5639	24079	29718
Q_n	722	3083	3805

,

Zatem $P_{10} = 29718$ i $Q_{10} = 3805$ oraz najmniejszym rozwiązaniem równania Pella $x^2 - 61y^2 = 1$ jest para $(x_0, y_0) = (1766319049, 226153980)$. Zauważmy, że te obliczenia są o wiele krótsze niż w przypadku stosowania tylko twierdzenia 19.24, bo wtedy musielibyśmy liczyć na ogromnych liczbach aż do P_{21} i Q_{21}! Warto o tym zawsze pamiętać, gdy k jest nieparzyste.

Jeśli chodzi o wypisanie wszystkich rozwiązań równania Pella $x^2 - 61y^2 = 1$, to lepiej jest stosować wzory rekurencyjne niż te, które podaje twierdzenie 19.24. Mianowicie z twierdzenia 17.22 uzyskujemy, że $x_{n+1} = 1766319049x_n + 61 \cdot 226153980y_n$ oraz $y_{n+1} = 226153980x_n + 1766319049y_n$ dla $n \in \mathbb{N}_0$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 20

Funkcje arytmetyczne

Każdą funkcję f ze zbioru $\mathbb{N}$ w zbiór $\mathbb{C}$ liczb zespolonych nazywamy **funkcją arytmetyczną**. Zbiór wszystkich funkcji arytmetycznych będziemy oznaczali przez $\mathbb{A}$.

Przykład 20.1. Podamy przykłady ważnych funkcji arytmetycznych.

1) Funkcja Eulera φ. Przypomnijmy, że dla $n \in \mathbb{N}$ $\varphi(n)$ jest liczbą wszystkich liczb naturalnych k takich, że $\mathrm{NWD}(k, n) = 1$.

2) Funkcja τ, przy czym $\tau(n)$ jest liczbą dodatnich dzielników liczby naturalnej n.

3) Funkcja σ, przy czym $\sigma(n)$ jest sumą wszystkich dodatnich dzielników liczby naturalnej n.

4) Funkcja $\mathbb{I}$, przy czym $\mathbb{I}(n) = n$ dla $n \in \mathbb{N}$.

5) Funkcja 1, przy czym $1(n) = 1$ dla $n \in \mathbb{N}$.

6) Funkcja α_p dla $p \in \mathbb{P}$, przy czym dla $n \in \mathbb{N}$ mamy, że $\alpha_p(n) = \max\{k \in \mathbb{N}_0 : p^k \mid n\}$.

7) Funkcja e taka, że $e(1) = 1$ oraz $e(n) = 0$ dla wszystkich liczb naturalnych $n > 1$.

8) Funkcja zerowa 0 określona wzorem $0(n) = 0$ dla każdego $n \in \mathbb{N}$.

Sumą funkcji arytmetycznych f i g nazywamy funkcję $f + g \colon \mathbb{N} \to \mathbb{C}$ taką, że $(f + g)(n) = f(n) + g(n)$ dla każdego $n \in \mathbb{N}$.

Funkcją przeciwną do funkcji arytmetycznej f nazywamy funkcję $(-f)$ taką, że $(-f)(n) = -f(n)$ dla każdego $n \in \mathbb{N}$.

Prosty, standardowy dowód następującego stwierdzenia pozostawiamy Czytelnikowi jako ćwiczenie.

Stwierdzenie 20.2. *Dla dowolnych $f, g, h \in \mathbb{A}$ mamy spełnione następujące zależności:*
(i) $f + g = g + f$,
(ii) $(f + g) + h = f + (g + h)$,
(iii) $f + 0 = 0 + f = f$,
(iv) $f + (-f) = (-f) + f = 0$.

Z algebraicznego punktu widzenia stwierdzenie 20.2 mówi o tym, że struktura algebraiczna $(\mathbb{A}, +, 0)$ jest grupą abelową.

Definicja 20.3. Splotem Dirichleta funkcji arytmetycznych f i g nazywamy funkcję $f*g : \mathbb{N} \to \mathbb{C}$ taką, że $(f*g)(n)$ jest sumą wszystkich liczb postaci $f(d) \cdot g(\frac{n}{d})$, gdzie d przebiega wszystkie dodatnie dzielniki liczb naturalnej n, czyli

$$(f * g)(n) = \sum_{d\in\mathbb{N},\ d|n} f(d) \cdot g(n/d). \tag{20.1}$$

Zauważmy, że wzór (20.1) możemy zapisać w postaci równoważnej:

$$(f * g)(n) = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} f(d) \cdot g(d'). \tag{20.2}$$

Wynika stąd, że $f * g = g * f$ dla dowolnych $f, g \in \mathbb{A}$, to znaczy splot Dirichleta jest działaniem przemiennym.

Przykład 20.4. Pokażemy, że $1 * 1 = \tau$. Rzeczywiście, dla dowolnego $n \in \mathbb{N}$ mamy, że $(1 * 1)(n) = \sum_{d\in\mathbb{N},\ d|n} 1(d) \cdot 1(n/d) = \sum_{d\in\mathbb{N},\ d|n} 1 \cdot 1 =$
$= \sum_{d\in\mathbb{N},\ d|n} 1 = \tau(n)$.

Przykład 20.5. Pokażemy, że $\mathbb{I} * 1 = \sigma$. Rzeczywiście, dla dowolnego $n \in \mathbb{N}$ mamy, że $(\mathbb{I} * 1)(n) = \sum_{d\in\mathbb{N},\ d|n} \mathbb{I}(d) \cdot 1(n/d) = \sum_{d\in\mathbb{N},\ d|n} d \cdot 1 =$
$= \sum_{d\in\mathbb{N},\ d|n} d = \sigma(n)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 20.6. *Dla każdego $f \in \mathbb{A}$ mamy, że $f * e = f$ (czyli funkcja e jest elementem neutralnym splotu Dirichleta).*

Dowód. Zauważmy, że $(f * e)(1) = f(1) \cdot e(1) = f(1) \cdot 1 = f(1)$ oraz dla dowolnej liczby naturalnej $n > 1$ mamy, że $(f * e)(n) = \sum_{d\in\mathbb{N},\ d|n} f(d) \cdot e(n/d) = f(n) \cdot 1 = f(n)$, bo dla $d \neq n$ jest $\frac{n}{d} > 1$, czyli $e(\frac{n}{d}) = 0$. Stąd $f * e = f$. □

Stwierdzenie 20.7. *Dla dowolnych $f, g, h \in \mathbb{A}$ zachodzi wzór: $f * (g + h) = f * g + f * h$.*

Dowód. Weźmy dowolne $n \in \mathbb{N}$. Wtedy $[f * (g + h)](n) = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} f(d) \cdot (g + h)(d') = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} [f(d) \cdot (g(d') + h(d')] = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} [f(d) \cdot g(d') + f(d) \cdot h(d')] = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} f(d) \cdot g(d') + \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} f(d) \cdot h(d') = (f * g)(n) + (f * h)(n) = [f * g + f * h](n)$ i z dowolności n mamy, że $f * (g + h) = f * g + f * h$. □

Stwierdzenie 20.8. *Dla dowolnych $f, g, h \in \mathbb{A}$ zachodzi wzór: $f * (g * h) = (f * g) * h$.*

Dowód. Weźmy dowolne $n \in \mathbb{N}$. Wtedy mamy, że $[f * (g * h)](n) = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} f(d) \cdot (g * h)(d')$ oraz $(g * h)(d') = \sum_{k,l\in\mathbb{N},\ k\cdot l=d'} g(k) \cdot h(l)$, więc $f(d)\cdot(g*h)(d') = \sum_{k,l\in\mathbb{N},\ k\cdot l=d'} f(d) \cdot g(k) \cdot h(l)$ i w konsekwencji tego $[f * (g * h)](n) = \sum_{d,d'\in\mathbb{N},\ d\cdot d'=n} \sum_{k,l\in\mathbb{N},\ k\cdot l=d'} f(d) \cdot g(k) \cdot h(l)$, a zatem $[f * (g * h)](n) = \sum_{d,k,l\in\mathbb{N},\ d\cdot k\cdot l=n} f(d) \cdot g(k) \cdot h(l)$. Analogicznie pokazujemy, że $[(f * g) * h](n) = \sum_{d,k,l\in\mathbb{N},\ d\cdot k\cdot l=n} f(d) \cdot g(k) \cdot h(l)$, więc z dowolności n mamy tezę. □

Z algebraicznego punktu widzenia uzyskane rezultaty pokazują, że struktura algebraiczna $(\mathbb{A}, +, *, 0, e)$ jest przemiennym pierścieniem łącznym z jedynką, którą jest funkcja e.

Stwierdzenie 20.9. *Dla dowolnych $f, g \in \mathbb{A}$ z tego, że $f \neq 0$ i $g \neq 0$ wynika, że $f * g \neq 0$.*

Dowód. Z zasady minimum istnieje najmniejsza liczba naturalna a taka, że $f(a) \neq 0$ i istnieje najmniejsza liczba naturalna b taka, że $g(b) \neq 0$. Niech $n = a \cdot b$ i niech $d \in \mathbb{N}$ oraz $d \mid n$. Jeśli $d < a$, to $f(d) = 0$, skąd $f(d) \cdot g(n/d) = 0$. Jeśli $d > a$, to $d \cdot b > a \cdot b = n$, skąd $n/d < b$ i $g(n/d) = 0$ oraz $f(d) \cdot g(n/d) = 0$. Wobec tego na mocy wzoru (20.1) mamy, że $(f * g)(n) = f(a) \cdot g(b) \neq 0$, a zatem $f * g \neq 0$. □

Powiemy, że funkcja arytmetyczna f jest **odwracalna**, jeżeli $f * g = e$ dla pewnego $g \in \mathbb{A}$. Zauważmy, że jeżeli $f * g = f * h = e$ dla pewnych $g, h \in \mathbb{A}$, to $h = h * e = h * (f * g) = (h * f) * g = e * g = g$. Z tego powodu funkcje arytmetyczną g taką, że $f * g = e$ nazywamy **funkcją odwrotną** do f i oznaczamy przez f^{-1}.

Stwierdzenie 20.10. *Funkcja arytmetyczna f jest odwracalna wtedy i tylko wtedy, gdy $f(1) \neq 0$.*

Dowód. Załóżmy, że f jest odwracalna. Wtedy $f * g = e$ dla pewnego $g \in \mathbb{A}$, skąd $(f * g)(1) = e(1) = 1$, ale $(f * g)(1) = f(1) \cdot g(1)$, więc stąd $f(1) \neq 0$.

Na odwrót, przypuśćmy, że $f(1) \neq 0$. Określamy $g(1) = \frac{1}{f(1)}$. Niech teraz $n > 1$ będzie taką liczbą naturalną, że $g(k)$ jest już zdefiniowane dla wszystkich liczb naturalnych $k < n$. Kładziemy

$$g(n) = -\frac{1}{f(1)} \cdot \sum_{d \in \mathbb{N},\ d \mid n, d > 1} f(d) \cdot g(n/d). \tag{20.3}$$

Dla tak zdefiniowanej indukcyjnie funkcji arytmetycznej g na mocy wzorów (20.1) i (20.3) mamy, że $(f * g)(n) = 0$ dla wszystkich $n > 1$. Ponadto $(f * g)(1) = f(1) \cdot g(1) = 1$. Stąd mamy, że $f * g = e$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

20.1 Funkcje multiplikatywne

Mówimy, że funkcja $f\colon \mathbb{N} \to \mathbb{C}$ jest **multiplikatywna**, jeżeli $f \neq 0$ oraz

$$f(a \cdot b) = f(a) \cdot f(b)$$

dla dowolnych liczb naturalnych a i b takich, że $\mathrm{NWD}(a, b) = 1$.

Przykład 20.11. Proste sprawdzenie pokazuje, że funkcje $\mathbb{I}$, 1 i e są multiplikatywne. Na mocy twierdzenia 10.16 funkcja Eulera φ też jest multiplikatywna.

Stwierdzenie 20.12. *Jeżeli funkcja $f \in \mathbb{A}$ jest multiplikatywna, to $f(1) = 1$ oraz*

$$f(a_1 \cdot \ldots \cdot a_n) = f(a_1) \cdot \ldots \cdot f(a_n)$$

dla dowolnych parami względnie pierwszych $a_1, \ldots, a_n \in \mathbb{N}$.

Dowód. Na mocy założenia $f \neq 0$, więc $f(n) \neq 0$ dla pewnego $n \in \mathbb{N}$. Ponieważ $\mathrm{NWD}(1, n) = 1$, więc $f(n) = f(n \cdot 1) = f(n) \cdot f(1)$, skąd po skróceniu przez $f(n)$ otrzymujemy $1 = f(1)$.

Drugą część stwierdzenia dowodzimy przez indukcję względem $n \geqslant 2$. Dla $n = 2$ teza wynika wprost z definicji funkcji multiplikatywnej. Przypuśćmy, że teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ i niech liczby naturalne $a_1, \ldots, a_n, a_{n+1}$ będą parami względnie pierwsze. Wtedy $\mathrm{NWD}(a_{n+1}, a_1 \cdot \ldots \cdot a_n) = 1$ na mocy stwierdzenia 8.49, więc $f(a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}) = f(a_1 \cdot \ldots \cdot a_n) \cdot f(a_{n+1})$. Ponadto, na mocy założenia indukcyjnego $f(a_1 \cdot \ldots \cdot a_n) = f(a_1) \cdot \ldots \cdot f(a_n)$, więc $f(a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}) = f(a_1) \cdot \ldots \cdot f(a_n) \cdot f(a_{n+1})$, co kończy dowód. □

Stwierdzenie 20.13. *Niezerowa funkcja arytmetyczna f jest multiplikatywna wtedy i tylko wtedy, gdy dla dowolnego $s \in \mathbb{N}$ i dla dowolnych różnych liczb pierwszych $p_1, \ldots, p_s$ oraz dla dowolnych nieujemnych liczb całkowitych $\alpha_1, \ldots, \alpha_s$ zachodzi wzór:*

$$f(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1^{\alpha_1}) \cdot \ldots \cdot f(p_s^{\alpha_s}). \tag{20.4}$$

Dowód. Jeśli f jest funkcją multiplikatywną, to wzór (20.4) wynika od razu ze stwierdzenia 20.12.

Na odwrót, niech $f \neq 0$ i f spełnia wzór (20.4) dla dowolnego $s \in \mathbb{N}$ i dla dowolnych różnych liczb pierwszych $p_1, \ldots, p_s$ oraz dla dowolnych nieujemnych liczb całkowitych $\alpha_1, \ldots, \alpha_s$. Weźmy dowolne $a, b \in \mathbb{N}$ takie, że $\mathrm{NWD}(a, b) = 1$. Wtedy istnieją różne liczby pierwsze $p_1, \ldots, p_t, q_1, \ldots, q_r$ oraz istnieją nieujemne liczby całkowite $\alpha_1, \ldots, \alpha_t$, $\beta_1, \ldots, \beta_r$ takie, że $a = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$ i $b = q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}$. Zatem ze wzoru (20.4) zastosowanego dla $s = t + r$ uzyskamy, że

$$f(a \cdot b) = f(p_1^{\alpha_1}) \cdot \ldots \cdot f(p_t^{\alpha_t}) \cdot f(q_1^{\beta_1}) \cdot \ldots \cdot f(q_r^{\beta_r}).$$

Ponadto ze wzoru (20.4) zastosowanego dla $s = t$ i $s = r$ otrzymamy odpowiednio, że $f(a) = f(p_1^{\alpha_1}) \cdot \ldots \cdot f(p_t^{\alpha_t})$ i $f(b) = f(q_1^{\beta_1}) \cdot \ldots \cdot f(q_r^{\beta_r})$. Wobec tego $f(a \cdot b) = f(a) \cdot f(b)$. □

Z twierdzenia 9.22 o postaci dzielników oraz ze stwierdzenia 20.13 mamy od razu następujące

Stwierdzenie 20.14. *Funkcja τ jest multiplikatywna.*

Lemat 20.15. *Dla dowolnych względnie pierwszych liczb naturalnych a i b funkcja $w\colon D_a \times D_b \to D_{ab}$ dana wzorem $w((x, y)) = x \cdot y$ jest bijekcją. W szczególności, każdy naturalny dzielnik liczby $a \cdot b$ można jednoznacznie zapisać w postaci $x \cdot y$, gdzie $x, y \in \mathbb{N}$ oraz $x \mid a$ i $y \mid b$.*

Dowód. Oczywiście $|D_a \times D_b| = |D_a| \cdot |D_b| = \tau(a) \cdot \tau(b)$ oraz $|D_{ab}| = \tau(a \cdot b)$. Stąd na mocy stwierdzenia 20.14 mamy, że $|D_a \times D_b| = |D_{ab}|$. Ponieważ zbiór D_{ab} jest skończony, więc wystarczy wykazać, że funkcja w jest różnowartościowa (oczywiste jest, że jeżeli $x \in D_a$ i $y \in D_b$, to $x \cdot y \in D_{ab}$). Jeśli $d \in \mathbb{N}$ jest wspólnym dzielnikiem liczb $x \in D_a$ i $y \in D_b$, to z przechodniości relacji podzielności $d \mid a$ i $d \mid b$, skąd $d = 1$, bo $\mathrm{NWD}(a, b) = 1$. Wobec tego $\mathrm{NWD}(x, y) = 1$.

Niech $x_1, x_2 \in D_a$ oraz $y_1, y_2 \in D_b$ będą takie, że $x_1 \cdot y_1 = x_2 \cdot y_2$. Wtedy $x_1 \mid x_2 \cdot y_2$, więc z $x_1 \mid x_2$ na mocy zasadniczego twierdzenia arytmetyki. Analogicznie pokazujemy, że $x_2 \mid x_1$. Stąd uzyskujemy, że $x_1 = x_2$ i w konsekwencji tego $y_1 = y_2$, czyli $(x_1, y_1) = (x_2, y_2)$, co kończy dowód. □

Twierdzenie 20.16. *Splot Dirichleta funkcji multiplikatywnych jest funkcją multiplikatywną.*

Dowód. Niech f i g będą funkcjami multiplikatywnymi. Wtedy $f(1) = 1$ i $g(1) = 1$, więc $(f * g)(1) = f(1) \cdot g(1) = 1$, skąd $f * g \neq 0$.

Weźmy dowolne $a, b \in \mathbb{N}$ takie, że $\mathrm{NWD}(a, b) = 1$. Na mocy lematu 20.15 i wzoru (20.1) mamy, że

$$(f * g)(a \cdot b) = \sum_{(x,y) \in D_a \times D_b} f(x \cdot y) \cdot g\left(\frac{a}{x} \cdot \frac{b}{y}\right).$$

Z dowodu lematu 20.15 wynika, że jeżeli $(x, y) \in D_a \times D_b$, to $\mathrm{NWD}(x, y) = 1$ i $\mathrm{NWD}\left(\frac{a}{x}, \frac{b}{y}\right) = 1$, więc $f(x \cdot y) = f(x) \cdot f(y)$ i $g\left(\frac{a}{x} \cdot \frac{b}{y}\right) = g\left(\frac{a}{x}\right) \cdot g\left(\frac{b}{y}\right)$. Wobec tego

$$(f * g)(a \cdot b) = \sum_{(x,y) \in D_a \times D_b} [f(x) \cdot g\left(\frac{a}{x}\right)] \cdot [f(y) \cdot g\left(\frac{b}{y}\right)].$$

Prawa strona ostatniego wzoru jest równa iloczynowi liczb $\sum\limits_{x \in \mathbb{N},\, x|a} f(x) \cdot g(a/x)$ i $\sum\limits_{y \in \mathbb{N},\, y|b} f(y) \cdot g(b/y)$, czyli jest równa $(f * g)(a) \cdot (f * g)(b)$. Wobec tego $(f * g)(a \cdot b) = (f * g)(a) \cdot (f * g)(b)$. □

Wniosek 20.17. *Dla dowolnej funkcji multiplikatywnej f funkcja $D(f)$ dana wzorem $(D(f))(n) = \sum\limits_{d \in D_n} f(d)$ dla $n \in \mathbb{N}$ też jest multiplikatywna.*

Dowód. Funkcja 1 jest multiplikatywna, więc na mocy twierdzenia 20.16 funkcja $f * 1$ jest multiplikatywna. Ponadto $1(k) = 1$ dla każdego $k \in \mathbb{N}$, więc na mocy wzoru (20.1) uzyskujemy, że $(f * 1)(n) = \sum\limits_{d \in D_n} f(d)$ dla $n \in \mathbb{N}$, czyli $D(f) = f * 1$. □

Stwierdzenie 20.18. *Funkcja σ jest multiplikatywna.*

Dowód. Z przykładu 20.5 wiemy, że $\sigma = \mathbb{I} * 1$. Ponadto funkcje $\mathbb{I}$ oraz 1 są multiplikatywne na mocy przykładu 20.11. Stąd na mocy twierdzenia 20.16 mamy tezę. □

Stwierdzenie 20.19. *Dla dowolnych różnych liczb pierwszych* $p_1, \ldots, p_s$ *i dla dowolnych* $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ *zachodzi wzór:*

$$\sigma(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

Dowód. Na mocy stwierdzeń 20.18 i 20.13 wystarczy wykazać, że $\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$ dla dowolnych $p \in \mathbb{P}$ i $k \in \mathbb{N}_0$. Jednak na mocy twierdzenia 9.22 mamy, że $D_{p^\alpha} = \{1, p, \ldots, p^\alpha\}$, więc $\sigma(p^\alpha) = 1 + p + \ldots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$, co kończy nasz dowód.

□

Twierdzenie 20.20. *Dla dowolnej liczby naturalnej* n *zachodzi wzór:*

$$\sum_{d \in D_n} \varphi(d) = n. \tag{20.5}$$

Dowód. Ponieważ $(D(\varphi))(n) = \sum_{d \in D_n} \varphi(d)$ i na mocy przykładu 20.11 funkcja φ jest multiplikatywna, więc z wniosku 20.17 uzyskujemy, że funkcja $D(\varphi)$ jest multiplikatywna. Ponadto funkcja $\mathbb{I}$ też jest multiplikatywna, więc dzięki stwierdzeniu 20.13 wzór $D(\varphi) = \mathbb{I}$ będzie udowodniony, gdy pokażemy, że $\sum_{d \in D_{p^k}} \varphi(d) = p^k$ dla dowolnych $p \in \mathbb{P}$ i $k \in \mathbb{N}$. Ponadto na mocy twierdzenia 10.18 mamy, że $\varphi(p^s) = p^{s-1} \cdot (p-1)$ dla każdego $s \in \mathbb{N}$, więc $\sum_{d \in D_{p^k}} \varphi(d) = 1 + (p-1) + p \cdot (p-1) + \ldots + p^{k-1} \cdot (p-1) = 1 + (p-1) \cdot (1 + p + \ldots + p^{k-1}) = 1 + p^k - 1 = p^k$, co kończy nasz dowód. □

20.2 Funkcja Möbiusa

Funkcją Möbiusa nazywamy funkcję arytmetyczna μ zdefiniowaną w sposób następujący: $\mu(1) = 1$, $\mu(n) = 0$, jeśli istnieje liczba pierwsza p taka, że $p^2 \mid n$ oraz $\mu(p_1 \cdot \ldots \cdot p_k) = (-1)^k$, jeśli $p_1, \ldots, p_k$ są różnymi liczbami pierwszymi.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Przykład 20.21. Wprost z definicji mamy, że $\mu(5!) = 0$, bo $2^2 \mid 5!$ oraz $\mu(21 \cdot 22 \cdot 23) = \mu(3 \cdot 7 \cdot 2 \cdot 11 \cdot 23) = (-1)^5 = -1$. Ponadto, jeśli $p \in \mathbb{P}$, to $\mu(p) = -1$ i $\mu(p^k) = 0$ dla każdej liczby naturalnej $k \geqslant 2$. Zatem $\sum_{k=0}^{n} \mu(p^k) = 1 - 1 + 0 = 0$ dla każdej liczby naturalnej n.

Stwierdzenie 20.22. *Funkcja Möbiusa μ jest multiplikatywna.*

Dowód. Ponieważ $\mu(1) = 1$, więc $\mu \neq 0$. Weźmy dowolne względnie pierwsze liczby naturalne a i b. Jeżeli $a = 1$ lub $b = 1$, to oczywiście $\mu(a \cdot b) = \mu(a) \cdot \mu(b)$. Niech dalej $a > 1$ i $b > 1$. Jeżeli istnieje $q \in \mathbb{P}$ taka, że $q^2 \mid a$, to $q^2 \mid a \cdot b$, skąd $\mu(a \cdot b) = 0$ i $\mu(a) = 0$, więc $\mu(a \cdot b) = \mu(a) \cdot \mu(b)$. Podobnie, jeśli $q^2 \mid b$ dla pewnego $q \in \mathbb{P}$, to też $\mu(a \cdot b) = \mu(a) \cdot \mu(b)$. Z twierdzenia o jednoznaczności rozkładu wynika, że pozostaje do rozważenia przypadek, gdy $a = p_1 \cdot \ldots \cdot p_s$ dla pewnych różnych liczb pierwszych $p_1, \ldots, p_s$ oraz $b = q_1 \cdot \ldots \cdot q_r$ dla pewnych różnych liczb pierwszych $q_1, \ldots, q_r$. Ponadto $\mathrm{NWD}(a, b) = 1$, więc liczby $p_1, \ldots, p_s, q_1, \ldots, q_r$ są różne i stąd $\mu(a \cdot b) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(a) \cdot \mu(b)$. □

Stwierdzenie 20.23. *Funkcja Möbiusa μ jest odwrotnością funkcji 1, czyli $\mu * 1 = e$. W szczególności dla dowolnej liczby naturalnej $n > 1$ zachodzi wzór:*

$$\sum_{d \in D_n} \mu(d) = 0. \tag{20.6}$$

Dowód. Funkcja 1 jest multiplikatywna i funkcja μ na mocy stwierdzenia 20.22 jest multiplikatywna. Stąd i z twierdzenia 20.16 wynika, że funkcja $\mu * 1$ jest multiplikatywna. Ponadto funkcja e jest multiplikatywna. Wobec tego na mocy twierdzenia o jednoznaczności rozkładu i stwierdzenia 20.13 wystarczy pokazać, że $(\mu * 1)(p^k) = e(p^k)$ dla dowolnych $p \in \mathbb{P}$ i $k \in \mathbb{N}$. Wiemy też, że $(\mu * 1)(n) = (D(\mu))(n) = \sum_{d \in D_n} \mu(d)$ dla każdego $n \in \mathbb{N}$ oraz $e(n) = 0$ dla $n > 1$. Dalej, na mocy przykładu 20.21 mamy, że $\sum_{d \in D_{p^k}} \mu(d) = 0$, a to oznacza, ze dowód naszego twierdzenia został zakończony. □

Następne twierdzenie nazywane jest **twierdzeniem Möbiusa o odwracaniu**.

Twierdzenie 20.24. *Niech f będzie funkcją arytmetyczną i niech $F(n) = \sum_{d\in D_n} f(d)$ dla każdego $n \in \mathbb{N}$. Wtedy $f(n) = \sum_{d\in D_n} \mu(d) \cdot F(n/d)$ dla każdego $n \in \mathbb{N}$. Ponadto funkcja F jest multiplikatywna wtedy i tylko wtedy, gdy funkcja f jest multiplikatywna.*

Dowód. Z definicji funkcji F wynika, że $F = f * 1$. Stąd $F * \mu = (f*1)*\mu = f*(1*\mu) = f*e = f$ na mocy stwierdzeń 20.8 i 20.6 oraz 20.23. Z tych wzorów na mocy twierdzenia 20.16 i na mocy multiplikatywności funkcji 1 i μ wynika, że funkcja F jest multiplikatywna wtedy i tylko wtedy, gdy funkcja f jest multiplikatywna. Ponadto ze wzoru (20.1) dla dowolnego $n \in \mathbb{N}$ mamy $f(n) = (F * \mu)(n) = (\mu * F)(n) = \sum_{d\in D_n} \mu(d) \cdot F(n/d)$. □

Ćwiczenie 20.25. Niech n będzie liczbą naturalną. Udowodnij, że $\tau(n)$ jest liczbą nieparzystą wtedy i tylko wtedy, gdy n jest kwadratem liczby naturalnej.

Ćwiczenie 20.26. Niech n będzie liczbą naturalną. Udowodnij, że $\sigma(n)$ jest liczbą nieparzystą wtedy i tylko wtedy, gdy n jest kwadratem liczby naturalnej lub podwojonym kwadratem liczby naturalnej.

Ćwiczenie 20.27. Niech n oraz k będą liczbami naturalnymi. Udowodnij, że $\varphi(n^k) = n^{k-1}\varphi(n)$.

Ćwiczenie 20.28. Rozwiąż równania:
(a) $\varphi(n) = 12$, (b) $\varphi(n) = \frac{n}{2}$.

Ćwiczenie 20.29. Dla jakich liczb naturalnych n, liczba $\varphi(n)$ dzieli n?

20.3 Liczby doskonałe

Liczbę naturalną n, która jest równa sumie wszystkich swoich dodatnich dzielników mniejszych od n nazywamy **liczbą doskonałą**. Pro-

blem liczb doskonałych swoją historią sięga czasów antycznych. Pierwsze zapiski w tym temacie przypisuje się Euklidesowi, który w swoich *Elementach* około 300 r. p.n.e. napisał:

> „Jeśli wziąć dowolnie dużo liczb, z których pierwsza jest jedynką, a każda następna jest dwa razy większa od poprzedniej i dodać je do siebie to, jeśli w wyniku otrzyma się liczbę pierwszą, to liczba ta pomnożona przez ostatnią w tym szeregu będzie liczbą doskonałą".

Pierwsze cztery liczby doskonałe, czyli 6, 28, 496, 8128 można uzyskać tym sposobem i były one znane już w starożytności. Kolejną odkryto dopiero w 1456 roku. W międzyczasie Nikomachos z Gerazy sformułował kilka hipotez. W przełożeniu na język współczesny brzmiałyby one następująco:
(1) n-ta liczba doskonała ma n cyfr.
(2) Wszystkie liczby doskonałe są parzyste.
(3) Wszystkie liczby doskonałe kończą się na 6 oraz 8 naprzemiennie.
(4) Algorytm Euklidesa generujący liczby doskonałe tworzy wszystkie liczby doskonałe (inaczej: Każda liczba doskonała jest postaci $2^{k-1}(2^k-1)$*, dla pewnego* $k>1$*, gdzie* 2^k-1 *jest liczbą pierwszą).*
(5) Istnieje nieskończenie wiele liczb doskonałych.

Obecnie znamy 51 liczb doskonałych. Już piąta z nich równa 33550336 pozwala obalić hipotezę (1), a szósta równa 8589869056 obala (3). Pozostałe hipotezy natomiast wciąż stanowią wyzwanie dla współczesnej matematyki.

Stwierdzenie 20.30. *Liczba naturalna n jest doskonała wtedy i tylko wtedy, gdy* $\sigma(n)=2n$*.*

Dowód. $\Rightarrow$. Jeśli n jest liczbą doskonałą, to $n>1$ i $n=\sum\limits_{d\in D_n\setminus\{n\}} d$, więc $2n=n+\sum\limits_{d\in D_n\setminus\{n\}} d=\sum\limits_{d\in D_n} d=\sigma(n)$. Zatem $\sigma(n)=2n$.

$\Leftarrow$. Niech $\sigma(n)=2n$. Wtedy $n>1$ oraz $2n=\sum\limits_{d\in D_n} d$, skąd $n=$ $=\sum\limits_{d\in D_n} d-n=\sum\limits_{d\in D_n\setminus\{n\}} d$. Zatem liczba n jest doskonała. □

Udowodnimy teraz, że zacytowany we wstępie algorytm Euklidesa wyznaczania parzystych liczb doskonałych jest poprawny. Wynika to z następujących trzech twierdzeń:

Twierdzenie 20.31. (Euklidesa). *Jeśli* 2^n-1 *dla pewnego* $n \in \mathbb{N}$ *jest liczbą pierwszą, to* $2^{n-1}(2^n-1)$ *jest liczbą doskonałą.*

Dowód. Ponieważ 2^n-1 jest nieparzystą liczbą pierwszą, więc na mocy stwierdzenie 20.19 mamy, że $\sigma(2^{n-1}\cdot(2^n-1)) = \frac{2^n-1}{2-1}\cdot\frac{(2^n-1)^2-1}{(2^n-1)-1} = (2^n-1)\cdot(2^n-1+1) = 2^n\cdot(2^n-1) = 2\cdot 2^{n-1}\cdot(2^n-1)$. Zatem na mocy stwierdzenia 20.30 liczba $2^{n-1}(2^n-1)$ jest doskonała. □

Twierdzenie 20.32. (Cataldi'ego-Fermata). *Jeżeli* 2^n-1 *dla pewnego* $n \in \mathbb{N}$ *jest liczbą pierwszą, to* n *jest liczbą pierwszą.*

Dowód. Jeżeli $n = 1$ to $2^n - 1 = 1 \notin \mathbb{P}$. Załóżmy, że n jest liczbą złożoną. Możemy ją wtedy zapisać jako $n = kl$, gdzie $k, l \in \mathbb{N}$, $k, l > 1$. Ale $2^n - 1 = 2^{kl} - 1 = (2^k-1)((2^k)^{l-1} + \ldots + 2^k + 1)$, więc $(2^k-1)|(2^n-1)$. Ponadto $1 < 2^k-1 < 2^n-1$, bo $1 < k < n$, czyli otrzymujemy sprzeczność z założeniem o pierwszości liczby 2^n-1. Wobec tego n jest liczbą pierwszą. □

Uwaga 20.33. Warto zaznaczyć, że twierdzenie odwrotne jest fałszywe, na przykład, $11 \in \mathbb{P}$, ale $2^{11} - 1 = 2047 = 23 \cdot 89 \notin \mathbb{P}$.

Liczby pierwsze postaci $2^n - 1$ dla $n \in \mathbb{N}$ nazywamy **liczbami pierwszymi Mersenne'a**. Obecnie (tak, jak liczb doskonałych) znamy ich 51. Pierwsze cztery, czyli 3, 7, 31, 127, znano już w starożytności. Kolejną, równą $8191 = 2^{13}-1$ odkryto dopiero w 1456 roku. Nie jest znany jednak odkrywca. Następne dwie liczby: $131071 = 2^{17} - 1$ oraz $524287 = 2^{19}-1$ przedstawił w 1588 roku Cataldi. Niecałe 200 lat później, w roku 1772 kolejną „cegiełkę" dołożył sam Euler dowodząc pierwszości liczby $2147483647 = 2^{31} - 1$. Dziewiątą liczbę Mersenne'a, czyli $2^{61}-1$, odkrył w 1883 roku Iwan Perwuszin. Kolejne dwie, $2^{89}-1$ oraz $2^{107} - 1$ są dziełem pracy Ralpha Ernesta Powersa kolejno z 1911 i 1914 roku. Co ciekawe, następna co do wielkości liczba Mersenne'a,

czyli $2^{127} - 1$ była znana jeszcze przed trzema jej poprzedniczkami, gdyż pierwszość tej liczby udowodnił w 1876 roku Lucas. Rok 1952 przyniósł matematycznemu światu aż pięć nowych liczb Mersenne'a. Wszystkie z nich zostały odkryte przez Raphaela Mitchela Robinsona, a wynoszą kolejno: $2^{521} - 1$, $2^{607} - 1$, $2^{1279} - 1$, $2^{2203} - 1$, $2^{2281} - 1$. Pięć lat później za pomocą komputera BESK szwedzki matematyk Hans Riesel rozszerzył zbiór liczb pierwszych Mersenne'a o osiemnastą już z kolei, wynoszącą $2^{3217} - 1$. Następne dwie, $2^{4253} - 1$ oraz $2^{4423} - 1$ odkrył 3 listopada 1961 roku Alexander Hurwitz. Obie z nich w zapisie dziesiętnym składają się z ponad 1000 cyfr. Kolejnym poszukiwaczem był Donald Bruce Gillies, który w 1963 roku dowiódł pierwszości liczb $2^{9689} - 1$, $2^{9941} - 1$ i $2^{11213} - 1$. Jego następcą został w 1971 roku Bryant Tuckerman, odkrywca liczby $2^{19937} - 1$. Swoje zasługi w tej dziedzinie miał też Landon Curt Noll, który, początkowo razem z Laurą Nickel w 1978 roku, a rok później sam, skutecznie poddał testowi pierwszości $2^{21701} - 1$ i $2^{23209} - 1$. Lata 1979-1996 to okres ciężkiej pracy Davida Slowinskiego. W tym czasie udało mu się odkryć siedem liczb pierwszych Mersenne'a. W poszukiwaniu pierwszej z nich, równej $2^{44497} - 1$, pomógł mu Harry Lewis Nelson. Kolejne trzy: $2^{86243} - 1$, $2^{110503} - 1$, $2^{132049} - 1$, są owocem jego samodzielnych badań. Nie poprzestał jednak na tym, gdyż współpracując z Paulem Gagem, dowiedli pierwszości liczb $2^{756839} - 1$, $2^{859433} - 1$ oraz $2^{1257787} - 1$. W międzyczasie 28 stycznia 1988 roku Walt Colquitt i Luke Welsch odkryli dwudziestą dziewiątą liczbę pierwszą Mersenne'a wynoszącą $2^{110503} - 1$. W 1996 roku wystartował Great Internet Mersenne Prime Search (GIMPS). Jest to projekt obliczeń rozproszonych, czyli wykorzystujący współdzielenie zasobów obliczeniowych. Dzięki temu wolontariusze z całego świata przy użyciu powszechnie dostępnego oprogramowania, podejmują się szukania kolejnych liczb pierwszych Mersenne'a. Inicjatywa trwa do dziś i to właśnie jej członkowie przyczyniają się do kolejnych odkryć. Największą obecnie odkrytą 7 grudnia 2018 w ten sposób liczbą jest $2^{82589933} - 1$, która w zapisie dziesiętnym składa się z 24862048 cyfr.

Jak w ogóle sprawdzane są tak ogromne liczby? Używa się w tym celu testu Lucasa-Lehmera [19]. Przyjmijmy $t_1 = 4$ oraz $t_k = {t_{k-1}}^2 - 2$

dla $k \geqslant 2$. Liczba M_p jest pierwsza wtedy i tylko wtedy, gdy $t_{p-1} \equiv 0 \pmod{M_p}$.

Przykład 20.34. Rozpatrzmy $M_7 = 127$. Wtedy:
$t_1 = 4$,
$t_2 = 4^2 - 2 = 14$,
$t_3 = 14^2 - 2 = 194 \equiv 67 \pmod{127}$,
$t_4 = 67^2 - 2 = 4487 \equiv 42 \pmod{127}$,
$t_5 = 42^2 - 2 = 1762 \equiv 111 \pmod{127}$,
$t_6 = 111^2 - 2 = 12319 \equiv 0 \pmod{127}$.
Zatem $M_7 = 2^7 - 1 = 127$ jest liczbą pierwszą.

Twierdzenie 20.35. (Eulera). *Jeśli k jest parzystą liczbą doskonałą, to istnieje liczba pierwsza p taka, że $k = 2^{p-1}(2^p - 1)$, gdzie $2^p - 1$ jest liczbą pierwszą Mersenne'a.*

Dowód. Zastosujemy pomysł Dicksona z [10]. Oczywiście $k = 2^{n-1}m$ dla pewnej liczby naturalnej $n > 1$ i dla pewnej nieparzystej liczby naturalnej m. Jako, że $2 \nmid m$, zatem liczby m oraz 2^{n-1} są względnie pierwsze. Stąd na mocy stwierdzeń 20.18 i 20.19,

$$\sigma(k) = \sigma(2^{n-1}m) = \sigma(2^{n-1})\sigma(m) = \frac{2^n - 1}{2 - 1}\sigma(m) = (2^n - 1)\sigma(m).$$

Liczba k jest doskonała, więc ze stwierdzenia 20.30, $\sigma(k) = 2k = 2(2^{n-1}m) = 2^n m$. Zatem otrzymujemy, że $2^n m = (2^n - 1)\sigma(m)$. Stąd

$$\sigma(m) = \frac{2^n m}{2^n - 1} = \frac{((2^n - 1) + 1)m}{2^n - 1} = m + \frac{m}{2^n - 1}.$$

Wobec tego $\frac{m}{2^n-1} \in \mathbb{Z}$, skąd wynika, że $2^n - 1 \in D_m$, a więc także $\frac{m}{2^n-1} \in D_m$. Ale $n > 1$, więc $\frac{m}{2^n-1} < m$, przy czym $\sigma(m) = m + \frac{m}{2^n-1}$, więc ponieważ $\sigma(m) = m + \sum_{d \in D_m \setminus \{m\}} d$ oraz $m > 1$ i $1 \in D_m$, to $|D_m| = 2$ i $\frac{m}{2^n-1} = 1$. Stąd $2^n - 1 = m \in \mathbb{P}$ i na mocy twierdzenia 20.32, $n \in \mathbb{P}$, co kończy dowód, gdyż $k = 2^{n-1}(2^n - 1)$. □

Problem istnienia nieparzystej liczby doskonałej jest nadal otwarty. Oto wypowiedzi niektórych wybitnych matematyków na ten temat [20]:

Leonard Euler: „Pytanie, czy istnieją nieparzyste liczby doskonałe, jest najtrudniejsze".

Chris Caldwell: „To prawdopodobnie najstarszy nierozwiązany problem w matematyce".

Jay Goldman: „Prawdopodobnie najstarszy nierozwiązany problem w teorii liczb oraz prawdopodobnie w całej matematyce".

Stan Wagon: „Może jakaś prosta kombinacja kilkunastu liczb pierwszych faktycznie daje nieparzystą liczbę doskonałą".

Thomas Milton Putnam: „Jest to problem o dużym znaczeniu historycznym".

Paulo Ribenboim: „Jest to pytanie, które zostało obszernie zbadane, jednak odpowiedź na to pytanie jest wciąż nieznana"oraz „Wierzę, że problem jest jak forteca nie do zdobycia. Wszyscy wiedzą, że to prawdopodobnie dzięki szczęściu nieparzysta liczba doskonała zostałaby odkryta. Z drugiej strony nic, co zostało udowodnione, nie stwierdza, że nieparzysta liczba doskonała nie istnieje. Potrzebne są nowe pomysły."

Zacytujemy teraz kilka znanych twierdzeń dotyczących nieparzystej liczby doskonałej. Pierwszy z nich, to twierdzenie J. A. Holdener podane w [18].

Twierdzenie 20.36. *Nie istnieje nieparzysta liczba doskonała postaci* $6k - 1$.

Następny rezultat to **twierdzenie Eulera o nieparzystych liczbach doskonałych** (por. [11]).

Twierdzenie 20.37. *Niech n będzie nieparzystą liczbą doskonałą. Wówczas istnieje dokładnie jedna liczba pierwsza $p \equiv 1 \pmod 4$, która wchodzi w rozkład kanoniczny liczby n z wykładnikiem $\alpha \equiv 1 \pmod 4$ i pozostałe czynniki pierwsze liczby n wchodzą w jej rozkład kanoniczny z wykładnikami parzystymi.*

Następny rezultat nazywamy **twierdzeniem Toucharda** (por. [18]).

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Twierdzenie 20.38. *Niech n będzie nieparzystą liczbą doskonałą. Jeżeli $3 \nmid n$, to $n \equiv 1 \pmod{12}$. Jeżeli zaś $3 \mid n$, to $n \equiv 9 \pmod{36}$. W szczególności $n \equiv 1, 9, 13, 25 \pmod{36}$.*

Następne twierdzenie zostało odkryte i udowodnione przez Peirce'a w [31].

Twierdzenie 20.39. *Każda nieparzysta liczba doskonała posiada co najmniej cztery różne dzielniki pierwsze.*

Następne ważne twierdzenie pochodzi od Sylvestera (patrz [13]).

Twierdzenie 20.40. *Jeżeli nieparzysta liczba doskonała n jest podzielna przez 17, to n posiada dzielnik pierwszy $q \geqslant 67$.*

A teraz słynne **twierdzenie Sylvestera o liczbach doskonałych**:

Twierdzenie 20.41. *Każda nieparzysta liczba doskonała posiada co najmniej pięć różnych czynników pierwszych.*

Już w 1957 roku Kanold udowodnił, że nieparzysta liczba doskonała musi być większa niż 10^{20}. W 1973 roku Tuckerman zwiększył tę liczbę do 10^{36}, a jeszcze w tym samym roku Hagis podniósł poprzeczkę do 10^{50}. W 1989 roku oszacowanie to wzrosło do 10^{160}, co jest zasługą dwóch matematyków, Cohena i Brenta. Drugi z nich już dwa lata później pokazał, że najmniejsza nieparzysta liczba doskonała musi być większa od 10^{300}. Dzisiaj wiemy, że nie może być ona mniejsza niż 10^{1500}, co w 2012 roku udowodnili Ochem i Rao. Obecnie wiemy, że różnych dzielników pierwszych nieparzystej liczby doskonałej jest co najmniej dziewięć, co udowodnił Nielsen w 2006 roku.

Rozdział 21

Pierwiastki pierwotne

21.1 Pojęcia wstępne

Sformalizujemy i usystematyzujemy najpierw pojęcia omawiane przez nas w podrozdziale 10.3. Dla $m \in \mathbb{N}$ oznaczmy przez R_m zbiór wszystkich $a \in \mathbb{Z}$ takich, że $\mathrm{NWD}(a, m) = 1$. Oczywiście $R_m = \{u + km : u \in \mathbb{Z}_m^*, k \in \mathbb{Z}\}$. Na mocy stwierdzenia 8.49 $a_1 \cdot \ldots \cdot a_s \in R_m$ dla dowolnych $a_1, \ldots, a_s \in R_m$.

Definicja 21.1. Niech $m \in \mathbb{N}$ i niech $a \in R_m$. Najmniejszą liczbę naturalną k taką, że $a^k \equiv 1 \pmod{m}$ nazywamy **rzędem liczby** a **modulo** m. Rząd liczby a modulo m oznaczamy symbolem $w_m(a)$.

Istnienie $w_m(a)$ wynika z twierdzenia 10.13 i z zasady minimum.

Stwierdzenie 21.2. *Niech $m \in \mathbb{N}$ i niech $a \in R_m$. Wówczas:*
(i) jeśli $b \in \mathbb{Z}$ i $b \equiv a \pmod{m}$, to $b \in R_m$ oraz $w_m(b) = w_m(a)$,
(ii) dla każdego $k \in \mathbb{N}$: $a^k \equiv 1 \pmod{m} \iff w_m(a) \mid k$,
(iii) $w_m(a) \mid \varphi(m)$,
(iv) jeżeli $b \in R_m$ oraz liczby $w_m(a)$ i $w_m(b)$ są względnie pierwsze, to $w_m(a \cdot b) = w_m(a) \cdot w_m(b)$,
(v) dla dowolnych $k, l \in \mathbb{N}$: $a^k \equiv a^l \pmod{m} \iff k \equiv l \pmod{w_m(a)}$.

Dowód. Dowody podpunktów $(i) - (iii)$ były przedstawione w podrozdziale 10.3. (iv). Na mocy (ii) mamy, że $a^{w_m(a)\cdot w_m(b)} \equiv 1 \pmod{m}$ i $b^{w_m(a)\cdot w_m(b)} \equiv 1 \pmod{m}$, więc $(a \cdot b)^{w_m(a)\cdot w_m(b)} \equiv 1 \pmod{m}$. Stąd $w_m(a \cdot b) \mid w_m(a) \cdot w_m(b) = k$. Ponadto $(a \cdot b)^k \equiv 1 \pmod{m}$, więc po podniesieniu tej kongruencji stronami do potęgi $w_m(a)$ i uwzględnieniu tego, że $a^{w_m(a)} \equiv 1 \pmod{m}$ dostaniemy, że $b^{k\cdot w_m(a)} \equiv 1 \pmod{m}$. Zatem $w_m(b) \mid k \cdot w_m(a)$ na mocy (ii), więc z zasadniczego twierdzenia arytmetyki $w_m(b) \mid k$. Podobnie pokazujemy, że $w_m(a) \mid k$, a ponieważ liczby $w_m(a)$ i $w_m(b)$ są względnie pierwsze, więc $w_m(a) \cdot w_m(b) \mid k$, co wobec $k \mid w_m(a) \cdot w_m(b)$ daje tezę.

(v). Bez zmniejszania ogólności możemy zakładać, że $k \geqslant l$. Wtedy $k - l \in \mathbb{N}_0$ i na mocy twierdzenia 10.6, $a^k \equiv a^l \pmod{m}$ wtedy i tylko wtedy, gdy $a^{k-l} \equiv 1 \pmod{m}$, co na mocy (ii) jest równoważne temu, że $k \equiv l \pmod{w_m(a)}$. □

Przykład 21.3. Udowodnimy, że dla dowolnego $n \in \mathbb{N}_0$ każdy dzielnik pierwszy p liczby Fermata $F_n = 2^{2^n} + 1$ jest postaci $p = 2^{n+1}k + 1$ dla pewnego $k \in \mathbb{N}_0$. Oczywiście $p > 2$ i $\varphi(p) = p - 1$ oraz $2^{p-1} \equiv 1 \pmod{p}$. Zatem $w_p(2) \mid p - 1$ na mocy stwierdzenia 21.2. Ponadto $2^{2^n} \equiv -1 \pmod{p}$, więc po podniesieniu tej kongruencji do kwadratu uzyskamy, że $2^{2^{n+1}} \equiv 1 \pmod{p}$. Stąd znowu na mocy stwierdzenia 21.2, $w_p(2) \mid 2^{n+1}$. Zatem $w_p(2) = 2^l$ dla pewnego $l \in \{0, 1, \ldots, n+1\}$. Jeśli $l \leqslant n$, to $2^l \equiv 1 \pmod{p}$ i po podniesieniu tej kongruencji stronami do potęgi 2^{n-l} uzyskamy, że $2^{2^n} \equiv 1 \pmod{p}$. Ale $2^{2^n} \equiv -1 \pmod{p}$, więc stąd $1 \equiv -1 \pmod{p}$, czyli $p \mid 2$, co prowadzi do sprzeczności. Wobec tego $l = n + 1$ i $w_p(2) = 2^{n+1}$ oraz $2^{n+1} \mid p - 1$, czyli $p = 2^{n+1}k + 1$ dla pewnego $k \in \mathbb{N}_0$.

Ćwiczenie 21.4. Niech $p, q \in \mathbb{P}$. Udowodnij, że jeżeli $q \mid 2^p - 1$, to $w_q(2) = p$ i $q = kp + 1$ dla pewnego $k \in \mathbb{N}$.

Ćwiczenie 21.5. Uzasadnij, że $w_{11}(9) = 5$, a następnie udowodnij, że $x \in \mathbb{N}_0$ spełnia kongruencję $9^x \equiv x \pmod{11}$ wtedy i tylko wtedy, gdy $x \equiv 3, 31, 37, 45, 49 \pmod{55}$.

Stwierdzenie 21.6. *Niech $m, k \in \mathbb{N}$ i $a \in \mathbb{Z}_m^*$. Wtedy*

$$w_m(a^k) = \frac{w_m(a)}{\mathrm{NWD}(w_m(a), k)}.$$

W szczególności, jeśli $k \mid w_m(a)$, *to* $w_m(a^k) = \frac{w_m(a)}{k}$.

Dowód. Oznaczmy $d = \mathrm{NWD}(w_m(a), k)$ i $u = w_m(a^k)$. Wtedy na mocy twierdzenia 8.32 $w_m(a) = dw$ i $k = dk_1$ dla pewnych względnie pierwszych liczb naturalnych w i k_1. Zauważmy, że $(a^k)^w = a^{kw} = a^{w_m(a)k_1} \equiv 1 \pmod{m}$, więc ze stwierdzenia 21.2, $u \mid w$. Dalej, $1 \equiv (a^k)^u \equiv a^{ku} \equiv a^{dk_1u} \pmod{m}$, więc znowu na mocy stwierdzenia 21.2, $w_m(a) \mid dk_1u$, czyli $dw \mid dk_1u$, więc $w \mid k_1u$ i z zasadniczego twierdzenia arytmetyki, $w \mid u$. Ale wcześniej pokazaliśmy, że $u \mid w$, więc $w_m(a^k) = u = w = \frac{w_m(a)}{\mathrm{NWD}(w_m(a),k)}$. □

W podrozdziale 10.3 dla liczby naturalnej m przez $\lambda(m)$ oznaczyliśmy najmniejszą liczbę naturalną k o tej własności, że $a^k \equiv 1 \pmod{m}$ dla każdego $a \in R_m$. Zatem λ jest funkcją arytmetyczną. Nazywamy ją **funkcją Carmichaela**.

Twierdzenie 21.7. *Dla dowolnej liczby naturalnej* m *w zbiorze* R_m *istnieje element maksymalnego rzędu modulo* m. *Jeżeli* $c \in R_m$ *jest elementem maksymalnego rzędu modulo* m, *to* $w_m(a) \mid w_m(c)$ *dla każdego* $a \in R_m$. *W szczególności* $a^{w_m(c)} \equiv 1 \pmod{m}$ *dla każdego* $a \in R_m$ *i* $w_m(c) = \lambda(m)$.

Dowód. Ponieważ $w_m(a) \mid \varphi(m)$ dla każdego $a \in R_m$, więc na mocy zasady maksimum w zbiorze $\{w_m(a) : a \in R_m\}$ istnieje liczba największa $k = w_m(c)$ dla pewnego $c \in R_m$. Przypuśćmy, że $w_m(a) \nmid k$ dla pewnego $a \in R_m$. Wtedy z twierdzenia o postaci dzielników liczby naturalnej wynika, że istnieje liczba pierwsza p oraz istnieją $\alpha, \beta \in \mathbb{N}_0$ takie, że $\alpha > \beta$, $w_m(a) = p^\alpha x$ i $w_m(c) = p^\beta y$ dla pewnych $x, y \in \mathbb{N}$ takich, że $p \nmid x$ i $p \nmid y$. Ze stwierdzenia 21.6 mamy, że $w_m(a^x) = p^\alpha$ i $w_m(c^{p^\beta}) = y$. Stąd i ze stwierdzenia 21.2 wynika, że $w_m(a^x \cdot c^{p^\beta}) = p^\alpha \cdot y > k = w_m(c)$, co prowadzi do sprzeczności z maksymalnością k. Zatem dla każdego $a \in R_m$ mamy, że $w_m(a) \mid w_m(c)$ i stąd $a^{w_m(c)} \equiv 1 \pmod{m}$ na mocy stwierdzenia 21.2. Teraz ze stwierdzenia 10.25 wynika, że $\lambda(m) \mid w_m(c)$ oraz $w_m(c) \mid \lambda(m)$, czyli $w_m(c) = \lambda(m)$. □

Definicja 21.8. Niech $m > 1$ będzie liczbą naturalną i niech $a \in R_m$. Jeżeli $w_m(a) = \varphi(m)$, to a będziemy nazywać **pierwotnym pierwiastkiem modulo** m.

Przykład 21.9. Z ćwiczenia 10.29 wynika, że 2 jest pierwotnym pierwiastkiem modulo 3^α dla każdego $\alpha \in \mathbb{N}$.

Z twierdzenia 21.7 i ze stwierdzenia 21.2 uzyskujemy od razu następujący

Wniosek 21.10. *Liczba naturalna $m > 1$ posiada pierwotny pierwiastek modulo m wtedy i tylko wtedy, gdy $\lambda(m) = \varphi(m)$.*

Z wniosku 21.10 i z twierdzeń 10.18 i 10.28 dostajemy od razu następujący

Wniosek 21.11. *Dla $\alpha \in \mathbb{N}$ istnieje pierwotny pierwiastek modulo 2^α wtedy i tylko wtedy, gdy $\alpha = 1$ lub $\alpha = 2$.*

Twierdzenie 21.12. *Jeżeli a jest pierwiastkiem pierwotnym modulo m, gdzie $m > 1$, to $\{[a^1]_m, [a^2]_m, \ldots, [a^{\varphi(m)}]_m\} = \mathbb{Z}_m^*$. Ponadto dla $k \in \mathbb{N}$ liczba a^k jest pierwiastkiem pierwotnym modulo m wtedy i tylko wtedy, gdy $\mathrm{NWD}(k, \varphi(m)) = 1$. W szczególności w zbiorze $\mathbb{Z}_m^*$ istnieje dokładnie $\varphi(\varphi(m))$ wszystkich pierwiastków pierwotnych modulo m.*

Dowód. Ponieważ $a \in R_m$, więc $a^k \in R_m$, a ponieważ $[a^k]_m \equiv a^k \pmod{m}$, więc $[a^k]_m \in \mathbb{Z}_m^*$ dla każdego $k = 1, 2, \ldots, \varphi(m)$. Stąd $\{[a^1]_m, [a^2]_m, \ldots, [a^{\varphi(m)}]_m\} \subseteq \mathbb{Z}_m^*$. Ponadto $|\mathbb{Z}_m^*| = \varphi(m)$, więc wystarczy wykazać, że liczby $[a^1]_m, [a^2]_m, \ldots, [a^{\varphi(m)}]_m$ są parami różne. Gdyby tak nie było, to istniałyby liczby naturalne i oraz j takie, że $i < j \leqslant \varphi(m)$ i $a^j \equiv a^i \pmod{m}$. Ale wtedy na mocy stwierdzenia 21.2 (v) mielibyśmy, że $j \equiv i \pmod{\varphi(m)}$, co prowadzi do sprzeczności. Wobec tego $\{[a^1]_m, [a^2]_m, \ldots, [a^{\varphi(m)}]_m\} = \mathbb{Z}_m^*$.

Zauważmy, że a^k jest pierwiastkiem pierwotnym modulo m wtedy i tylko wtedy, gdy $w_m(a^k) = w_m(a) = \varphi(m)$, co na mocy stwierdzenia 21.6 jest równoważne temu, że $\mathrm{NWD}(k, \varphi(m)) = 1$. Stąd i z pierwszej części dowodu w zbiorze $\mathbb{Z}_m^*$ istnieje dokładnie $\varphi(\varphi(m))$ wszystkich pierwiastków pierwotnych modulo m. □

21.2 Istnienie pierwiastków pierwotnych

W tym podrozdziale opiszemy wszystkie liczby naturalne $m > 1$ posiadające pierwiastek pierwotny modulo m.

Lemat 21.13. *Jeżeli liczba naturalna $m > 1$ posiada pierwiastek pierwotny modulo m, to $m \in \{2, 4\}$ lub $m = p^\alpha$ lub $m = 2p^\alpha$, gdzie $p \in \mathbb{P} \setminus \{2\}$ i $\alpha \in \mathbb{N}$.*

Dowód. Istnieją $s, \alpha_1, \ldots, \alpha_s \in \mathbb{N}$ i istnieją różne liczby pierwsze $p_1, \ldots, p_s$ takie, że $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Jeżeli $s = 1$ i $p_1 = 2$, to $\alpha_1 \in \{1, 2\}$ na mocy wniosku 21.11, czyli $m \in \{2, 4\}$ lub $m = p^\alpha$ dla pewnych $p \in \mathbb{P} \setminus \{2\}$ i $\alpha \in \mathbb{N}$.

Niech dalej $s \geqslant 2$. Wtedy z wniosku 10.27, $\lambda(m) = \mathrm{NWW}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s}))$, a z twierdzenia 10.18 mamy, że $\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1)$. Stąd i na mocy wniosku 21.10 uzyskujemy, że $\mathrm{NWW}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1)$. Ponadto na mocy stwierdzenia 10.25 i twierdzenia 10.18 dla każdego $i = 1, \ldots, s$ istnieje $c_i \in \mathbb{N}$ takie, że $p_i^{\alpha_i - 1}(p_i - 1) = \lambda(p_i^{\alpha_i}) \cdot c_i$. Zatem $\mathrm{NWW}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})) = [\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})] \cdot (c_1 \cdot \ldots \cdot c_s)$, skąd $c_1 \cdot \ldots \cdot c_s = 1$, więc $c_1 = \ldots = c_s = 1$, czyli $\lambda(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1)$ dla $i = 1, \ldots, s$ i $\mathrm{NWW}(p_1^{\alpha_1 - 1}(p_1 - 1), \ldots, p_s^{\alpha_s - 1}(p_s - 1)) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1)$. Wobec tego liczby $p_1^{\alpha_1 - 1}(p_1 - 1), \ldots, p_s^{\alpha_s - 1}(p_s - 1)$ są parami względnie pierwsze. Jeśli $s > 2$, to co najmniej dwie z tych liczb są parzyste, co prowadzi do sprzeczności. Wobec tego $s = 2$ i bez zmniejszania ogólności można zakładać, że $p_1 = 2$ oraz $p_2 = p > 2$. Ponadto, dla $\alpha_1 > 1$ liczby $2^{\alpha_1 - 1}$ i $p^{\alpha_2 - 1}(p - 1)$ są parzyste, więc dodatkowo $\alpha_1 = 1$. Zatem, $m = 2p^\alpha$ dla $\alpha = \alpha_2 \in \mathbb{N}$ i $p \in \mathbb{P} \setminus \{2\}$. □

Twierdzenie 21.14. *Każda liczba pierwsza p posiada pierwiastek pierwotny modulo p.*

Dowód. Z pierwszości p wynika, że $\mathbb{Z}_p^* = \{1, \ldots, p - 1\}$ i $\varphi(p) = p - 1$. Na mocy twierdzenia 21.7 istnieje $c \in \{1, \ldots, p - 1\}$ takie, że $a^{w_p(c)} \equiv 1 \pmod{m}$ dla każdego $a \in \mathbb{Z}_p^*$, więc $w_p(c) \mid p - 1$ na mocy stwierdzenia 21.2, skąd $w_p(c) \leqslant p - 1$. Wobec tego kongruencja $x^{w_p(c)} - 1 \equiv 0 \pmod{p}$ posiada dokładnie $p - 1$ rozwiązań, zaś z twierdzenia 10.32 wynika, że liczba rozwiązań tej kongruencji jest niewiększa niż $w_p(c)$, więc $p - 1 \leqslant w_p(c)$ i ostatecznie $w_p(c) = p - 1 = \varphi(p)$ i c jest pierwiastkiem pierwotnym modulo p. □

Twierdzenie 21.15. *Niech p będzie liczbą pierwszą. Jeżeli a jest pierwiastkiem pierwotnym modulo p, to a lub $a+p$ jest pierwiastkiem pierwotnym modulo p^2. W szczególności istnieje pierwiastek pierwotny modulo p^2.*

Dowód. Na mocy założenia $w_p(a) = p-1$. Oznaczmy $w_{p^2}(a) = n$. Wtedy $a^n \equiv 1 \pmod{p^2}$, skąd $a^n \equiv 1 \pmod{p}$, więc $p-1 \mid n$ na mocy stwierdzenia 21.2, czyli $n = (p-1)d$ dla pewnego $d \in \mathbb{N}$. Ale ze stwierdzenia 21.2 mamy też, że $n \mid \varphi(p^2) = p(p-1)$, więc $d \mid p$, skąd z pierwszości p, $n = p-1$ lub $n = p(p-1)$. Jeśli $n = p(p-1)$, to a jest pierwiastkiem pierwotnym modulo p^2. Niech dalej $n = p-1$. Wtedy $a^{p-1} \equiv 1 \pmod{p^2}$ i $a+p \equiv a \pmod{p}$, więc $a+p$ jest pierwiastkiem pierwotnym modulo p. Zatem z pierwszej części dowodu $w_{p^2}(a+p) = p-1$ lub $w_{p^2}(a+p) = p(p-1)$. Przypuśćmy, że $w_{p^2}(a+p) = p-1$. Wtedy $(a+p)^{p-1} \equiv 1 \pmod{p^2}$. Tymczasem ze wzoru dwumianowego Newtona $(a+p)^{p-1} \equiv a^{p-1} + (p-1)pa^{p-2} \pmod{p^2}$, więc ponieważ $a^{p-1} \equiv 1 \pmod{p^2}$, to otrzymamy stąd, że $1 - pa^{p-2} \equiv 1 \pmod{p^2}$. Zatem $p^2 \mid pa^{p-2}$, czyli $p \mid a^{p-2}$, więc $p \mid 1$ lub $p \mid a$, co prowadzi do sprzeczności. Wobec tego $w_{p^2}(a+p) = p(p-1)$ i $a+p$ jest pierwiastkiem pierwotnym modulo p^2.

Stąd i z twierdzenia 21.14 wynika, że istnieje pierwiastek pierwotny modulo p^2. □

Lemat 21.16. *Niech $p \in \mathbb{P} \setminus \{2\}$ i niech a będzie pierwiastkiem pierwotnym modulo p^2. Wówczas $a^{p-1} \equiv 1 + Up \pmod{p^2}$ dla pewnej liczby całkowitej U niepodzielnej przez p oraz dla dowolnej liczby naturalnej $k \geqslant 2$ jest $a^{p^{k-2}(p-1)} \equiv 1 + Up^{k-1} \pmod{p^k}$.*

Dowód. Na mocy założenia $w_{p^2}(a) = p(p-1)$, skąd $a^{p-1} \not\equiv 1 \pmod{p^2}$ i $a^{p(p-1)} \equiv 1 \pmod{p^2}$. Stąd $a^{p(p-1)} \equiv 1 \pmod{p}$, więc na mocy małego twierdzenia Fermata $a^{p-1} \equiv 1 \pmod{p}$. Zatem $a^{p-1} = 1 + Up$ dla pewnego $U \in \mathbb{Z}$, przy czym $p \nmid U$, bo $a^{p-1} \not\equiv 1 \pmod{p^2}$. Oznacza to, że $a^{p^{k-2}(p-1)} \equiv 1 + Up^{k-1} \pmod{p^k}$ dla $k = 2$.

Przypuśćmy, że $a^{p^{k-2}(p-1)} \equiv 1 + Up^{k-1} \pmod{p^k}$ dla pewnej liczby naturalnej $k \geqslant 2$. Wtedy $a^{p^{k-2}(p-1)} = (1 + Up^{k-1}) + p^k V$ dla pewnego $V \in \mathbb{Z}$. Stąd na mocy wzoru dwumianowego Newtona $a^{p^{k-2}(p-1)} \equiv$

$\equiv (1 + Up^{k-1})^p \pmod{p^{k+1}}$ oraz $(1 + Up^{k-1})^p = 1 + Up^k + \sum_{i=2}^{p} \binom{p}{i} U^i p^{i(k-1)}$. Ponadto na mocy twierdzenia 9.28 mamy, że $p \mid \binom{p}{i}$ dla $i = 2, \ldots, p-1$ oraz $1 + i(p-1) \geqslant 1 + 2(k-1) = 2k - 1 \geqslant k + 1$ a także $p(k-1) \geqslant 3(k-1) \geqslant k+1$, gdyż $p \neq 2$ i $k \geqslant 2$, więc $a^{p^{k-1}(p-1)} \equiv 1 + Up^k \pmod{p^{k+1}}$.

Stąd na mocy indukcji mamy, że $a^{p^{k-2}(p-1)} \equiv 1 + Up^{k-1} \pmod{p^k}$ dla każdej liczby naturalnej $k \geqslant 2$. □

Twierdzenie 21.17. *Niech p będzie nieparzystą liczbą pierwszą. Wówczas dla każdego $\alpha \in \mathbb{N}$ istnieje pierwiastek pierwotny modulo p^α i istnieje pierwiastek pierwotny modulo $2p^\alpha$. Jeśli a jest pierwiastkiem pierwotnym modulo p^2, to a jest pierwiastkiem pierwotnym modulo p^k dla dowolnego $k \in \mathbb{N}$. Ponadto, jeśli $2 \nmid a$, to a jest pierwiastkiem pierwotnym modulo $2p^k$ dla dowolnego $k \in \mathbb{N}$, a jeśli $2 \mid a$, to $a + p^2$ jest pierwiastkiem pierwotnym modulo $2p^k$ dla dowolnego $k \in \mathbb{N}$.*

Dowód. Na mocy twierdzenia 21.15 istnieje pierwiastek pierwotny a modulo p^2. Oznaczmy $r = w_p(a)$. Wtedy $r \mid p-1$ na mocy stwierdzenia 21.2 oraz $a^r \equiv 1 \pmod{p}$, czyli $a^r = 1 + Up$ dla pewnego $U \in \mathbb{Z}$. Stąd i ze wzoru dwumianowego Newtona mamy, że $a^{rp} = (1 + Up)^p \equiv 1 \pmod{p^2}$. Ale $w_{p^2}(a) = p(p-1)$, więc ze stwierdzenia 21.2, $p(p-1) \mid pr$, skąd $p - 1 \mid r$ i wobec tego, że też $r \mid p - 1$ mamy, że $r = p - 1$, co oznacza, że a jest pierwiastkiem pierwotnym modulo p.

Niech dalej $k \in \{3, 4, \ldots\}$ i oznaczmy $n = w_{p^k}(a)$. Wtedy $a^n \equiv 1 \pmod{p^k}$, skąd $a^n \equiv 1 \pmod{p^2}$ i ze stwierdzenia 21.2, $p(p-1) \mid n$, czyli $n = p(p-1)d$ dla pewnego $d \in \mathbb{N}$. Dalej, $n \mid \varphi(p^k) = p^{k-1}(p-1)$ na mocy stwierdzenia 21.2, więc $d \mid p^{k-2}$, skąd $d = p^i$ dla pewnego $i = 0, 1, \ldots, k-2$ oraz $n = p^{i+1}(p-1)$. Jeśli $i < k-2$, to $i \leqslant k-3$, skąd $i + 1 \leqslant k - 2$, a ponieważ $a^{p^{i+1}(p-1)} \equiv 1 \pmod{p^k}$, więc wtedy $a^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$, co przeczy lematowi 21.16. Zatem $i = k - 2$ i $n = p^{k-1}(p-1) = \varphi(p^k)$, co oznacza, że a jest pierwiastkiem pierwotnym modulo p^k.

Załóżmy, że $2 \nmid a$. Wtedy $a \in R_{2p^k}$. Oznaczmy $n = w_{2p^k}(a)$. Wtedy ze stwierdzenia 21.2, $n \mid \varphi(2p^k) = \varphi(p^k)$. Ponadto $a^n \equiv 1 \pmod{2p^k}$, skąd $a^n \equiv 1 \pmod{p^k}$, więc znowu ze stwierdzenia 21.2, $w_{p^k}(a) =$

$= \varphi(p^k)$ dzieli n, co razem z $n \mid \varphi(p^k)$ implikuje, że $n = \varphi(2p^k)$. Zatem a jest pierwiastkiem pierwotnym modulo $2p^k$.

Jeśli $2 \mid a$, to $2 \nmid a + p^2$ i $a + p^2 \equiv a \pmod{p^2}$, więc $a + p^2$ jest pierwiastkiem pierwotnym modulo p^2 i z pierwszej części dowodu $a + p^2$ jest pierwiastkiem pierwotnym modulo p^k dla dowolnego $k \in \mathbb{N}$. Zatem z przedostatniego akapitu tego dowodu, $a+p^2$ jest pierwiastkiem pierwotnym modulo $2p^k$ dla każdego $k \in \mathbb{N}$. □

Podsumowanie wyników tego podrozdziału jest zatem następujące

Twierdzenie 21.18. *Liczba naturalna $m > 1$ posiada pierwiastek pierwotny modulo m wtedy i tylko wtedy, gdy $m \in \{2, 4\}$ lub $m \in \{p^k, 2p^k\}$ dla pewnej nieparzystej liczby pierwszej p i dla pewnej liczby naturalnej k.*

Z twierdzenia 21.17 i z wniosku 21.10 otrzymujemy od razu następujący

Wniosek 21.19. *Dla dowolnej nieparzystej liczby pierwszej p i dla dowolnej liczby naturalnej α mamy, że $\lambda(p^\alpha) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Uwaga 21.20. Wnioski 21.19 i 10.27 oraz twierdzenie 10.28 pozwalają efektywnie obliczać wartość $\lambda(m)$ funkcji Carmichaela λ dla dowolnej liczby naturalnej $m > 1$ (oczywiście $\lambda(1) = 1$). Z udowodnionych wzorów wynika, że funkcja ξ podana w twierdzeniu 10.21 niewiele różni się od funkcji λ. Mianowicie, jeśli $8 \nmid m$, to $\xi(m) = \lambda(m)$, $\xi(2^k) = 2\lambda(2^k)$ dla $k \in \{3, 4, \ldots\}$ i jeżeli $m = 2^k \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ dla pewnych $s, \alpha_1, \ldots, \alpha_s \in \mathbb{N}$ i dla pewnych różnych nieparzystych liczb pierwszych $p_1, \ldots, p_s$, to $\xi(m) = \lambda(m)$, jeżeli $2^{k-1} \mid p_i - 1$ dla pewnego $i = 1, \ldots, s$ oraz $\xi(m) = 2\lambda(m)$, jeżeli $2^{k-1} \nmid p_j - 1$ dla każdego $j = 1, \ldots, s$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

21.3 Własności pierwiastków pierwotnych

Twierdzenie 21.21. *Niech $m > 2$ będzie liczbą naturalną. Jeżeli a jest pierwiastkiem pierwotnym modulo m, to kongruencja $x^2 \equiv a \pmod{m}$ nie posiada rozwiązania.*

Dowód. Przypuśćmy, że istnieje $x_0 \in \mathbb{Z}$ takie, że $x_0^2 \equiv a \pmod{m}$. Ponieważ $a \in R_m$, więc stąd $x_0 \in R_m$. Dalej, na mocy wniosku 10.19 liczba $\varphi(m)$ jest parzysta. Stąd $\frac{\varphi(m)}{2} \in \mathbb{N}$ oraz po podniesieniu stronami kongruencji $x_0^2 \equiv a \pmod{m}$ do potęgi $\frac{\varphi(m)}{2}$ i zastosowaniu twierdzenia 10.13 dostaniemy, że $1 \equiv a^{\varphi(m)/2} \pmod{m}$. Ale $\frac{\varphi(m)}{2} < \varphi(m) = w_m(a)$, więc otrzymaliśmy sprzeczność. □

Twierdzenie 21.22. *Niech p będzie nieparzystą liczbą pierwszą i niech a będzie pierwiastkiem pierwotnym modulo p. Wówczas dla dowolnego $k \in \mathbb{N}$: a^{2k-1} jest nieresztą kwadratową modulo p oraz a^{2k} jest resztą kwadratową modulo p.*

Dowód. Na mocy twierdzenia 21.21 mamy, że $(\frac{a}{p}) = -1$, więc dla $k \in \mathbb{N}$: $(\frac{a^{2k-1}}{p}) = (\frac{a}{p})^{2k-1} = (-1)^{2k-1} = -1$ i $(\frac{a^{2k}}{p}) = 1$, czyli a^{2k-1} jest nieresztą kwadratową modulo p oraz a^{2k} jest resztą kwadratową modulo p. □

Twierdzenie 21.23. *Niech $m > 2$ będzie liczbą naturalną. Jeżeli a jest pierwiastkiem pierwotnym modulo m, to $a^{\varphi(m)/2} \equiv -1 \pmod{m}$.*

Dowód. Dla $m = 4$ mamy, że $a \equiv 3 \pmod{4}$ i $\varphi(m) = 2$, więc teza zachodzi. Niech dalej $m \in \{3, 5, , \ldots\}$. Wtedy na mocy twierdzenia 21.18, $m = p^k$ lub $m = 2p^k$ dla pewnego $k \in \mathbb{N}$ i dla pewnej nieparzystej liczby pierwszej p. W obu przypadkach $\varphi(m) = p^{k-1}(p-1) = 2n$ dla pewnego $n \in \mathbb{N}$ oraz $m \mid (a^n - 1) \cdot (a^n + 1)$, bo $a^{2n} \equiv 1 \pmod{m}$. W pierwszym przypadku $p^k \mid (a^n-1)\cdot(a^n+1)$, przy czym $p^k \nmid a^n-1$, bo $w_m(a) = 2n$, więc $p \mid a^n+1$. Jeśli $p \mid a^n-1$, to $p \mid (a^n+1)-(a^n-1) = 2$, co prowadzi do sprzeczności. Wobec tego z zasadniczego twierdzenia arytmetyki $p^k \mid a^n + 1$, czyli $a^n \equiv -1 \pmod{m}$ w tym przypadku.

Niech teraz $m = 2p^k$. Wtedy $2p^k \mid (a^n - 1) \cdot (a^n + 1)$ i podobnie jak w pierwszym przypadku stąd wynika, że $a^n \equiv -1 \pmod{p^k}$. Dodatkowo, $a \in R_{2p^k}$, więc $2 \nmid a$, skąd $a^n \equiv -1 \pmod 2$ i wobec tego $a^n \equiv -1 \pmod{2p^k}$, czyli $a^n \equiv -1 \pmod m$, co kończy dowód. □

Twierdzenie 21.24. *Niech $m > 1$ będzie liczbą naturalną posiadającą pierwiastek pierwotny modulo m. Wówczas iloczyn wszystkich liczb naturalnych mniejszych od m i względnie pierwszych z m przystaje do -1 modulo m.*

Dowód. Dla $m = 2$ teza jest prawdziwa, bo iloczyn podany w twierdzeniu jest równy 1. Dla $m = 4$ ten iloczyn jest równy $1 \cdot 3 \equiv -1 \pmod 4$. Niech dalej $m \neq 2, 4$. Wtedy na mocy wniosku 10.19 mamy, że $n = \frac{\varphi(m)}{2} \in \mathbb{N}$. Ponadto istnieje pierwiastek pierwotny a modulo m i z twierdzenia 21.12 iloczyn wszystkich liczb naturalnych mniejszych od m i względnie pierwszych z m przystaje do liczby $a^1 \cdot a^2 \cdot \ldots \cdot a^{2n} = a^{1+2+\ldots+2n} = a^{n(2n+1)} = a^n \cdot a^{n\varphi(m)}$ modulo m. Dodatkowo $a^{n\varphi(m)} \equiv 1 \pmod m$, więc ten iloczyn przystaje do a^n modulo m. Natomiast $a^n \equiv -1 \pmod m$ na mocy twierdzenia 21.23. □

Podstawiając w powyższym twierdzeniu za m liczbę pierwszą p uzyskujemy, że $(p-1)! \equiv -1 \pmod p$, co daje nowy dowód twierdzenia Wilsona.

Następne stwierdzenie podaje warunki konieczne i wystarczające na to aby dana liczba całkowita a była pierwiastkiem pierwotnym modulo p dla ustalonej liczby pierwszej $p > 2$.

Stwierdzenie 21.25. *Niech $p > 2$ będzie liczbą pierwszą, która nie dzieli liczby całkowitej a. Wówczas a jest pierwiastkiem pierwotnym modulo p wtedy i tylko wtedy, gdy dla dowolnego dzielnika pierwszego q liczby $p - 1$ mamy, że $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$.*

Dowód. $\Rightarrow$. Z założenia $w_p(a) = p - 1$, więc dla każdego pierwszego dzielnika q liczby $p-1$ mamy, że $\frac{p-1}{q}$ jest liczbą naturalną mniejszą od $p - 1$, więc $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$.

$\Leftarrow$. Przypuśćmy, że $w_p(a) < p-1$. Na mocy stwierdzenia 21.2 mamy, że $p - 1 = n \cdot w_p(a)$ dla pewnej liczby naturalnej $n > 1$. Zatem istnieje

liczba pierwsza q taka, że $q \mid n$, czyli $n = pk$ dla pewnego $k \in \mathbb{N}$. Stąd $\frac{p-1}{q} = k \cdot w_p(a)$ i ze stwierdzenia 21.2, $a^{k \cdot w_p(a)} \equiv 1 \pmod{p}$, więc $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, co prowadzi do sprzeczności. □

Ćwiczenie 21.26. Pokazać, że 2 jest pierwiastkiem pierwotnym modulo liczba pierwsza p jeżeli $p = 4q + 1$ dla pewnego $q \in \mathbb{P}$.

Ćwiczenie 21.27. Pokazać, że 2 jest pierwiastkiem pierwotnym modulo liczba pierwsza p jeżeli $p = 2q + 1$ dla pewnego $q \in \mathbb{P}$ takiego, że $q \equiv 1 \pmod{4}$.

Ćwiczenie 21.28. Pokazać, że -2 jest pierwiastkiem pierwotnym modulo liczba pierwsza p jeżeli $p = 2q + 1$ dla pewnego $q \in \mathbb{P}$ takiego, że $q \equiv -1 \pmod{4}$.

21.4 Zastosowania pierwiastków pierwotnych

Omówimy najpierw zastosowanie pierwiastków pierwotnych do znajdowania rozwiązań pewnych kongruencji. Na początek będziemy potrzebowali pewnego narzędzia, które nazwiemy indeksem, jest on również nazywany logarytmem dyskretnym. Niech $m > 1$ będzie liczbą naturalną i niech r będzie pierwiastkiem pierwotnym modulo m. Wówczas na mocy twierdzenia 21.12 istnieje dokładnie jedna liczba $k \in \{0, 1, 2, \ldots, \varphi(m) - 1\}$ taka, że $r^k \equiv a \pmod{m}$. Zauważmy, że k jest najmniejszą liczbą w zbiorze $\{s \in \mathbb{N}_0 : r^s \equiv a \pmod{m}\}$. Liczbę k nazywamy **indeksem przy podstawie** r z liczby a i piszemy $\mathrm{ind}_r(a) = k$.

Przykład 21.29. Z przykładu 21.9 wiemy, że 2 jest pierwiastkiem pierwotnym modulo $m = 9$. Dalej, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ i $2^1 \equiv 2 \pmod{9}$, $2^2 \equiv 4 \pmod{9}$, $2^3 \equiv 8 \pmod{9}$, $2^4 \equiv 7 \pmod{9}$, $2^5 \equiv 5 \pmod{9}$, $2^6 \equiv 1 \pmod{9}$, więc dla modułu $m = 9$ mamy, że $\mathrm{ind}_2(1) = 0$, $\mathrm{ind}_2(2) = 1$, $\mathrm{ind}_2(4) = 2$, $\mathrm{ind}_2(5) = 5$, $\mathrm{ind}_2(7) = 4$ i $\mathrm{ind}_2(8) = 3$.

Na mocy stwierdzenia 21.2 (v) otrzymujemy następujące

Twierdzenie 21.30. *Niech $m > 1$ będzie liczbą naturalną, niech $a, b \in R_m$ i niech r będzie pierwiastkiem pierwotnym modulo m. Wówczas: $a \equiv b \pmod m \iff \operatorname{ind}_r(a) = \operatorname{ind}_r(b)$.*

Twierdzenie 21.31. *Niech $m > 1$ będzie liczbą naturalną, niech r będzie pierwiastkiem pierwotnym modulo m i niech $r', k, l \in R_m$. Wówczas:*

(i) $\operatorname{ind}_r(1) = 0$,
(ii) $\operatorname{ind}_r(kl) \equiv \operatorname{ind}_r(k) + \operatorname{ind}_r(l) \pmod{\varphi(m)}$,
(iii) $\operatorname{ind}_r(k^s) \equiv s \cdot \operatorname{ind}_r(k) \pmod{\varphi(m)}$ *dla każdego* $s \in \mathbb{N}$,
(iv) $\operatorname{ind}_r(-1) = \frac{\varphi(m)}{2}$ *dla* $n > 2$,
(v) $\operatorname{ind}_r(k) \equiv \operatorname{ind}_{r'}(k) \cdot \operatorname{ind}_r(r') \pmod{\varphi(m)}$.

Dowód. (i). Oczywiste, bo $r^0 = 1 \equiv 1 \pmod m$. (ii). Ponieważ $r^{\operatorname{ind}_r(k)} \equiv k \pmod m$ i $r^{\operatorname{ind}_r(l)} \equiv l \pmod m$, więc po pomnożeniu stronami tych kongruencji uzyskamy, że $r^{\operatorname{ind}_r(k)+\operatorname{ind}_r(l)} \equiv kl \pmod m$. Ponadto $r^{\operatorname{ind}_r(kl)} \equiv kl \pmod m$, więc $r^{\operatorname{ind}_r(kl)} \equiv r^{\operatorname{ind}_r(k)+\operatorname{ind}_r(l)} \pmod m$ i z twierdzenia 21.30, $\operatorname{ind}_r(kl) \equiv \operatorname{ind}_r(k) + \operatorname{ind}_r(l) \pmod{\varphi(m)}$.

(iii). Standardowe rozumowanie indukcyjne względem s z zastosowaniem (ii).

(iv). Na mocy twierdzenia 21.12 mamy, że $\frac{\varphi(m)}{2} \in \mathbb{N}$ i $r^{\varphi(m)/2} \equiv -1 \pmod m$, a ponieważ $\frac{\varphi(m)}{2} < \varphi(m)$, więc $\operatorname{ind}_r(-1) = \frac{\varphi(m)}{2}$.

(v). Wykorzystując własności kongruencji i określenie indeksu uzyskujemy, że $r^{\operatorname{ind}_{r'}(k)\cdot\operatorname{ind}_r(r')} = \left(r^{\operatorname{ind}_r(r')}\right)^{\operatorname{ind}_{r'}(k)} \equiv (r')^{\operatorname{ind}_{r'}(k)} \equiv k \pmod m$ i $r^{\operatorname{ind}_r(k)} \equiv k \pmod m$, więc $r^{\operatorname{ind}_r(k)} \equiv r^{\operatorname{ind}_{r'}(k)\cdot\operatorname{ind}_r(r')} \pmod m$ i na mocy twierdzenia 21.30, $\operatorname{ind}_r(k) \equiv \operatorname{ind}_{r'}(k) \cdot \operatorname{ind}_r(r') \pmod{\varphi(m)}$. □

Twierdzenie 21.32. *Niech $m > 1$ będzie liczbą naturalną, niech r będzie pierwiastkiem pierwotnym modulo m i niech $a, b \in R_m$ oraz $n \in \mathbb{N}$. Wówczas kongruencja $ax^n \equiv b \pmod m$ ma rozwiązanie wtedy i tylko wtedy, gdy $\operatorname{NWD}(n, \varphi(m)) \mid \operatorname{ind}_r(b) - \operatorname{ind}_r(a)$. Ponadto, jeśli $\operatorname{NWD}(n, \varphi(m)) \mid \operatorname{ind}_r(b) - \operatorname{ind}_r(a)$, to kongruencja $ax^n \equiv b \pmod m$ ma dokładnie $\operatorname{NWD}(n, \varphi(m)) = d$ rozwiązań i są one postaci $x_i + m\mathbb{Z}$, gdzie $x_i = r^{y_i}$ dla $i = 1, \ldots, d$, przy czym liczby $y_1, \ldots, y_d \in \mathbb{Z}_{\varphi(m)}$ są parami różne oraz $ny_i \equiv \operatorname{ind}_r(b) - \operatorname{ind}_r(a) \pmod{\varphi(m)}$.*

Dowód. Załóżmy, że istnieje $x_0 \in \mathbb{Z}$ takie, że $ax_0^n \equiv b \pmod{m}$. Ponieważ $a, b \in R_m$, więc stąd $x_0 \in R_m$. Ponadto $\operatorname{ind}_r(ax_0^n) \equiv \operatorname{ind}_r(b) \pmod{\varphi(m)}$ na mocy twierdzenia 21.2. Korzystając z twierdzenia 21.31 uzyskujemy, że $\operatorname{ind}_r(ax_0^n) \equiv \operatorname{ind}_r(a) + n \cdot \operatorname{ind}_r(x_0) \pmod{\varphi(m)}$. Zatem $\operatorname{ind}_r(a) + n \cdot \operatorname{ind}_r(x_0) \equiv \operatorname{ind}_r(b) \pmod{\varphi(m)}$, czyli $n \cdot \operatorname{ind}_r(x_0) \equiv \operatorname{ind}_r(b) - \operatorname{ind}_r(a) \pmod{\varphi(m)}$, więc na mocy twierdzenia 11.18 mamy, że $\operatorname{NWD}(n, \varphi(m)) \mid \operatorname{ind}_r(b) - \operatorname{ind}_r(a)$.

Na odwrót, niech $\operatorname{NWD}(n, \varphi(m)) \mid \operatorname{ind}_r(b) - \operatorname{ind}_r(a)$. Wtedy na mocy twierdzenia 11.18 kongruencja $n \cdot y \equiv \operatorname{ind}_r(b) - \operatorname{ind}_r(a) \pmod{\varphi(m)}$ posiada dokładnie $\operatorname{NWD}(n, \varphi(m)) = d$ rozwiązań $y_i + \varphi(m)\mathbb{Z}$, gdzie $y_i \in \mathbb{Z}_{\varphi(m)}$ dla $i = 1, \ldots, d$. Stąd dla $i = 1, \ldots, d$ mamy, że $x_i = r^{y_i} \in \mathbb{N}$, $y_i = \operatorname{ind}_r(x_i)$ i na mocy twierdzenia 21.2 klasy $x_1 + m\mathbb{Z}, \ldots, x_d + m\mathbb{Z}$ są parami różne. Ponadto dla $i = 1, \ldots, d$ mamy, że $n \cdot \operatorname{ind}_r(x_i) + \operatorname{ind}_r(a) \equiv \operatorname{ind}_r(b) \pmod{\varphi(m)}$. Zatem na mocy twierdzenia 21.31 jest $\operatorname{ind}_r(ax_i^n) \equiv \operatorname{ind}_r(b) \pmod{\varphi(m)}$, skąd $\operatorname{ind}_r(ax_i^n) = \operatorname{ind}_r(b)$ i $ax_i^n \equiv b \pmod{m}$ na mocy twierdzenia 21.2. Ponadto z pierwszej części dowodu wynika, że jeżeli $x_0 \in \mathbb{Z}$ i $ax_0^n \equiv b \pmod{m}$, to $\operatorname{ind}_r(x_0) + \varphi(m)\mathbb{Z}$ jest rozwiązaniem kongruencji $n \cdot y \equiv \operatorname{ind}_r(b) - \operatorname{ind}_r(a) \pmod{\varphi(m)}$, więc $\operatorname{ind}_r(x_0) \equiv y_i \pmod{\varphi(m)}$ dla pewnego $i = 1, \ldots, d$, skąd $\operatorname{ind}_r(x_0) = y_i$, a zatem $x_0 \equiv r^{y_i} \pmod{m}$, czyli $x_0 \equiv x_i \pmod{m}$. □

Wniosek 21.33. *Niech a będzie liczbą całkowitą niepodzielną przez nieparzystą liczbę pierwszą p i niech $n > 1$ oraz α będą liczbami naturalnymi. Wówczas kongruencja*

$$x^n \equiv a \pmod{p^\alpha} \tag{21.1}$$

nie posiada rozwiązania albo posiada dokładnie $d = \operatorname{NWD}(n, \varphi(p^\alpha))$ rozwiązań, przy czym rozwiązania istnieją wtedy i tylko wtedy, gdy $d \mid \operatorname{ind}_r(a)$, gdzie r jest dowolnym pierwiastkiem pierwotnym modulo p^2 i te rozwiązania są postaci $x_i = r^{y_i}$, gdzie $y_1, \ldots, y_d$ są różnymi liczbami ze zbioru $\mathbb{Z}_{\varphi(p^\alpha)}$ takimi, że $ny_i \equiv \operatorname{ind}_r(a) \pmod{\varphi(p^\alpha)}$ dla $i = 1, \ldots, s$.

Wniosek 21.34. *Niech a będzie liczbą całkowitą niepodzielną przez nieparzystą liczbę pierwszą p i niech $n > 1$ oraz α będą liczbami naturalnymi. Jeżeli $p \nmid n$, to kongruencja* (21.1) *ma rozwiązanie wtedy*

i tylko wtedy, gdy kongruencja $x^n \equiv a \pmod p$ *ma rozwiązanie. Jeśli kongruencja* $x^n \equiv a \pmod p$ *ma rozwiązanie, to kongruencja* (21.1) *ma dokładnie* $\mathrm{NWD}(n, p-1)$ *rozwiązań. Ponadto kongruencja* $x^n \equiv a \pmod p$ *posiada rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(n, p-1) \mid \mathrm{ind}_r(a)$*, gdzie* r *jest dowolnym pierwiastkiem pierwotnym modulo* p*.*

Z twierdzeń 21.31 i 11.18 uzyskujemy natychmiast następujące

Twierdzenie 21.35. *Niech* $m > 1$ *będzie liczbą naturalną, niech* r *będzie pierwiastkiem pierwotnym modulo* m *i niech* $a, b \in R_m$ *oraz niech* $d = \mathrm{NWD}(\mathrm{ind}_r(a), \varphi(m))$*. Wówczas dla dowolnego* $x \in \mathbb{N}_0$*:* $a^x \equiv b \pmod m \iff \mathrm{ind}_r(a) \cdot x \equiv \mathrm{ind}_r(b) \pmod{\varphi(m)}$*. W szczególności istnieje* $x \in \mathbb{N}_0$ *takie, że* $a^x \equiv b \pmod m$ *wtedy i tylko wtedy, gdy* $d \mid \mathrm{ind}_r(b)$*. Ponadto, jeśli* $d \mid \mathrm{ind}_r(b)$*, to istnieją parami różne liczby* $x_1, \ldots, x_d \in \mathbb{Z}_{\varphi(m)}$ *takie, że wszystkimi nieujemnymi liczbami całkowitymi* x *spełniającymi kongruencję* $a^x \equiv b \pmod m$ *są jedynie liczby postaci* $x = x_i + t \cdot \varphi(m)$*, gdzie* $t \in \mathbb{N}_0$ *oraz* $i = 1, \ldots, d$*.*

Uwaga 21.36. Następne zastosowanie pierwiastków pierwotnych dotyczy **okresu zasadniczego** rozwinięcia na ułamek dziesiętny w systemie pozycyjnym S_g liczby wymiernej $\frac{k}{n}$, gdzie $k, n \in \mathbb{N}$, $k < n$ i $\mathrm{NWD}(k, n) = 1$. Z podrozdziału 15.2 wiemy, że taki ułamek będzie czysto okresowy wtedy i tylko wtedy, gdy $\mathrm{NWD}(n, g) = 1$. Gdy ten warunek jest spełniony, to na mocy stwierdzeń 15.10 i 15.12 okres zasadniczy s jest najmniejszą liczbą naturalną r taką, że $g^r \equiv 1 \pmod n$, a zatem $s = w_n(g)$. W szczególności dla $g = 10$ i dla nieparzystej liczby naturalnej $n > 1$ niepodzielnej przez 5 mamy, że okres zasadniczy s rozwinięcia na ułamek dziesiętny w systemie S_{10} liczby $\frac{1}{n}$ jest równy $s = w_n(10)$.

Przykład 21.37. Znajdziemy okres zasadniczy rozwinięcia dziesiętnego ułamka $\frac{1}{17}$. Ze stwierdzenia 21.2 mamy, że $w_{17}(10) \mid 16$, bo $\varphi(17) = 16$, skąd $w_{17}(10) \in \{2, 4, 8, 16\}$. Ponadto $10^2 \equiv 49 \equiv \equiv -2 \pmod{17}$, $10^4 \equiv 4 \pmod{17}$, $10^8 \equiv 16 \equiv -1 \pmod{17}$, więc $w_{17}(10) = 16$. Zatem podstawowy okres rozwinięcia dziesiętnego liczby $\frac{1}{17}$ jest równy 16. Stąd 10 jest pierwiastkiem pierwotnym modulo 17.

Twierdzenie 21.38. *Niech $n > 1$ będzie nieparzystą liczbą naturalną niepodzielną przez 5. Okres zasadniczy rozwinięcia na ułamek dziesiętny liczby $\frac{1}{n}$ jest równy $n-1$ wtedy i tylko wtedy, gdy n jest liczbą pierwszą i 10 jest pierwiastkiem pierwotnym modulo n.*

Dowód. $\Rightarrow$. Na mocy uwagi 21.36 mamy, że $w_n(10) = n - 1$. Ponadto $w_n(10) \mid \varphi(n)$, więc $n - 1 \mid \varphi(n)$, skąd $n - 1 \leqslant \varphi(n)$. Dalej, $n > 2$, więc $\varphi(n) < n$. Wobec tego $\varphi(n) = n - 1$, co oznacza, że każda liczba naturalna $k < n$ jest względnie pierwsza z n. Jeśli $n \notin \mathbb{P}$, to $n = ab$ dla pewnych liczb naturalnych $a > 1$ i $b > 1$ takich, że $a < n$. Wtedy $\mathrm{NWD}(a, n) = a > 1$, co prowadzi do sprzeczności. Zatem n jest nieparzystą liczbą pierwszą i $w_n(10) = n - 1 = \varphi(n)$, czyli 10 jest pierwiastkiem pierwotnym modulo n.

$\Leftarrow$. Z założenia mamy, że $w_n(10) = \varphi(n) = n - 1$, więc na mocy uwagi 21.36 okres zasadniczy rozwinięcia na ułamek dziesiętny liczby $\frac{1}{n}$ jest równy $n - 1$. □

W kontekście rozważanych problemów wspomnijmy **hipotezę Gaussa**, która głosi, że istnieje nieskończenie wiele liczb pierwszych p takich, że $\frac{1}{p}$ ma w rozwinięciu dziesiętnym okres zasadniczy równy $p - 1$. Równoważnie: Istnieje nieskończenie wiele liczb pierwszych p takich, że 10 jest pierwiastkiem pierwotnym modulo p. Natomiast **hipoteza Artina** wysunięta w 1927 roku głosi, że jeśli $a \neq -1$ jest liczbą całkowitą niebędącą kwadratem liczby całkowitej, to a jest pierwiastkiem pierwotnym modulo p dla nieskończenie wielu liczb pierwszych p. W 1983 roku R. Gupta i M. Ram Murty wykazali w [15], że dla dowolnych różnych trzech liczb pierwszych q, r, s przynajmniej jedna liczba a ze zbioru

$$\{qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs\}$$

spełnia hipotezę Artina, to znaczy a jest pierwiastkiem pierwotnym modulo p dla nieskończenie wielu liczb pierwszych p. Dwa lata później D. R. Heath-Brown w [17] ulepszył metody użyte przez wspomnianych wyżej autorów i pokazał między innymi, że co najwyżej dwie liczby pierwsze nie spełniają hipotezy Artina oraz, że co najwyżej trzy liczby

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

bezkwadratowe $a > 1$ nie spełniają tej hipotezy. Dodatkowo, z pierwszego twierdzenia udowodnionego w tej pracy wynika natychmiastowo, że co najmniej jedna z liczb $2, 3$ lub 5 spełnia hipotezę Artina.

Rozdział 22

Zadania

22.1 Zadania łatwiejsze

Zadania zaprezentowane w tym i w kolejnym rozdziale mają na celu zobrazowanie teorii oraz metod omówionych w tej książce. Do ich pełnego rozwiązania wystarcza zrozumienie odpowiednich fragmentów wyłożonych w poprzednich paragrafach. Dla wygody Czytelnika w rozdziale 22 przedstawimy kompletne ich rozwiązania. Warto wspomnieć, że nie wszystkie zadania tu przytoczone są oryginalne. Część z nich to klasyczne problemy pojawiające się w różnych opracowaniach - ich włączenie do tego rozdziału jest spowodowane ich istotnym walorem edukacyjnym. Część zadań to problemy pochodzące z różnorodnych zawodów i olimpiad matematycznych. Wybór zadań, dokonany przez Autora, opierał się na jego wieloletnich doświadczeniach w pracy ze studentami Matematyki UwB. W tym miejscu warto zwrócić uwagę zainteresowanego Czytelnika na wspaniały cykl książek prof. Andrzeja Nowickiego *Podróże po imperium liczb* [30], w których można znaleźć bardzo bogaty wybór zadań i niebanalnych problemów.

Zadanie 22.1. Stosując metodę dzielników dopełniających wyznaczyć wszystkie dodatnie dzielniki liczb: 18, 24, 30, 48, 124, 564.

Zadanie 22.2. Dla jakich liczb naturalnych n;

a) $n+1 \mid n^2+1$, b) $7n+1 \mid 19n+17$, c) $n+2 \mid n^3-7n^2-5n+10$, d) $n^2-5n-14 \mid n^3-7n^2-5n+10$?

Zadanie 22.3. Dla jakich liczb całkowitych x:
a) $x \mid x+1$, b) $x+1 \mid 2x$, c) $x-3 \mid x^3-3$?

Zadanie 22.4. Obliczyć reszty:
a) $[-67]_9$, b) $[123]_7$, c) $[-78]_{14}$, d) $[169]_{13}$.

Zadanie 22.5. Pewna liczba całkowita daje przy dzieleniu przez 6 resztę 4, zaś przy dzieleniu przez 11 daje resztę 1. Jaką resztę daje ta liczba przy dzieleniu przez 66?

Zadanie 22.6. Stosując algorytm Euklidesa oblicz NWD liczb:
a) 252 i 198, b) 221 i 754, c) 420, 360, 270 i 225, d) 328 i 1804, e) 522 i 1551.

Zadanie 22.7. Jaką resztę z dzielenia przez 3 daje suma kwadratów trzech kolejnych liczb całkowitych?

Zadanie 22.8. Udowodnić, że kwadrat liczby całkowitej niepodzielnej przez 3 daje resztę 1 z dzielenia przez 3.

Zadanie 22.9. Udowodnić, że iloczyn dwóch kolejnych liczb całkowitych jest podzielny przez 2.

Zadanie 22.10. Udowodnić, że iloczyn trzech kolejnych liczb całkowitych jest podzielny przez 3.

Zadanie 22.11. Udowodnij, że dla każdej liczby całkowitej n:
a) $2 \mid n^2-n$, b) $3 \mid n^3-n$.

Zadanie 22.12. Udowodnić, że iloczyn dwóch kolejnych liczb całkowitych parzystych jest podzielny przez 8.

Zadanie 22.13. Udowodnić, że kwadrat liczby nieparzystej daje z dzielenia przez 8 resztę 1.

Zadanie 22.14. Udowodnić, że wśród dowolnych sześciu liczb całkowitych istnieją dwie liczby, których różnica jest podzielna przez 5.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.15. Udowodnić, że wśród pięciu dowolnych liczb całkowitych istnieją trzy liczby, których suma jest podzielna przez 3.

Zadanie 22.16. Niech a, b, c, d będą liczbami całkowitymi takimi, że $a \mid b$ i $c \mid d$. Udowodnić, że wtedy $ac \mid bd$.

Zadanie 22.17. Stosując algorytm Euklidesa oblicz:
NWW$(1804, 328)$, NWW$(722, 874)$, NWW$(522, 1551)$.

Zadanie 22.18. Znaleźć najmniejszą liczbę naturalną podzielną przez 18 i 24.

Zadanie 22.19. Udowodnić, że jeżeli liczby całkowite $a_1, a_2, \ldots, a_n$ są podzielne przez liczbę całkowitą a, to dla dowolnych liczb całkowitych $c_1, c_2, \ldots, c_n$ liczba $c_1a_1 + c_2a_2 + \ldots + c_na_n$ też jest podzielna przez a.

Zadanie 22.20. Udowodnić, że liczba naturalna jest podzielna przez 11 wtedy i tylko wtedy, gdy jej naprzemienna suma cyfr jest podzielna przez 11.

Zadanie 22.21. Wykazać, że nie istnieje liczba całkowita, która przy dzieleniu przez 18 daje resztę 13, a przy dzieleniu przez 21 daje resztę 2.

Zadanie 22.22. Ile dzielników naturalnych posiada liczba $6^{20} \cdot 10^{18} \cdot 15^{16}$?

Zadanie 22.23. Ile wspólnych dzielników naturalnych mają liczby $6^{20} \cdot 10^{18} \cdot 15^{16}$ i $12^4 \cdot 18^{20}$?

Zadanie 22.24. Wypisz wszystkie wspólne dzielniki naturalne liczb 168 i 396.

Zadanie 22.25. Opisz wszystkie liczby naturalne, które mają dokładnie 3 dzielniki naturalne.

Zadanie 22.26. Dla jakich cyfr x liczba $(31x2)_{10}$ jest podzielna przez:
a) 3, b) 9, c) 4?

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.27. Niech p będzie liczbą pierwszą. Opisz wszystkie liczby naturalne, które mają dokładnie p dzielników naturalnych.

Zadanie 22.28. Udowodnij, że reszta z dzielenia liczby pierwszej przez 30 jest liczbą pierwszą lub jest równa 1.

Zadanie 22.29. Stosując sito Eratostenesa wyznacz wszystkie liczby pierwsze $p \leqslant 200$.

Zadanie 22.30. Niech $n > 1$ będzie liczbą naturalną taką, że $n \mid (n-1)! + 1$. Udowodnij, że wówczas n jest liczbą pierwszą.

Zadanie 22.31. Czy 437 jest liczbą pierwszą? A 1997?

Zadanie 22.32. Przedstaw w postaci kanonicznej liczby 112, 143, 201, 2001.

Zadanie 22.33. Wyznacz wszystkie liczby naturalne a, b takie, że $a^3 + b^3$ jest liczbą pierwszą.

Zadanie 22.34. Wyznacz wszystkie liczby pierwsze p, q i wszystkie liczby naturalne n, m takie, że $2p^n = 25q^m$.

Zadanie 22.35. Udowodnij, że jeżeli liczby naturalne a i b są względnie pierwsze, to liczby $a + b$ i $a \cdot b$ też są względnie pierwsze.

Zadanie 22.36. Udowodnij, że każde dwie kolejne liczby całkowite są względnie pierwsze.

Zadanie 22.37. Niech a i b będą względnie pierwszymi liczbami naturalnymi takimi, że $a \mid b^n$ dla pewnej liczby naturalnej n. Udowodnij, że wówczas $a = 1$.

Zadanie 22.38. Korzystając z rozkładów kanonicznych znajdź:
$\mathrm{NWD}(168, 396)$, $\mathrm{NWW}(168, 396)$, $\mathrm{NWD}(1115, 630)$,
$\mathrm{NWD}(2516, 3655)$, $\mathrm{NWW}(1115, 630)$, $\mathrm{NWW}(2516, 3655)$.

Zadanie 22.39. Niech p, q, r będą różnymi liczbami pierwszymi oraz $a = q^3r^2$, $b = p^2r$, $c = p^2qr^3$. Oblicz $\mathrm{NWD}(a, b, c)$, $\mathrm{NWW}(a, b, c)$, $\mathrm{NWD}(ab, c)$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.40. Wypisz wszystkie liczby naturalne $n \leqslant 20$, które są względnie pierwsze z liczbą 98.

Zadanie 22.41. Przedstaw liczbę 330 w postaci iloczynu dwóch liczb naturalnych względnie pierwszych na wszystkie możliwe sposoby.

Zadanie 22.42. Przedstaw liczbę 22 w postaci sumy dwóch liczb naturalnych względnie pierwszych na wszystkie możliwe sposoby.

Zadanie 22.43. Czy liczby 15, 21, 35 są względnie pierwsze?

Zadanie 22.44. Udowodnij, że dla każdej nieparzystej liczby naturalnej n liczba $n^3 + 3n^2 - n - 3$ jest podzielna przez 48.

Zadanie 22.45. Udowodnij, że dla każdej liczby pierwszej $p > 5$ liczba $p^4 - 1$ jest podzielna przez 240.

Zadanie 22.46. Pokazać, dla każdej liczby naturalnej n liczba $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ jest całkowita.

Zadanie 22.47. Napisz ogólną postać liczby naturalnej będącej wspólną wielokrotnością liczb 18, 24 i 45.

Zadanie 22.48. Znajdź cyfrę setek i cyfrę jedności liczby $(42 * 4*)_{10}$, jeśli wiadomo, że ta liczba jest podzielna przez 72.

Zadanie 22.49. Udowodnij, że jeżeli suma kwadratów dwóch liczb całkowitych jest podzielna przez 3, to te liczby też są podzielne przez 3.

Zadanie 22.50. Ile jest liczb naturalnych $n \in [100, 1000]$ takich, że
a) $7 \mid n$, b) $8 \mid n$ lub $5 \mid n$, c) $3 \mid n$ i $4 \nmid n$?

Zadanie 22.51. Wyznacz wszystkie liczby całkowite n spełniające równanie $2^n \cdot (4 - n) = 2n + 4$.

Zadanie 22.52. Udowodnij, że dla wszystkich liczb naturalnych n liczba $n^2 - n + 9$ nie jest podzielna przez 49.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.53. Udowodnij, że dla dowolnego naturalnego n liczba $n(n+1)(n+2)(n+3)+1$ jest kwadratem pewnej liczby naturalnej.

Zadanie 22.54. Wyznaczyć wszystkie liczby dwucyfrowe, które są sumami cyfry dziesiątek i kwadratu cyfry jedności.

Zadanie 22.55. Wyznacz wszystkie różne liczby naturalne a, b, c takie, że $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1$.

Zadanie 22.56. Udowodnij, że jeżeli $p>3$ i liczby p oraz $10p+1$ są pierwsze, to liczba $5p+1$ nie jest pierwsza.

Zadanie 22.57. Udowodnij, że iloczyn czterech kolejnych liczb całkowitych jest podzielny przez 24.

Zadanie 22.58. Niech a i b będą liczbami całkowitymi dającymi różne reszty z dzielenia przez 3. Udowodnij, że dla dowolnego całkowitego n wśród liczb: $n, n+a, n+b$ dokładnie jedna jest podzielna przez 3.

Zadanie 22.59. Udowodnij, że każde dwie kolejne liczby całkowite nieparzyste są względnie pierwsze.

Zadanie 22.60. Niech $a, b \in \mathbb{Z}$, $b>0$ będą takie, że ułamek $\frac{a}{b}$ jest nieskracalny. Uzasadnij, że wówczas ułamki $\frac{a+b}{b}$ i $\frac{b-a}{b}$ też są nieskracalne.

Zadanie 22.61. Liczbę $1\frac{1}{12}$ przedstaw w postaci sumy trzech ułamków prostych na wszystkie możliwe sposoby.

Zadanie 22.62. Udowodnij, że ułamek, którego licznik jest iloczynem czterech kolejnych liczb naturalnych, a mianownik jest iloczynem trzech kolejnych liczb naturalnych parzystych, jest skracalny przez 24.

Zadanie 22.63. Udowodnij, że dla każdego całkowitego n liczby: n^3+5n, n^3+11n i n^3-19n są podzielne przez 6.

Zadanie 22.64. Udowodnij, że dla każdego całkowitego n liczba $n(n+1)(2n+1)$ jest podzielna przez 6.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.65. Udowodnij, że dla dowolnych liczb całkowitych a i b: $3 \mid a$ lub $3 \mid b$ lub $3 \mid a+b$ lub $3 \mid a-b$.

Zadanie 22.66. Wykaż, że różnica czwartych potęg dwóch liczb całkowitych różniących się o 2 jest podzielna przez 16.

Zadanie 22.67. Wykaż, że wśród 11 dowolnych liczb całkowitych istnieją zawsze dwie liczby, których różnica jest podzielna przez 10.

Zadanie 22.68. Udowodnij, że suma liczby dwucyfrowej i liczby utworzonej z tych samych cyfr w odwrotnej kolejności, jest zawsze podzielna przez 11.

Zadanie 22.69. Udowodnij, że różnica trzycyfrowych liczb, z których jedna napisana jest tymi samymi cyframi co druga, lecz w odwrotnym porządku, jest podzielna przez 99.

Zadanie 22.70. Udowodnij, że różnica między liczbą trzycyfrową, a liczbą zapisaną tymi samymi cyframi, ale w odwrotnej kolejności, nie może być kwadratem liczby naturalnej.

Zadanie 22.71. Wyznacz wszystkie liczby dwucyfrowe $(xy)_{10}$, dla których liczba $(xy)_{10} - (yx)_{10}$ jest kwadratem liczby naturalnej.

Zadanie 22.72. Dla liczb trzycyfrowych $\overline{xyz}$ wyznacz największą wartość wyrażenia $\frac{\overline{xyz}}{x+y+z}$.

Zadanie 22.73. Udowodnij, że suma kwadratów dwóch liczb całkowitych nie daje reszty 3 z dzielenia przez 4.

Zadanie 22.74. Dane są trzy kolejne liczby naturalne, z których pierwsza jest parzysta. Udowodnij, że iloczyn tych liczb jest podzielny przez 24.

Zadanie 22.75. Udowodnij, że różnica kwadratów dwóch kolejnych liczb całkowitych jest liczbą nieparzystą.

Zadanie 22.76. Wyznacz wszystkie $x, y, z \in \{0, 1, \ldots, 9\}$ takie, że $8x + 24y + 5z = 308$.

Zadanie 22.77. Wyznacz wszystkie $x, y \in \mathbb{N}$ takie, że $2x + 5y = 2001$.

Zadanie 22.78. Udowodnij, że suma sześcianów trzech kolejnych liczb całkowitych jest podzielna przez 9.

Zadanie 22.79. Znajdź liczbę czterocyfrową, której dwie pierwsze cyfry są jednakowe, dwie ostatnie cyfry są jednakowe i która jest kwadratem liczby całkowitej.

Zadanie 22.80. Udowodnij, że liczba naturalna n jest złożona wtedy i tylko wtedy, gdy suma jej dzielników naturalnych jest większa niż $n + 1$.

Zadanie 22.81. Znajdź liczbę trzycyfrową o sumie cyfr równej 9 i mającą tę własność, że jest ona równa $\frac{47}{36}$ liczby utworzonej z tych samych cyfr, ale w odwrotnym porządku.

Zadanie 22.82. Wyznacz wszystkie $x, y \in \mathbb{N}$ takie, że $x(y+1)^2 = 243y$.

Zadanie 22.83. Wyznacz wszystkie $x, y \in \mathbb{N}$ takie, że $x^4 - y^4 = 65$.

Zadanie 22.84. Wyznacz wszystkie $x, y \in \mathbb{Z}$ takie, że $2xy + 3y^2 = 24$.

Zadanie 22.85. Niech $a, b \in \mathbb{N}$ będą takie, że $a+b \mid a^2$. Udowodnij, że wówczas $a + b \mid b^2$.

Zadanie 22.86. Wyznaczyć wszystkie liczby naturalne x, y takie, że:
a) $x^2 - y^2 = 24$, b) $x^2 - y^2 = 18$, c) $xy = x + y$, d) $xy = 3x + 2y + 12$.

Zadanie 22.87. Udowodnij, że dla dowolnej liczby naturalnej $n \geqslant 2$ i dla dowolnych liczb x i y zachodzi wzór:

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}). \qquad (22.1)$$

Zadanie 22.88. Niech x, y będą liczbami całkowitymi. Udowodnić, że dla dowolnej liczby naturalnej n: $x - y \mid x^n - y^n$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.89. Udowodnij, że dla dowolnej liczby naturalnej n: a) $9 \mid 10^n - 1$, b) $3 \mid 10^n - 1$, c) $11 \mid 10^n - (-1)^n$, d) $3 \mid 10^n + 4^n - 2$, e) $8 \mid 9^n - 1$.

Zadanie 22.90. Udowodnij, że dla dowolnego $k \in \mathbb{N}$ i dla dowolnych liczb x i y zachodzi wzór:

$$x^{2k+1} + y^{2k+1} = (x+y)(x^{2k} - x^{2k-1}y + \ldots - xy^{2k-1} + y^{2k}). \quad (22.2)$$

Zadanie 22.91. Niech x, y będą liczbami całkowitymi. Udowodnić, że dla dowolnej liczby naturalnej k: $x + y \mid x^{2k-1} + y^{2k-1}$.

Zadanie 22.92. Udowodnij, że dla każdej liczby naturalnej n: a) $4 \mid 5^{5n-2} + 3$, b) $10 \mid 3^{4n+2} + 1$, c) $133 \mid 11^{n+2} + 12^{2n+1}$.

Zadanie 22.93. Udowodnij, że dla dowolnych liczb rzeczywistych a, b i c zachodzi tożsamość:

$$a^3 + b^3 + c^3 - 3abc = (a+b+c) \cdot (a^2 + b^2 + c^2 - ab - ac - bc).$$

Zadanie 22.94. Wyznacz wszystkie liczby naturalne x takie, że $\frac{8^x - 2^x}{6^x - 3^x} = 2$.

Zadanie 22.95. Wyznacz wszystkie liczby naturalne x i y takie, że $\frac{1}{x} + \frac{1}{y} = \frac{2}{35}$.

Zadanie 22.96. Niech $a, b, c \in \mathbb{N}$ będą takie, że $\mathrm{NWD}(a, c) = 1$. Udowodnij, że wówczas $\mathrm{NWD}(a \cdot b, c) = \mathrm{NWD}(b, c)$.

Zadanie 22.97. Niech $p \in \mathbb{P}$ i niech $a \in \mathbb{Z}$. Pokazać, że $p \mid a^{p^k} - a$ dla każdego $k \in \mathbb{N}$.

Zadanie 22.98. Niech $x, y, z \in \mathbb{Z}$ będą takie, że przynajmniej jedna z liczb $a = 2x + 3y + 4z$, $b = 6x + 2y + 5z$ i $c = x + 5y + 2z$ jest podzielna przez 7. Udowodnij, że wówczas każda z liczb a, b i c jest podzielna przez 7.

Zadanie 22.99. Wyznacz wszystkie liczby naturalne x i y takie, że $x^2 + y$ i $x + y^2$ są kwadratami pewnych liczb naturalnych.

Zadanie 22.100. Czy istnieją różne liczby pierwsze p, q i r takie, że liczba $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}$ jest całkowita?

Zadanie 22.101. Udowodnij, że $3 \nmid 2n^2+n+1$ dla każdego $n \in \mathbb{N}$.

Zadanie 22.102. Udowodnij, że dla dowolnych liczb całkowitych m i n z tego, że $9 \mid m^2+mn+n^2$ wynika, że $3 \mid m$ i $3 \mid n$.

Zadanie 22.103. Wyznacz wszystkie trójki (a,b,c) liczb naturalnych takich, że $a \equiv b \pmod{c}$ i $b \equiv c \pmod{a}$ i $c \equiv a \pmod{b}$.

22.2 Zadania trudniejsze

Zadanie 22.104. Wyznacz wszystkie liczby naturalne x, y takie, że:
a) $x \mid y+1$ i $y \mid x+1$, b) $x \mid 2y+1$ i $y \mid 2x+1$.

Zadanie 22.105. Dla naturalnych n zbadać skracalność ułamków: $\frac{12n+1}{30n+2}$, $\frac{19n+7}{7n+11}$, $\frac{2n+1}{9n+4}$, $\frac{8n+3}{13n+5}$, $\frac{2n-1}{9n+4}$, $\frac{14n+3}{21n+4}$.

Zadanie 22.106. Liczby 4373 i 826 podzielono przez tę samą liczbę naturalną i otrzymano odpowiednio reszty 8 i 7. Znajdź tę liczbę.

Zadanie 22.107. Wyznacz wszystkie liczby naturalne n, które są podzielne przez wszystkie liczby naturalne k takie, że $k^2 \leqslant n$.

Zadanie 22.108. Opisz wszystkie liczby naturalne, które mają dokładnie 4 dzielniki naturalne.

Zadanie 22.109. Opisz wszystkie liczby naturalne, które mają dokładnie
a) 18, b) 24
dzielniki naturalne.

Zadanie 22.110. Wyznacz wszystkie liczby naturalne podzielne przez 12, które posiadają dokładnie 18 dzielników naturalnych.

Zadanie 22.111. Wyznacz wszystkie liczby naturalne podzielne przez 10, które posiadają dokładnie 6 dzielników naturalnych.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.112. Wyznacz wszystkie liczby pierwsze, które są jednocześnie sumą dwóch liczb pierwszych i różnicą dwóch liczb pierwszych.

Zadanie 22.113. Udowodnij, że dla dowolnej liczby naturalnej b równoważne są warunki:
a) nie istnieje liczba naturalna $d > 1$ taka, że $d^2 \mid b$;
b) nie istnieje liczba pierwsza p taka, że $p^2 \mid b$;
c) $b = 1$ lub b jest iloczynem różnych liczb pierwszych.

Zadanie 22.114. Opisz liczby naturalne a takie, że dla dowolnych liczb naturalnych b, n z tego, że $a \mid b^n$ wynika, że $a \mid b$.

Zadanie 22.115. Opisz liczby naturalne a takie, że dla dowolnych liczb naturalnych x, y, z tego, że $a \mid x \cdot y$ wynika, że $a \mid x$ lub $a \mid y$.

Zadanie 22.116. Niech k i l będą względnie pierwszymi liczbami naturalnymi. Wyznacz wszystkie liczby naturalne x, y spełniające równanie: $x^k = y^l$.

Zadanie 22.117. Udowodnij, że każdą liczbę naturalną n można jednoznacznie zapisać w postaci $n = a^2 \cdot b$, gdzie a i b są liczbami naturalnymi takimi, że b nie jest podzielne przez kwadrat liczby pierwszej.

Zadanie 22.118. Udowodnij, że każdą liczbę naturalną a można jednoznacznie zapisać w postaci $a = 2^{l-1} \cdot (2k - 1)$ dla pewnych liczb naturalnych k i l.

Zadanie 22.119. Liczby $x, y \in \mathbb{Z}$ są takie, że $6x + 13y$ dzieli się przez 35. Wykazać, że liczba $x + 8y$ też dzieli się przez 35.

Zadanie 22.120. Wyznacz najmniejszą liczbę naturalną, która przy dzieleniu przez k daje resztę $k - 1$ dla każdego $k = 2, 3, \ldots, 10$.

Zadanie 22.121. Opisz wszystkie liczby pierwsze p, dla których liczba $p^2 + 2$ też jest liczbą pierwszą.

Zadanie 22.122. Wyznacz wszystkie liczby pierwsze p, q, r takie, że $p \cdot q \cdot r = 5 \cdot (p + q + r)$.

Zadanie 22.123. Wyznacz wszystkie liczby naturalne n takie, że $n^4 + 4$ jest liczbą pierwszą.

Zadanie 22.124. Wyznacz wszystkie liczby naturalne n takie, że $n^4 + n^2 + 1$ jest liczbą pierwszą.

Zadanie 22.125. Wyznacz wszystkie liczby pierwsze p, q, r takie, że $p = q^3 - r^3$.

Zadanie 22.126. Wyznacz wszystkie liczby pierwsze p, q takie, że $p^2 - 2q^2 = 1$.

Zadanie 22.127. Wyznacz wszystkie liczby pierwsze p, q takie, że $6p - 22q = 12$.

Zadanie 22.128. Udowodnij, że dla dowolnych liczb całkowitych a, b, c liczba $a^3b^3c^3(a^3 - b^3)(b^3 - c^3)(c^3 - a^3)$ jest podzielna przez 7.

Zadanie 22.129. Udowodnij, że dla każdej liczby naturalnej m istnieje m kolejnych liczb naturalnych, które są liczbami złożonymi.

Zadanie 22.130. Udowodnij, że dla dowolnej liczby naturalnej $n > 2$ w przedziale $(n, n!)$ istnieje liczba pierwsza. Wyprowadź stąd wniosek, że liczb pierwszych jest nieskończenie wiele.

Zadanie 22.131. Niech $a, n > 1$ będą liczbami naturalnymi takimi, że $a^n - 1$ jest liczbą pierwszą. Udowodnij, że wówczas $a = 2$ i n jest liczbą pierwszą.

Zadanie 22.132. Udowodnij, że jeżeli p i $8p^2+1$ są liczbami pierwszymi, to $8p^2 - 1$ też jest liczbą pierwszą.

Zadanie 22.133. Udowodnij, że jeżeli liczby p i $5p^2-2$ są liczbami pierwszymi, to liczby $5p^2 - 4$ i $5p^2 + 2$ też są liczbami pierwszymi.

Zadanie 22.134. Udowodnij, że dla dowolnej liczby naturalnej n równoważne są warunki:
a) n jest liczbą pierwszą, b) równanie $\frac{1}{x} - \frac{1}{y} = \frac{1}{n}$ posiada dokładnie jedno rozwiązanie w liczbach naturalnych x, y.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.135. Znajdź wszystkie liczby pierwsze x, y, z takie, że $2x - y = 1$ i $2x - z = -1$.

Zadanie 22.136. Znajdź wszystkie liczby pierwsze p, q takie, że $11p - 5q = 7$.

Zadanie 22.137. Niech S będzie zbiorem wszystkich liczb naturalnych postaci $4k+1$ dla $k = 0, 1, \ldots$. Pokaż, że $1 \in S$ oraz dla dowolnych $r, s \in S$ mamy, że $r \cdot s \in S$. Powiemy, że $p \in S$ jest liczbą „pierwszą w S", jeżeli $p > 1$ oraz p nie jest iloczynem dwóch liczb $r, s \in S$ mniejszych niż p. Wyznacz wszystkie liczby „pierwsze w S", które są nie większe niż 101. Udowodnij, że każda liczba $s \in S$ większa od 1 jest iloczynem skończonej liczby liczb „pierwszych w S". Czy rozkład taki jest zawsze jednoznaczny?

Zadanie 22.138. Znajdź liczby naturalne $a \neq b$ oraz liczby naturalne k, l, m, n takie, że $n \neq k$ lub $m \neq l$ oraz $a^n \cdot b^m = a^k \cdot b^l$.

Zadanie 22.139. Udowodnij, że dla dowolnych liczb naturalnych a, b:

$$\mathrm{NWD}(a, b) + \mathrm{NWW}(a, b) \geqslant a + b.$$

Kiedy zachodzi równość?

Zadanie 22.140. Znajdź wszystkie liczby naturalne x, y takie, że $\mathrm{NWD}(x, y) = 15$ oraz $\mathrm{NWW}(x, y) = 24360$.

Zadanie 22.141. Jakie wartości przyjmuje $\mathrm{NWW}(a, b, c)$, jeżeli a, b, c są liczbami naturalnymi o sumie 12?

Zadanie 22.142. Jakie wartości przyjmuje $\mathrm{NWD}(a, b, c)$, jeżeli a, b, c są liczbami naturalnymi o sumie 12?

Zadanie 22.143. Znajdź wszystkie liczby naturalne $n \geqslant 2$ takie, że $\sqrt[n]{10^{80} \cdot 6^{60} \cdot 15^{40}}$ jest liczbą wymierną.

Zadanie 22.144. Udowodnij, że dla dowolnych liczb naturalnych a, b, c:
a) $\mathrm{NWD}(a, \mathrm{NWW}(b, c)) = \mathrm{NWW}(\mathrm{NWD}(a, b), \mathrm{NWD}(a, c))$,
b) $\mathrm{NWW}(a, \mathrm{NWD}(b, c)) = \mathrm{NWD}(\mathrm{NWW}(a, b), \mathrm{NWW}(a, c))$,
c) $\mathrm{NWD}(a, b, c)\mathrm{NWW}(a, b, c) \mid abc$.

Zadanie 22.145. Znajdź wszystkie liczby naturalne x, y takie, że:
a) $\mathrm{NWD}(x,y) = \mathrm{NWW}(x,y)$, b) $\mathrm{NWD}(x,y) = xy$,
c) $\mathrm{NWD}(x,y) = x+y$, d) $\mathrm{NWD}(x,y) = x-y$, e) $\mathrm{NWD}(x,y) = \frac{x}{y}$,
f) $\mathrm{NWW}(x,y) = xy$, g) $\mathrm{NWW}(x,y) = x+y$, h) $\mathrm{NWW}(x,y) = x-y$,
i) $\mathrm{NWW}(x,y) = \frac{x}{y}$, j) $\mathrm{NWW}(x,y) = x$, k) $\mathrm{NWD}(x,y) = x$.

Zadanie 22.146. Znajdź wszystkie liczby naturalne x, y takie, że:
a) $x+y = 180$ i $\mathrm{NWD}(x,y) = 30$,
b) $7x = 11y$ i $\mathrm{NWD}(x,y) = 45$,
c) $xy = 720$ i $\mathrm{NWD}(x,y) = 4$,
d) $\mathrm{NWD}(x,y) = 15$ i $\mathrm{NWW}(x,y) = 420$,
e) $x+y = 667$ i $\mathrm{NWW}(x,y) = 120 \cdot \mathrm{NWD}(x,y)$.

Zadanie 22.147. Wyznacz wszystkie liczby naturalne x, y, z takie, że $2x^2 = 3y^3 = 5z^5$.

Zadanie 22.148. Niech s będzie liczbą wszystkich dzielników naturalnych liczby naturalnej n. Udowodnij, że iloczyn wszystkich dzielników naturalnych liczby n jest równy $\sqrt{n^s}$.

Zadanie 22.149. Udowodnij, że dla każdego naturalnego $n > 2$ istnieje n liczb naturalnych względnie pierwszych i takich, że każde $n-1$ liczb spośród nich nie są względnie pierwsze.

Zadanie 22.150. Udowodnij, że dla każdej liczby naturalnej n liczba $\frac{n^3}{6} + \frac{n^2}{2} + \frac{n}{3}$ jest całkowita.

Zadanie 22.151. Dane są ułamki $\frac{35}{396}$ i $\frac{28}{297}$. Znajdź najmniejszą liczbę dodatnią, przy dzieleniu której przez każdy z danych ułamków otrzymamy liczbę całkowitą.

Zadanie 22.152. Dane są ułamki $\frac{8}{15}$ i $\frac{18}{55}$. Znajdź taką największą liczbę, przy dzieleniu przez którą każdego z danych ułamków otrzymamy liczbę całkowitą.

Zadanie 22.153. Pokaż, że $1965 \mid 1^3 + 2^3 + \ldots + 1964^3$.

Zadanie 22.154. Udowodnij, że $11 \cdot 31 \cdot 61 \mid 20^{15} - 1$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.155. Udowodnij, że dla liczb naturalnych $n > 2$ liczba $\sqrt{n^2 - 4}$ jest niewymierna.

Zadanie 22.156. Znajdź resztę z dzielenia przez 7 liczby $2222^{5555} + 5555^{2222}$.

Zadanie 22.157. Znajdź ostatnie cyfry liczb: 6^{1971}, 9^{1971}, 3^{1971}, 2^{1971}.

Zadanie 22.158. Iloma zerami kończy się liczba $100! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 100$?

Zadanie 22.159. Niech n będzie największą trzycyfrową liczbą naturalną taką, że $15n - 8$ dzieli się przez 34 i jednocześnie $3n^2 + 3n + 2$ ma resztę 3 z dzielenia przez 5. Wyznacz liczbę dzielników naturalnych liczby n.

Zadanie 22.160. Niech $a, m, n \in \mathbb{N}$ będą takie, że $a > 1$. Udowodnij, że reszta z dzielenia liczby $a^n - 1$ przez liczbę $a^m - 1$ jest równa $a^r - 1$, gdzie r jest resztą z dzielenia liczby n przez liczbę m. Wyprowadź stąd wzór: $\mathrm{NWD}(a^m - 1, a^n - 1) = a^{NWD(m,n)} - 1$ i uzasadnij, że $a^m - 1 \mid a^n - 1 \iff m \mid n$.

Zadanie 22.161. Obliczyć $\mathrm{NWD}(2^{63} - 1, 2^{91} - 1)$.

Zadanie 22.162. W jaki sposób można odmierzyć 9 minut dwiema klepsydrami: 7 minutową i 11-minutową?

Zadanie 22.163. Udowodnij, że dla dowolnej liczby naturalnej n zachodzą wzory:
a) $\mathrm{NWW}(1, 2, \ldots, 2n) = \mathrm{NWW}(n + 1, n + 2, \ldots, 2n)$;
b) $\mathrm{NWW}(1, 2, \ldots, 2n + 1) = \mathrm{NWW}(n + 1, n + 2, \ldots, 2n + 1)$.

Zadanie 22.164. Pewna liczba naturalna przy dzieleniu przez 76 jak i przez 77 ma tę samą resztę równą 46. Jaką resztę otrzymamy przy dzieleniu tej liczby przez 14?

Zadanie 22.165. Smok ma 2000 głów. Rycerz może ściąć jednym cięciem 33 głowy lub 21 głów lub 17 głów lub 1 głowę. Smokowi odrasta odpowiednio: 48, 0, 14 i 349 głów jednocześnie. Zostanie on zabity, jeśli wszystkie głowy zostaną ścięte. Czy rycerz może zabić smoka?

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.166. Uczennica rozwiązała test złożony z 60 pytań. Za każdą dobrą odpowiedź otrzymała 11 punktów, za każdą złą - minus 8 punktów, za pytanie pozostawione bez odpowiedzi - 0 punktów. W sumie uczennica otrzymała 24 punkty. Na ile pytań odpowiedziała dobrze, a na ile źle? Znaleźć wszystkie możliwe rozwiązania.

Zadanie 22.167. Opisać wszystkie liczby naturalne n takie, że $7 \mid 2^n - 1$.

Zadanie 22.168. Udowodnij, że

$$\mathrm{NWD}(a, b) = \mathrm{NWD}(a + b, \mathrm{NWW}(a, b))$$

dla dowolnych liczb naturalnych a, b, c.

Zadanie 22.169. Wyznacz wszystkie liczby naturalne m, n takie, że $m^5 n^9 = 2^{24} \cdot 3^{45} \cdot 5^{30}$.

Zadanie 22.170. Czy wśród dziesięciu kolejnych liczb naturalnych większych od 3 może być 5 liczb pierwszych? Odpowiedź uzasadnij.

Zadanie 22.171. Czy wśród dwunastu kolejnych liczb naturalnych większych od 3 może być pięć liczb pierwszych? Odpowiedź uzasadnij.

Zadanie 22.172. Znajdź wszystkie różne liczby naturalne x i y takie, że $\frac{2}{7} = \frac{1}{x} + \frac{1}{y}$.

Zadanie 22.173. Różnica dwóch nieparzystych liczb całkowitych dzieli się przez 5. Jaką cyfrę jedności posiada liczba, która jest różnicą sześcianów tych liczb?

Zadanie 22.174. Udowodnij, że dla parzystych liczb całkowitych n liczba $n^4 - 4n^3 - 4n^2 + 16n$ jest podzielna przez 384.

Zadanie 22.175. Opisać liczby, które są różnicami kwadratów dwóch liczb całkowitych.

Zadanie 22.176. Czy istnieją liczby naturalne x, y, z takie, że $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{8}{11}$?

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.177. Udowodnij, że nie istnieją liczby całkowite x, y, z takie, że $2x^2 - 5y^2 = 8z \pm 1$.

Zadanie 22.178. Wyznacz wszystkie liczby naturalne x, y, z takie, że $xyz = x + y + z$.

Zadanie 22.179. Dla każdej liczby naturalnej n sumę jej cyfr oznaczmy przez $S(n)$. Udowodnić, że jeżeli $n \in \mathbb{N}$ i $S(n) = S(6n)$, to $9 \mid n$.

Zadanie 22.180. Udowodnij, że jeżeli $a, b, c, d \in \mathbb{Z}$ i $a - c \mid ab + cd$, to $a - c \mid ad + bc$.

Zadanie 22.181. Udowodnij, że jeżeli liczby naturalne a i $n > 1$ są względnie pierwsze, to $n \mid a^d - 1$ dla pewnej liczby naturalnej $d < n$.

Zadanie 22.182. Każda z liczb naturalnych a, b, c, d jest podzielna przez $ab - cd$. Udowodnij, że $|ab - cd| = 1$.

Zadanie 22.183. Udowodnij, że jeżeli liczba naturalna ma 3^n cyfr ($n \in \mathbb{N}$) i wszystkie cyfry są jednakowe, to liczba ta dzieli się przez 3^n.

Zadanie 22.184. Znajdź najmniejszą trzycyfrową liczbę naturalną n taką, że $55 \mid 11n^2 + 3n + 17$.

Zadanie 22.185. Niech $a, b \in \mathbb{Z}$ będą takie, że $17 \mid 3a + 2b$. Udowodnij, że wtedy $17 \mid 10a + b - 51$.

Zadanie 22.186. Niech $a, b \in \mathbb{N}$ będą takie, że $\frac{a+1}{b} + \frac{b+1}{a} \in \mathbb{N}$ i niech $d = \mathrm{NWD}(a, b)$. Pokazać, że wtedy $d^2 \leqslant a + b$.

Zadanie 22.187. Niech S będzie zbiorem wszystkich takich liczb naturalnych n, że wśród cyfr liczby n są dokładnie dwa zera, te dwa zera są kolejnymi cyframi i jeżeli je pominąć, to otrzymamy liczbę 76 razy mniejszą niż n. Ile elementów ma zbiór S? Odpowiedź uzasadnić.

Zadanie 22.188. Niech S będzie zbiorem wszystkich takich liczb naturalnych n, że wszystkie cyfry liczby $23n$ są jednakowe.

a) Znaleźć najmniejszą liczbę należącą do zbioru S,

b) Udowodnij, że zbiór S jest nieskończony.

Zadanie 22.189. Udowodnij, że jeżeli liczby całkowite x, y, z spełniają równanie $x^2 + y^2 = z^2$, to $60 \mid xyz$.

Zadanie 22.190. Niech S będzie zbiorem wszystkich takich liczb naturalnych n, że liczba n^2 ma trzy razy więcej dzielników naturalnych niż liczba n.

a) Udowodnij, że jeżeli $n \in S$, to w rozkładzie kanonicznym liczby n występują dokładnie dwie liczby pierwsze,

b) Znajdź najmniejszą liczbę należącą do zbioru S.

Zadanie 22.191. Udowodnij, że jeżeli s jest sumą cyfr liczby naturalnej n, to s i $10n$ mają taką samą resztę z dzielenia przez 9.

Zadanie 22.192. Znajdź największą trzycyfrową liczbę naturalną n taką, że $59 \mid 12n - 35$ i jednocześnie $[5n]_3 = 1$.

Zadanie 22.193. Udowodnij, że nie istnieje liczba naturalna k taka, że $18k + 1$ jest różnicą dwóch liczb pierwszych.

Zadanie 22.194. Dla jakiej liczby naturalnej n, $n^2 + 4n - 8$ jest kwadratem liczby naturalnej?

Zadanie 22.195. Mówimy, że niepusty podzbiór X zbioru $\mathbb{Z}$ jest ograniczony z dołu, jeżeli istnieje liczba całkowita a taka, że $a \leqslant x$ dla każdego $x \in X$. Udowodnij, że każdy niepusty i ograniczony z dołu podzbiór X zbioru $\mathbb{Z}$ posiada element najmniejszy, to znaczy istnieje $x_0 \in X$ takie, że $x_0 \leqslant x$ dla każdego $x \in X$ (twierdzenie to nazywamy **zasadą minimum w zbiorze** $\mathbb{Z}$).

Zadanie 22.196. Niech $n_0 \in \mathbb{Z}$ i niech A będzie podzbiorem zbioru $\mathbb{Z}$ takim, że $n_0 \in A$ oraz dla każdej liczby całkowitej $k \geqslant n_0$ prawdziwa jest implikacja:

$$k \in A \Rightarrow k + 1 \in A.$$

Udowodnij, że wówczas każda liczba całkowita n większa lub równa n_0 należy do A (twierdzenie to nazywamy **zasadą indukcji matematycznej**).

Zadanie 22.197. Niech $a, b, m \in \mathbb{N}$ będą takie, że $m \mid a + b$ i $m \mid a^2 + b$. Udowodnij, że wówczas $m \mid a^n + b$ dla każdego $n \in \mathbb{N}$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.198. Udowodnij za pomocą zasady indukcji matematycznej, że $25 \mid 2^{n+2} \cdot 3^n + 5n - 4$ dla każdego $n \in \mathbb{N}_0$.

Zadanie 22.199. Udowodnij za pomocą zasady indukcji matematycznej, że $64 \mid 3^{2n+1} + 40n - 3$ dla każdego $n \in \mathbb{N}_0$.

Zadanie 22.200. Znajdź wszystkie liczby naturalne n, dla których każda z liczb n, $n+2$, $n+6$, $n+8$, $n+12$, $n+14$ jest liczbą pierwszą.

Zadanie 22.201. Liczbę naturalną n nazywamy liczbą doskonałą, jeżeli $n > 1$ i n jest sumą wszystkich swoich dzielników naturalnych mniejszych od n. Udowodnij, że jeżeli p jest liczbą pierwszą taką, że $2^p - 1$ też jest liczbą pierwszą, to $n = 2^{p-1}(2^p - 1)$ jest liczbą doskonałą.

Zadanie 22.202. Korzystając z zadania 22.201 znajdź trzy różne liczby doskonałe.

Zadanie 22.203. Udowodnij, że 8128 jest liczbą doskonałą.

Zadanie 22.204. Niech p będzie liczbą pierwszą. Pokazać, że jeżeli $2^p - 1$ nie jest liczbą pierwszą, to liczba $2^{p-1}(2^p - 1)$ nie jest doskonała.

Zadanie 22.205. Udowodnij, że liczba $2^{10} \cdot (2^{11} - 1)$ nie jest doskonała.

Zadanie 22.206. Liczbami Fermata nazywamy liczby postaci: $F_n = 2^{2^n} + 1$ dla $n \in \mathbb{N}_0$. Udowodnij, że dla dowolnego $n \in \mathbb{N}$ zachodzi wzór:

$$F_0 \cdot F_1 \cdot \ldots \cdot F_n = F_{n+1} - 2. \tag{22.3}$$

Zadanie 22.207. Udowodnij następujące własności liczb Fermata:
(i) $F_0 < F_1 < F_2 < \ldots$,
(ii) F_n jest nieparzystą liczbą naturalną większą od 1 dla każdego $n \in \mathbb{N}_0$,
(iii) dla dowolnych różnych liczb $m, n \in \mathbb{N}_0$ liczby F_n i F_m są względnie pierwsze.

Zadanie 22.208. Udowodnij opierając się na zadaniu 22.207, że liczb pierwszych jest nieskończenie wiele.

Zadanie 22.209. Udowodnij, że dla każdego naturalnego $n \geqslant 2$ cyfra jedności liczby Fermata F_n jest równa 7.

Zadanie 22.210. Znajdź wszystkie liczby naturalne $a, n > 1$ takie, że $a^n - 1$ i $a^n + 1$ są jednocześnie liczbami pierwszymi.

Zadanie 22.211. Czy można z cyfr 1, 2, 3, 4, 5, 6, wykorzystując każdą tylko raz, utworzyć liczbę sześciocyfrową podzielną przez 11?

Zadanie 22.212. Wyznacz wszystkie liczby pierwsze p takie, że $4p^2 + 1$ i $6p^2 + 1$ też są liczbami pierwszymi.

Zadanie 22.213. Udowodnij, że jeżeli a i b są liczbami naturalnymi takimi, że $40a = 51b$, to $a + b$ jest liczbą złożoną.

Zadanie 22.214. Udowodnij, że dla dowolnych $x, y, z \in \mathbb{Z}$: jeśli $17 \mid 2x + 4y + 5z$, to $17 \mid 3x + 6y - z$.

Zadanie 22.215. Udowodnij, że dla dowolnych liczb naturalnych a i b:

$$\mathrm{NWD}(5a + 3b, 13a + 8b) = \mathrm{NWD}(a, b).$$

Zadanie 22.216. Udowodnij, że dla dowolnych liczb naturalnych a, b, n:

$$\mathrm{NWD}(a^n, b^n) = [\mathrm{NWD}(a, b)]^n.$$

Zadanie 22.217. Znajdź różne liczby naturalne a, b, c takie, że liczby: $a + b + c, a + b, a + c, b + c$ są kwadratami liczb naturalnych.

Zadanie 22.218. Udowodnij, że nie istnieje liczba naturalna $n > 1$ taka, że $1 + \frac{1}{2} + \ldots + \frac{1}{n}$ jest liczbą całkowitą.

Zadanie 22.219. Niech p będzie nieparzystą liczbą pierwszą. Udowodnij, że wszystkimi różnymi resztami z dzielenia kwadratów liczb całkowitych przez p są $[0^2]_p, [1^2]_p, \ldots, [(\frac{p-1}{2})^2]_p$.

Zadanie 22.220. Udowodnij, że dla liczb całkowitych x liczba $2x^2 + 29$ nie jest podzielna przez żadną liczbę pierwszą mniejszą od 29.

Zadanie 22.221. Sprawdź, że $2x^2 + 29$ jest liczbą pierwszą dla $x = 0, 1, \ldots, 28$.

Zadanie 22.222. Udowodnij, że dla liczb całkowitych x liczba $x^2 + 163$ nie jest podzielna przez żadną nieparzystą liczbę pierwszą mniejszą od 41.

Zadanie 22.223. Sprawdź, że $x^2 - x + 41$ jest liczbą pierwszą dla $x = 1, \ldots, 40$.

Zadanie 22.224. Wykaż, że jeśli $a^2 + b^2 = (a + b - c)^2$ i $b \neq c$, to

$$\frac{a^2 + (a-c)^2}{b^2 + (b-c)^2} = \frac{a-c}{b-c}.$$

Zadanie 22.225. Udowodnij, że dla dowolnego $n \in \mathbb{N}$ liczba $\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$ nie jest całkowita.

Zadanie 22.226. Niech a i b będą liczbami naturalnymi większymi od 1. Pokazać, że $\log_a b$ jest liczbą wymierną wtedy i tylko wtedy, gdy istnieją liczby naturalne $n > 1$ oraz p i q takie, że $a = n^p$ i $b = n^q$. W szczególności, jeśli a i b są względnie pierwszymi liczbami naturalnymi większymi od 1, to liczba $\log_a b$ jest niewymierna.

Zadanie 22.227. Udowodnij, że istnieją dodatnie liczby niewymierne a i b takie, że a^b jest liczbą wymierną.

Zadanie 22.228. Wskaż konkretny przykład niewymiernych dodatnich liczb rzeczywistych a i b, dla których liczba a^b jest wymierna.

Zadanie 22.229. Czy liczbę 5555555 można przedstawić w postaci sumy dwóch liczb pierwszych?

Zadanie 22.230. Niech k będzie liczbą naturalną niepodzielną przez 3. Pokazać, że dla dowolnego $n \in \mathbb{N}$:

$$n^2 + n + 1 \mid n^{2k} + n^k + 1.$$

Zadanie 22.231. Niech $k > 1$ będzie liczbą naturalną niepodzielną przez 3. Wyznacz wszystkie liczby naturalne n, dla których $n^{2k} + n^k + 1$ jest liczbą pierwszą.

Zadanie 22.232. Udowodnij, że $121 \mid 10^{11} + 1$.

Zadanie 22.233. Korzystając z zadania 22.232 znajdź liczbę naturalną a o tej własności, że po dopisaniu z jej lewej strony liczby a uzyskamy liczbę będącą kwadratem liczby naturalnej.

Zadanie 22.234. Niech a będzie liczbą naturalną s-cyfrową o tej własności, że po dopisaniu z jej lewej strony liczby a uzyskamy liczbę będącą kwadratem liczby naturalnej. Udowodnić, że wówczas $10^s + 1$ jest podzielne przez kwadrat liczby pierwszej.

Zadanie 22.235. Znajdź wszystkie liczby całkowite x i y takie, że $x + y = (x - y)^2$.

Zadanie 22.236. Udowodnij, że nie istnieją $x, y \in \mathbb{Z}$ takie, że $2x^2 - 5y^2 = 6$.

Zadanie 22.237. Znajdź wszystkie $x, y \in \mathbb{Z}$ takie, że $3^x - 2^y = 1$.

Zadanie 22.238. Znajdź wszystkie $x, y \in \mathbb{Z}$ takie, że $x^3 + y^3 + 1 = 3xy$.

Zadanie 22.239. Udowodnij, że nie istnieją $x, y \in \mathbb{Z}$ takie, że

$$2x^2 - 4x - 5y^2 - 10y = 10.$$

Zadanie 22.240. Wyznacz wszystkie $x, y \in \mathbb{Z}$ takie, że

$$\frac{1}{x^2} + \frac{1}{xy} + \frac{1}{y^2} = 1.$$

Zadanie 22.241. Wyznacz wszystkie liczby naturalne x i y takie, że $2x^2 + 5xy - 12y^2 = 28$.

Zadanie 22.242. Wyznacz wszystkie liczby naturalne n, dla których $n^8 + n^6 + n^4 + n^2 + 1$ jest liczbą pierwszą.

Zadanie 22.243. Wyznacz wszystkie $x, y \in \mathbb{Z}$ takie, że $x + y = 5$ i $2^x + 3^y = 17$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.244. Udowodnij, że $2^n > n+1$ dla każdego naturalnego $n \geqslant 2$.

Zadanie 22.245. Wyznacz wszystkie $x, y \in \mathbb{N}$ takie, że $x^y = xy$.

Zadanie 22.246. Wyznacz wszystkie $x, y \in \mathbb{N}$ takie, że $x^y = y^x$.

Zadanie 22.247. Udowodnij, że równanie $x^2+xy-y^2 = 1$ posiada nieskończenie wiele rozwiązań w liczbach naturalnych x i y.

Zadanie 22.248. Wiedząc, że $x + \frac{1}{x} = 3$ oblicz $x^5 + \frac{1}{x^5}$.

Zadanie 22.249. Niech a i b będą liczbami rzeczywistymi, których suma równa jest 1. Wykazać, że jeżeli a^3 i b^3 są liczbami wymiernymi, to a i b też są liczbami wymiernymi.

Zadanie 22.250. Liczba x jest rzeczywista i taka, że $x^5 - x$ oraz $x^2 - 1$ są obie całkowite. Pokaż, że x jest również całkowite.

Zadanie 22.251. Udowodnij, że dla dowolnych liczb naturalnych m i n zachodzi wzór:

$$\mathrm{NWD}(\underbrace{11\ldots1}_{n}, \underbrace{11\ldots1}_{m}) = \underbrace{11\ldots1}_{\mathrm{NWD}(n,m)}.$$

Zadanie 22.252. Udowodnij, że w ciągu $1, 11, 111, 1111, \ldots$ istnieje podciąg złożony z liczb parami względnie pierwszych.

Zadanie 22.253. Udowodnij, że $n^2 \mid (n+1)^n - 1$ dla każdego $n \in \mathbb{N}$.

Zadanie 22.254. Udowodnij, że $2^n \mid (n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)$ dla każdego $n \in \mathbb{N}$.

Zadanie 22.255. Wyznacz wszystkie liczby naturalne n, dla których $4^n + 65$ jest kwadratem liczby naturalnej.

Zadanie 22.256. Udowodnij, że dla każdej liczby naturalnej n liczba $n^4 + 2n^3 + 2n^2 + 2n + 1$ nie jest kwadratem liczby naturalnej.

Zadanie 22.257. Znajdź wszystkie liczby naturalne n, dla których $101 \mid n^2 + 8n - 65$.

Zadanie 22.258. Wyznacz wszystkie liczby pierwsze a, b, c takie, że $a^2 = b^2 + c$.

Zadanie 22.259. Wyznacz wszystkie liczby naturalne n, dla których $\frac{n^4+4}{17}$ jest liczbą pierwszą.

Zadanie 22.260. Wyznacz wszystkie $n \in \mathbb{N}$ takie, że $17 \mid n^4 + 4$.

Zadanie 22.261. Udowodnij, że dla każdego $k \in \mathbb{N}_0$:

$$n^2 + n + 1 \mid n^{3k+2} + n + 1.$$

Zadanie 22.262. Znajdź wszystkie liczby całkowite x, y, z takie, że

$$\frac{yz}{x} + \frac{xz}{y} + \frac{xy}{z} = 3.$$

Zadanie 22.263. Udowodnij, że jeżeli $a, b, c, d \in \mathbb{Z}$ i $ad - bc = \pm 1$, to dla każdego $n \in \mathbb{Z}$ liczby $an + b$ i $cn + d$ są względnie pierwsze.

Zadanie 22.264. Udowodnij, że jeżeli liczby naturalne $a, n > 1$ są takie, że $a^n + 1$ jest liczbą pierwszą, to $n = 2^k$ dla pewnej liczby naturalnej k.

Zadanie 22.265. Wyznacz wszystkie liczby naturalne n takie, że $n^n + 1$ i $(2n)^{2n} + 1$ są liczbami pierwszymi.

Zadanie 22.266. Udowodnij, że jeżeli p jest liczbą pierwszą i $p \equiv 31 \pmod{40}$, to $p \nmid 10^n + 1$ dla dowolnej liczby naturalnej n.

Zadanie 22.267. Wyznacz najmniejszą liczbę naturalną n taką, że $2n = x^2$ i $3n = y^3$ i $4n = z^5$ dla pewnych liczb naturalnych x, y, z.

Zadanie 22.268. Wyznacz wszystkie liczby całkowite k takie, że $3k + 4 \mid 7k + 1$.

Zadanie 22.269. Udowodnij, że dla dowolnej nieparzystej liczby naturalnej a niepodzielnej przez 5 pewien wyraz ciągu

$$1, 11, 111, 1111, \ldots$$

jest podzielny przez a.

Zadanie 22.270. Niech a, b i c będą liczbami naturalnymi takimi, że $2c^2 = 3ab$. Udowodnij, że wówczas liczba $a^3+b^3+c^3$ nie jest pierwsza.

Zadanie 22.271. Udowodnij, że nie istnieje liczba naturalna $n > 1$ taka, że $n \mid 2^n - 1$.

Zadanie 22.272. Udowodnij twierdzenie Eulera, które mówi, że dla dowolnych liczb naturalnych x i y liczba $4xy - x - y$ nie jest kwadratem liczby całkowitej.

Zadanie 22.273. Udowodnij, że $2^n \nmid 3^n + 1$ dla każdej liczby naturalnej $n > 1$.

Zadanie 22.274. Wyznacz trzy ostatnie cyfry liczby n^{100} w zależności od wartości $n \in \mathbb{N}$.

Zadanie 22.275. Niech $a, b, c, d \in \mathbb{N}$ i $ab = cd$. Udowodnij, że wtedy

$$\frac{\mathrm{NWD}(a,c) \cdot \mathrm{NWD}(a,d)}{\mathrm{NWD}(a,b,c,d)} = a.$$

Zadanie 22.276. Udowodnij, że $a^3 \equiv 0, -1, 1 \pmod 9$ dla każdej liczby całkowitej a. Wykorzystaj to do pokazania, że dla każdego $k \in \mathbb{Z}$ ani liczba $9k + 4$ i ani liczba $9k + 5$ nie jest sumą sześcianów trzech liczb całkowitych.

Zadanie 22.277. Udowodnij, że każda liczba całkowita jest sumą sześcianów pięciu liczb całkowitych.

Zadanie 22.278. Udowodnij, że $a! \cdot (p-1-a)! \equiv (-1)^{a+1} \pmod p$ dla każdej liczby pierwszej p i dla dowolnego $a = 0, 1, \ldots, p-1$.

Zadanie 22.279. Udowodnij, że $\binom{np}{p} \equiv n \pmod{p^2}$ dla każdej liczby pierwszej p i dla dowolnego $n \in \mathbb{N}$.

Zadanie 22.280. Udowodnij, że $\binom{n}{p} \equiv \lfloor \frac{n}{p} \rfloor \pmod{p^2}$ dla każdej liczby pierwszej p i dla dowolnej liczby naturalnej $n \geqslant p$.

Rozdział 23

Rozwiązania zadań

Zadanie 22.1. Wyznaczamy dzielniki liczby 18: ponieważ $4^2 = 16 \leqslant$ $\leqslant 18 < 25 = 5^2$, więc wypisujemy liczby $1, 2, 3, 4$ i kolejno badamy, która z nich dzieli liczbę 18: $1 \mid 18$ i $1' = \frac{18}{1} = 18$, $2 \mid 18$ i $2' = \frac{18}{2} = 9$, $3 \mid 18$ i $3' = \frac{18}{3} = 6$, $4 \nmid 18$, bo $18 = 4 \cdot 4 + 2$ i $[18]_4 = 2 \neq 0$. Wobec tego na mocy twierdzenia 8.16 wszystkimi dzielnikami liczby 18 są: $1, 18, 2, 9, 3, 6$, co zapisujemy formalnie: $D_{18} = \{1, 18; 2, 9; 3, 6\}$.

Wyznaczamy dzielniki liczby 24: ponieważ $4^2 = 16 \leqslant 24 < 25 = 5^2$, więc wypisujemy liczby $1, 2, 3, 4$ i kolejno badamy, która z nich dzieli liczbę 24: $1 \mid 24$ i $1' = \frac{24}{1} = 24$, $2 \mid 24$ i $2' = \frac{24}{2} = 12$, $3 \mid 24$ i $3' = \frac{24}{3} = 8$, $4 \mid 24$ i $4' = \frac{24}{4} = 6$. Wobec tego na mocy twierdzenia 8.16 wszystkimi dzielnikami liczby 24 są: $1, 24, 2, 12, 3, 8, 4, 6$, co zapisujemy formalnie: $D_{24} = \{1, 24; 2, 12; 3, 8; 4, 6\}$.

Wyznaczamy dzielniki liczby 30: ponieważ $5^2 = 25 \leqslant 30 < 36 =$ $= 6^2$, więc wypisujemy liczby $1, 2, 3, 4, 5$ i kolejno badamy, która z nich dzieli liczbę 30: $1 \mid 30$ i $1' = \frac{30}{1} = 30$, $2 \mid 30$ i $2' = \frac{30}{2} = 15$, $3 \mid 30$ i $3' = \frac{30}{3} = 10$, $4 \nmid 30$, bo $30 = 7 \cdot 4 + 2$ i $[30]_4 = 2$, $5 \mid 30$ i $5' = \frac{30}{5} = 6$. Wobec tego na mocy twierdzenia 8.16 wszystkimi dzielnikami liczby 30 są: $1, 30, 2, 15, 3, 10, 5, 6$, co zapisujemy formalnie: $D_{30} = \{1, 30; 2, 15; 3, 10; 5, 6\}$.

Wyznaczamy dzielniki liczby 48: ponieważ $6^2 = 36 \leqslant 48 < 49 = 7^2$, więc wypisujemy liczby $1, 2, 3, 4, 5, 6$ i kolejno badamy, która z nich dzieli liczbę 48: $1|48$ i $1' = \frac{48}{1} = 48$, $2|48$ i $2' = \frac{48}{2} = 24$, $3|48$ i $3' =$

$= \frac{48}{3} = 16$, $4|48$ i $4' = \frac{48}{4} = 12$, $5 \nmid 48$, bo ostatnia cyfra liczby 48 nie jest równa ani 0 ani 5, $6|48$ i $6' = \frac{48}{6} = 8$. Wobec tego na mocy twierdzenia 8.16 wszystkimi dzielnikami liczby 48 są: $1, 48, 2, 24, 3, 16, 4, 12, 6, 8$, co zapisujemy formalnie: $D_{48} = \{1, 48; 2, 24; 3, 16; 4, 12; 6, 8\}$.

Wyznaczamy dzielniki liczby 124: ponieważ $11^2 = 121 \leqslant 124 < 144 = 12^2$, więc wypisujemy liczby $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ i kolejno badamy, która z nich dzieli liczbę 124: $1 \mid 124$ i $1' = \frac{124}{1} = 124$, $2 \mid 124$ i $2' = \frac{124}{2} = 62$, $3 \nmid 124$, bo suma cyfr liczby 124 wynosi $1 + 2 + 4 = 7$ i nie dzieli się przez 3, $4 \mid 124$ i $4' = \frac{124}{4} = 31$, $5 \nmid 124$, bo ostatnia cyfra liczby 124 nie jest równa ani 0 ani 5, $6 \nmid 124$, bo $3 \nmid 124$ i $3 \mid 6$, $7 \nmid 124$, bo $124 = 17 \cdot 7 + 5$ i $[124]_7 = 5 \neq 0$, $8 \nmid 124$, bo $124 = 15 \cdot 8 + 4$ i $[124]_8 = 4$, $9 \nmid 124$, bo $3 \nmid 124$ i $3 \mid 9$, $10 \nmid 124$, bo $5 \nmid 124$ i $5 \mid 10$, $11 \nmid 124$, bo $124 = 11 \cdot 11 + 3$ i $[124]_{11} = 3 \neq 0$. Wobec tego na mocy twierdzenia 8.16 wszystkimi dzielnikami liczby 124 są: $1, 124, 2, 62, 4, 31$, co zapisujemy formalnie: $D_{124} = \{1, 124; 2, 62; 4, 31\}$.

Wyznaczamy dzielniki liczby 564: $23^2 = 529 \leqslant 564 < 576 = 24^2$, więc wypisujemy liczby $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23$ i kolejno badamy, która z nich dzieli liczbę 564: $1|564$ i $1' = \frac{564}{1} = 564$, $2|564$ i $2' = \frac{564}{2} = 282$, $3|564$ i $3' = \frac{564}{3} = 188$, $4|564$ i $4' = \frac{564}{4} = 141$, $5 \nmid 564$, bo ostatnia cyfra liczby 564 nie jest równa ani 0 ani 5, $6|564$ i $6' = \frac{564}{6} = 94$, $7 \nmid 564$, bo $564 = 80 \cdot 7 + 4$ i $[564]_7 = 5$, $8 \nmid 564$, bo $564 = 70 \cdot 8 + 4$ i $[564]_8 = 4$, $9 \nmid 564$, bo suma cyfr liczby 564 wynosi $5 + 6 + 4 = 15$ i nie dzieli się przez 9, $10 \nmid 564$, bo $5 \nmid 564$ i $5|10$, $11 \nmid 564$, bo $564 = 51 \cdot 11 + 3$ i $[564]_{11} = 3$, $12|564$ i $12' = \frac{564}{12} = 47$, $13 \nmid 564$, bo $564 = 43 \cdot 13 + 5$ i $[564]_{13} = 5 \neq 0$, $14 \nmid 564$, bo $7 \nmid 564$ i $7|14$, $15 \nmid 564$, bo $5 \nmid 564$ i $5|15$, $16 \nmid 564$, bo $8 \nmid 564$ i $8|16$, $17 \nmid 564$, bo $564 = 33 \cdot 17 + 3$ i $[564]_{17} = 3 \neq 0$, $18 \nmid 564$, bo $9 \nmid 564$ i $9|18$, $19 \nmid 564$, bo $564 = 29 \cdot 19 + 13$ i $[564]_{19} = 13 \neq 0$, $20 \nmid 564$, bo $5 \nmid 564$ i $5|20$, $21 \nmid 564$, bo $7 \nmid 564$ i $7|21$, $22 \nmid 564$, bo $11 \nmid 564$ i $11|22$. Wobec tego na mocy twierdzenia 8.16 wszystkimi dzielnikami liczby 564 są: $1, 564, 2, 282, 3, 188, 4, 141, 6, 94, 12, 47$, co zapisujemy formalnie: $D_{564} = \{1, 564; 2, 282; 3, 188; 4, 141; 6, 94; 12, 47\}$.

Zadanie 22.2. a). Ponieważ $n^2 + 1 = (n - 1) \cdot (n + 1) + 2$, więc

$n+1 \mid n^2+1$ wtedy i tylko wtedy, gdy $n+1 \mid 2$, ale $D_2 = \{1,2\}$ i $n+1 > 1$ dla $n \in \mathbb{N}$, więc $n+1 = 2$, skąd $n = 1$.

b). Załóżmy, że $n \in \mathbb{N}$ oraz $17n+1 \mid 19n+17$. Ponieważ $19n+17 = (17n+1)+(2n+16)$, więc $17n+1 \mid 2n+16$, skąd $17n+1 \leqslant 2n+16$, czyli $15n \leqslant 15$, a zatem $n \leqslant 1$, czyli $n = 1$. Ponadto, dla $n = 1$ mamy, że $17n+1 = 18$ i $19n+17 = 36 = 2 \cdot 18$, więc ostatecznie: $n = 1$.

c). Ponieważ $n^3 - 7n^2 - 5n + 10 = (n^2 - 9n + 13) \cdot (n+2) - 16$, więc $n+2 \mid n^3 - 7n^2 - 5n + 10 \iff n+2 \mid 16 \iff n+2 \in D_{16}$, ale $D_{16} = \{1,2,4,8,16\}$ i $n+2 \geqslant 3$ dla $n \in \mathbb{N}$, więc $n+2 = 4$ lub $n+2 = 8$ lub $n+2 = 16$, skąd $n = 2$ lub $n = 6$ lub $n = 14$.

d). Ponieważ $n^3 - 7n^2 - 5n + 10 = (n-2) \cdot (n^2 - 5n - 14) - (n+18)$, więc
$n^2 - 5n - 14 \mid n^3 - 7n^2 - 5n + 10 \iff n^2 - 5n - 14 \mid n + 18$, ale $n^2 - 5n - 14 = (n-7) \cdot (n+2)$, więc jeżeli $n^2 - 5n - 14 \mid n+18$, to $n - 7 \mid n + 18$ i $n + 2 \mid n + 18$. Ponadto $n + 18 = (n-7) + 25$ i $n + 18 = (n+2) + 16$, więc jeżeli $n^2 - 5n - 14 \mid n + 18$, to $n - 7 \mid 25$ i $n + 2 \mid 16$. Dalej, $D_{16} = \{1,2,4,8,16\}$ i $D_{25} = \{1,5,25\}$, więc jeżeli $n^2 - 5n - 14 \mid n+18$, to $n = 2$ lub $n = 6$, ale $2^2 - 5 \cdot 2 - 14 = -20 \mid 20$ i $2+18 = 20$ oraz $6^2 - 5 \cdot 6 - 14 = -8 \mid 24$ i $6+18 = 24$, więc ostatecznie $n = 2$ lub $n = 6$.

Zadanie 22.3. a). $x \mid x+1 \iff x \mid 1 \iff x \in \{1,-1\}$. Zatem $x = 1$ lub $x = -1$.

b). Ponieważ $2x = 2 \cdot (x+1) - 2$, więc $x+1 \mid 2x \iff x+1 \mid 2$. Zatem $x+1 \mid 2x \iff x+1 \in \{1,-1,2,-2\}$. Stąd $x \in \{-3,-2,0,1\}$.

c). Ponieważ $x^3 - 3 = (x^2 + 3x + 9) \cdot (x-3) + 24$, więc $x - 3 \mid x^3 - 3$ wtedy i tylko wtedy, gdy $x - 3 \mid 24$. Dalej, $D_{24} = \{1,2,3,4,6,8,12,24\}$, więc $x - 3 \mid x^3 - 3$ wtedy i tylko wtedy, gdy

$$x - 3 \in \{-24,-12,-8,-6,-4,-3,-2,-1,1,2,3,4,6,8,12,24\}.$$

Wobec tego $x \in \{-21,-9,-5,-3,-1,0,1,4,5,6,7,9,11,15,27\}$.

Zadanie 22.4. a). $-67 = (-8) \cdot 9 + 5$, więc $[-67]_9 = 5$. b). $123 = 17 \cdot 7 + 4$, więc $[123]_7 = 4$. c). $-78 = (-6) \cdot 14 + 6$, więc $[-78]_{14} = 6$. d). $169 = 13^2$, więc $[169]_{13} = 0$.

Zadanie 22.5. Oznaczmy tę liczbę całkowitą przez a. Wtedy z twierdzenia o dzieleniu z resztą $a = 66q + r$, gdzie $q, r \in \mathbb{Z}$ i $0 \leqslant r < 66$. Ponieważ $66 = 11 \cdot 6$, więc $[a]_{11} = [r]_{11}$ i $[a]_6 = [r]_6$. Zatem $[r]_{11} = 1$ i $[r]_6 = 4$. Biorąc pod uwagę pierwszy z tych warunków mamy, że $r \in \{1, 12, 23, 34, 45, 56\}$. Dalej, $[1]_6 = 1$, $[12]_6 = 0$, $[23]_6 = 5$, $[34]_6 = 4$, $[45]_6 = 3$ i $[56]_6 = 2$, więc ostatecznie $r = 34$. Zatem ta liczba z dzielenia przez 66 daje resztę 34.

Zadanie 22.6. a). $\mathrm{NWD}(198, 252) = \mathrm{NWD}(198, 252 - 198) = \mathrm{NWD}(54, 198) = \mathrm{NWD}(54, 198 - 3 \cdot 54) = \mathrm{NWD}(54, 36) = \mathrm{NWD}(36, 54 - 36) = \mathrm{NWD}(36, 18) = 18$, bo $18 \mid 36$.

b). $\mathrm{NWD}(221, 754) = \mathrm{NWD}(221, 754 - 3 \cdot 221) = \mathrm{NWD}(221, 91) = \mathrm{NWD}(91, 221 - 2 \cdot 91) = \mathrm{NWD}(39, 91) = \mathrm{NWD}(39, 91 - 2 \cdot 39) = \mathrm{NWD}(13, 39) = 13$, bo $13 \mid 39$.

c). $\mathrm{NWD}(225, 270, 360, 420) = \mathrm{NWD}(225, 270-225, 360-225, 420-225) = \mathrm{NWD}(225, 45, 135, 195) = \mathrm{NWD}(45, 225 - 5 \cdot 45, 135 - 3 \cdot 45, 195 - 4 \cdot 45) = \mathrm{NWD}(15, 45, 0, 0) = 15$, bo $15 \mid 45$ i $15 \mid 0$.

d). $\mathrm{NWD}(328, 1804) = \mathrm{NWD}(328, 1804 - 5 \cdot 328) = \mathrm{NWD}(328, 164) = 164$, bo $2 \cdot 164 = 328$.

e). $\mathrm{NWD}(522, 1551) = \mathrm{NWD}(522, 1551 - 2 \cdot 522) = \mathrm{NWD}(522, 507) = \mathrm{NWD}(507, 522 - 507) = \mathrm{NWD}(507, 15) = \mathrm{NWD}(15, 507 - 33 \cdot 15) = \mathrm{NWD}(15, 12) = \mathrm{NWD}(12, 15 - 12) = \mathrm{NWD}(12, 3) = 3$, bo $3 \mid 12$.

Zadanie 22.7. Ogólna postać trzech kolejnych liczb całkowitych: $k - 1$, k, $k + 1$, gdzie $k \in \mathbb{Z}$. Stąd suma ich kwadratów jest równa $(k-1)^2 + k^2 + (k+1)^2 = k^2 - 2k + 1 + k^2 + k^2 + 2k + 1 = 3k^2 + 2$, a więc ta suma daje resztę 2 z dzielenia przez 3.

Zadanie 22.8. Niech a będzie liczbą całkowitą niepodzielną przez 3. Z twierdzenia o dzieleniu z resztą wynika, że istnieje $k \in \mathbb{Z}$ takie, że $a = 3k + 1$ lub $a = 3k + 2$. W pierwszym przypadku $a^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, a ponieważ $3k^2 + 2k \in \mathbb{Z}$, więc a^2 daje resztę 1 z dzielenia przez 3. W drugim przypadku $a^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$, a ponieważ $3k^2 + 4k + 1 \in \mathbb{Z}$, więc a^2 daje resztę 1 z dzielenia przez 3.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.9. Iloczyn dwóch kolejnych liczb całkowitych jest postaci: $k(k+1)$ dla pewnego $k \in \mathbb{Z}$. Wystarczy zatem pokazać, że $2 \mid k$ lub $2 \mid k+1$. Z twierdzenia o dzieleniu z resztą wynika, że $k = 2n$ lub $k = 2n+1$ dla pewnego $n \in \mathbb{Z}$. W pierwszym przypadku $2 \mid k$, zaś w drugim przypadku $k+1 = 2(n+1)$ i $n+1 \in \mathbb{Z}$, więc $2 \mid k+1$. Kończy to nasz dowód.

Zadanie 22.10. Iloczyn trzech kolejnych liczb całkowitych jest postaci $k(k+1)(k+2)$, gdzie $k \in \mathbb{Z}$. Wystarczy zatem pokazać, że pewna z liczb $k, k+1, k+2$ jest podzielna przez 3. Z twierdzenia o dzieleniu z resztą wynika, że $k = 3n$ lub $k = 3n+1$ lub $k = 3n+2$ dla pewnego $n \in \mathbb{Z}$. W pierwszym przypadku $3 \mid k$, w drugim przypadku, $k+2 = 3(n+1)$ i $n+1 \in \mathbb{Z}$, więc $3 \mid k+2$. Zaś w trzecim przypadku, $k+1 = 3(n+1)$ i $n+1 \in \mathbb{Z}$, więc $3 \mid k+1$. Kończy to nasz dowód.

Zadanie 22.11. a). Dla $n \in \mathbb{Z}$: $n^2 - n = (n-1)n$ jest iloczynem dwóch kolejnych liczb całkowitych $n-1$ i n, więc na mocy zadania 22.9 ten iloczyn jest podzielny przez 2.

b). Dla $n \in \mathbb{Z}$: $n^3 - n = n(n^2-1) = n(n-1)(n+1) = (n-1)n(n+1)$ jest iloczynem trzech kolejnych liczb całkowitych $n-1, n, n+1$, więc na mocy zadania 22.10 ten iloczyn jest podzielny przez 3.

Zadanie 22.12. Iloczyn dwóch kolejnych parzystych liczb całkowitych jest postaci: $2n(2n+2)$ dla pewnego $n \in \mathbb{Z}$. Dalej, $2n(2n+2) = 4 \cdot n(n+1)$ i z zadania 22.9, $n(n+1) = 2m$ dla pewnego $m \in \mathbb{Z}$, skąd $2n(2n+2) = 8m$. Zatem liczba $2n(2n+2)$ jest podzielna przez 8.

Zadanie 22.13. Ogólna postać kwadratu liczby nieparzystej: $(2n+1)^2$ dla pewnego $n \in \mathbb{Z}$, ale $(2n+1)^2 - 1 = 2n(2n+2)$ jest iloczynem dwóch kolejnych liczb parzystych, więc na mocy zadania 22.12 jest on podzielny przez 8. Stąd liczby $(2n+1)^2$ i 1 dają tę samą resztę z dzielenia przez 8. Zatem liczba $(2n+1)^2$ daje resztę 1 z dzielenia przez 8.

Zadanie 22.14. Ponieważ jest dokładnie 5 różnych reszt z dzielenia przez 5, więc wśród dowolnych sześciu liczb całkowitych istnieją dwie liczby a i b dające tę samą resztę r z dzielenia przez 5. Zatem $a = 5k+r$

i $b = 5l + r$ dla pewnych $k, l \in \mathbb{Z}$. Stąd $a - b = 5(k - l)$ i $k - l \in \mathbb{Z}$, więc $5 \mid a - b$, co należało udowodnić.

Zadanie 22.15. Możliwe są tylko dwa przypadki: 1) wśród tych liczb istnieją co najmniej trzy liczby dające tę samą resztę r z dzielenia przez 3, 2) wśród tych liczb nie ma trzech liczb dających tę samą resztę z dzielenia przez 3.

W przypadku 1) mamy trzy liczby a, b, c takie, że $a = 3k + r$, $b = 3l+r$ i $c = 3t+r$ dla pewnych $k, l, t \in \mathbb{Z}$, skąd $a+b+c = 3(k+l+t+r)$ i $k + l + t + r \in \mathbb{Z}$, więc $3 \mid a + b + c$.

Rozważmy teraz przypadek 2). Ponieważ resztami z dzielenia przez 3 są: $0, 1, 2$, a mamy 5 liczb całkowitych a, b, c, d, e, więc $0, 1, 2 \in \{[a]_3, [b]_3, [c]_3, [d]_3, [e]_3\}$, bo inaczej pewna reszta powtarzałaby się co najmniej trzy razy. Możemy zakładać, że $[a]_3 = 0$, $[b]_3 = 1$ i $[c]_3 = 2$. Wtedy $a = 3k$, $b = 3l + 1$ i $c = 3t + 2$ dla pewnych $k, l, t \in \mathbb{Z}$. Stąd $a + b + c = 3(k + l + t + 1)$ i $k + l + t + 1 \in \mathbb{Z}$, więc $3 \mid a + b + c$.

Zadanie 22.16. Z założenia wynika, że $b = k \cdot a$ i $d = l \cdot c$ dla pewnych $k, l \in \mathbb{Z}$. Stąd $bd = (kl) \cdot (ac)$, ale $kl \in \mathbb{Z}$, więc $ac \mid bd$.

Zadanie 22.17. Z twierdzenia 8.44: $\mathrm{NWW}(a, b) = \frac{ab}{\mathrm{NWD}(a,b)}$ dla dowolnych $a, b \in \mathbb{N}$.

Stąd i z zadania 22.6 mamy, że $\mathrm{NWW}(1804, 328) = \frac{328 \cdot 1804}{164} = 3608$ oraz $\mathrm{NWW}(522, 1551) = \frac{522 \cdot 1551}{3} = 269874$. Ponadto korzystając z algorytmu Euklidesa mamy, że $\mathrm{NWD}(722, 874) = \mathrm{NWD}(722, 152) = \mathrm{NWD}(152, 114) = \mathrm{NWD}(114, 38) = 38$, bo $38 \mid 114$.
Zatem $\mathrm{NWW}(722, 874) = \frac{722 \cdot 874}{38} = 16606$.

Zadanie 22.18. Najmniejsza liczba naturalna podzielna przez 18 i 24 to po prostu najmniejsza wspólna wielokrotność tych liczb, ale $\mathrm{NWD}(18, 24) = \mathrm{NWD}(18, 6) = 6$, więc na mocy twierdzenia 8.44, $\mathrm{NWW}(18, 24) = \frac{18 \cdot 24}{6} = 3 \cdot 24 = 72$.

Zadanie 22.19. Z założenia wynika, że dla każdego $i = 1, 2, \ldots, n$ istnieje $t_i \in \mathbb{Z}$ takie, że $a_i = t_i \cdot a$. Stąd $c_1a_1 + c_2a_2 + \ldots + c_na_n = t_1ac_1 + t_2ac_2 + \ldots + t_nac_n = (t_1c_1 + t_2c_2 + \ldots + t_nc_n)a$. A ponieważ $t_1c_1 + t_2c_2 + \ldots + t_nc_n \in \mathbb{Z}$, więc $a \mid c_1a_1 + c_2a_2 + \ldots + c_na_n$.

Zadanie 22.20. Niech $a = c_0 + 10c_1 + \ldots + 10^s c_s$, gdzie $c_0, \ldots, c_s \in \{0, 1, \ldots, 9\}$, $s \in \mathbb{N}$ i $c_s \neq 0$. Wówczas naprzemienna suma cyfr liczby a jest równa $C = c_0 - c_1 + c_2 - \ldots + (-1)^s c_s$. Stąd $a - C = (10 - (-1)^1)c_1 + \ldots + (10^s - (-1)^s)c_s$. Z zadania 22.89 c), $11 \mid 10^k - (-1)^k$ dla każdego $k = 1, 2, \ldots, s$. Zatem na mocy zadania 22.19, $11 \mid a - C$. Stąd na mocy stwierdzenia 8.8 (6), $11 \mid a \iff 11 \mid C$.

Zadanie 22.21. Załóżmy, że tak nie jest. Wtedy istnieją liczby całkowite a, k, l takie, że $a = 18k + 13$ i $a = 21l + 2$, skąd $18k + 13 = 21l + 2$. Zatem $18k - 21l = -11$, czyli $3(6k - 7l) = -11$, ale $6k - 7l \in \mathbb{Z}$, więc $3 \mid 11$ i mamy sprzeczność. Wobec tego nie istnieje liczba całkowita, która przy dzieleniu przez 18 daje resztę 13, a przy dzieleniu przez 21 daje resztę 2.

Zadanie 22.22. Mamy: $6^2 = 2^{20} \cdot 3^{20}$, $10^{18} = 2^{18} \cdot 5^{18}$ i $15^{16} = 3^{16} \cdot 5^{16}$. Zatem $6^{20} \cdot 10^{18} \cdot 15^{16} = 2^{38} \cdot 3^{36} \cdot 5^{34}$, więc ze stwierdzenia 9.23 liczba wszystkich dzielników tej liczby wynosi $39 \cdot 37 \cdot 35 = 50505$.

Zadanie 22.23. Z rozwiązania zadania 22.22 otrzymujemy, że $6^{20} \cdot 10^{18} \cdot 15^{16} = 2^{38} \cdot 3^{36} \cdot 5^{34}$. Ponadto $12^4 \cdot 18^{20} = (2^2 \cdot 3)^4 \cdot (2 \cdot 3^2)^{20} = 2^{28} \cdot 3^{44}$. Zatem z twierdzenia 9.30, $\mathrm{NWD}(6^{20} \cdot 10^{18} \cdot 15^{16}, 12^4 \cdot 18^{20}) = 2^{28} \cdot 3^{36}$. Z twierdzenia 8.39 każdy wspólny dzielnik liczb $6^{20} \cdot 10^{18} \cdot 15^{16}$ i $12^4 \cdot 18^{20}$ jest dzielnikiem ich największego dzielnika. Wobec tego liczba wspólnych dzielników tych liczb jest równa liczbie wszystkich dzielników liczby $2^{28} \cdot 3^{36}$, czyli na mocy stwierdzenia 9.23 wynosi $29 \cdot 37 = 1073$.

Zadanie 22.24. Za pomocą algorytmu Euklidesa obliczamy: $\mathrm{NWD}(168, 396) = \mathrm{NWD}(168, 60) = \mathrm{NWD}(60, 48) = \mathrm{NWD}(48, 12) = 12$, bo $12 \mid 48$. Zatem na mocy twierdzenia 8.41 zbiór wszystkich wspólnych dzielników liczb 168 i 396 jest równy $D_{12} = \{1, 2, 3, 4, 5, 12\}$.

Zadanie 22.25. Niech n będzie liczbą naturalną, która ma dokładnie 3 dzielniki. Ponieważ 1 ma dokładnie jeden dzielnik i liczby pierwsze mają dokładnie dwa dzielniki, więc n jest liczbą złożoną. Ist-

nieją zatem liczby naturalne $a, b > 1$ takie, że $n = ab$. Stąd $1, a, n$ są różnymi dzielnikami n i także $1, b, n$ są różnymi dzielnikami n, ale $1 < a < n$ i $1 < b < n$, więc $a = b$ i $n = a^2$. Jeżeli a nie jest liczbą pierwszą, to posiada dzielnik d taki, że $1 < d < a$ i wtedy $1, d, a, n$ są różnymi dzielnikami liczby n, co prowadzi do sprzeczności. Wobec tego a jest liczbą pierwszą.

Na odwrót. Niech $n = p^2$ dla pewnej liczby pierwszej p. Wtedy $D_p = \{1, p, p^2\}$, więc liczba n posiada dokładnie 3 dzielniki.

Ostatecznie mamy zatem, że liczbami naturalnymi, które posiadają dokładnie 3 dzielniki są kwadraty liczb pierwszych.

Zadanie 22.26. a). Z cechy podzielności przez 3 wynika, że $3 \mid (31x2)_{10} \iff 3 \mid 3 + 1 + x + 2 \iff 3 \mid x$, ale x jest cyfrą, więc $x \in \{0, 3, 6, 9\}$.

b). Z cechy podzielności przez 9 wynika, że $9 \mid (31x2)_{10}$ wtedy i tylko wtedy, gdy $9 \mid 3 + 1 + x + 2 \iff 9 \mid x + 6$, ale x jest cyfrą i na mocy a), $x \in \{0, 3, 6, 9\}$, więc $x = 3$.

c). Z cechy podzielności przez 4 wynika, że $4 \mid (31x2)_{10} \iff 4 \mid x2$, a to jest równoważne temu, że $4 \mid 10x+2 \iff 2 \mid 5x+1 \iff 2 \mid x+1$, ale x jest cyfrą, więc $x \in \{1, 3, 5, 7, 9\}$.

Zadanie 22.27. Niech n będzie liczbą naturalną posiadającą dokładnie p dzielników. Wtedy $n > 1$, więc istnieją różne liczby pierwsze $p_1, \ldots, p_s$ oraz liczby naturalne $a_1, \ldots, a_s$ takie, że $n = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$. Ze stwierdzenia 9.23 liczba wszystkich dzielników liczby n wynosi $\tau(n) = (a_1 + 1) \cdot \ldots \cdot (a_s + 1)$, więc $(a_1 + 1) \cdot \ldots \cdot (a_s + 1) = p$, ale $a_i + 1 \geqslant 2$, gdyż $a_i \geqslant 1$ dla każdego $i = 1, \ldots, s$, więc z pierwszości p, $s = 1$ i $a_1 = p_1$. Wobec tego $n = p_1^{p-1}$, czyli liczba naturalna ma dokładnie p dzielników (gdzie p jest liczbą pierwszą) wtedy i tylko wtedy, gdy jest $p - 1$-szą potęgą pewnej liczby pierwszej.

Zadanie 22.28. Niech p będzie liczbą pierwszą i niech $r = [p]_{30}$. Wtedy $r \in \{0, 1, \ldots, 29\}$ oraz $p = 30k + r$ dla pewnego $k \in \mathbb{N}_0$, ale $30 = 2 \cdot 3 \cdot 5$, więc $r > 0$. Jeżeli r jest parzyste i $r > 2$, to $p > 2$ i p jest parzyste, ale jedyną parzystą liczbą pierwszą jest 2, więc mamy sprzeczność. Stąd $2 \nmid r$. Jeżeli $3 \mid r$ i $r > 3$, to $p > 3$ i $3 \mid p$, skąd $p = 3$ i mamy sprzeczność. Zatem $3 \nmid r$. Jeżeli $5 \mid r$ i $r > 5$, to

$p > 5$ i $5 \mid p$, skąd $p = 5$ i mamy sprzeczność. Zatem $5 \nmid r$. Stąd $r \in \in \{1, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$, czyli $r = 1$ lub r jest liczbą pierwszą.

Zadanie 22.29. Ponieważ $14^2 = 196 \leqslant 200 < 225 = 15^2$, więc $s = 14$. Wypisujemy wszystkie liczby naturalne od 2 do 200:
2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~, 31, ~~32~~, ~~33~~, ~~34~~, ~~35~~, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~, 41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, ~~49~~, ~~50~~, ~~51~~, ~~52~~, 53, ~~54~~, ~~55~~, ~~56~~, ~~57~~, ~~58~~, 59, ~~60~~, 61, ~~62~~, ~~63~~, ~~64~~, ~~65~~, ~~66~~, 67, ~~68~~, ~~69~~, ~~70~~, 71, ~~72~~, 73, ~~74~~, ~~75~~, ~~76~~, ~~77~~, ~~78~~, 79, ~~80~~, ~~81~~, ~~82~~, 83, ~~84~~, ~~85~~, ~~86~~, ~~87~~, ~~88~~, 89, ~~90~~, ~~91~~, ~~92~~, ~~93~~, ~~94~~, ~~95~~, ~~96~~, 97, ~~98~~, ~~99~~, ~~100~~, 101, ~~102~~, 103, ~~104~~, ~~105~~, ~~106~~, 107, ~~108~~, 109, ~~110~~, ~~111~~, ~~112~~, 113, ~~114~~, ~~115~~, ~~116~~, ~~117~~, ~~118~~, ~~119~~, ~~120~~, ~~121~~, ~~122~~, ~~123~~, ~~124~~, ~~125~~, ~~126~~, 127, ~~128~~, ~~129~~, ~~130~~, 131, ~~132~~, ~~133~~, ~~134~~, ~~135~~, ~~136~~, 137, ~~138~~, 139, ~~140~~, ~~141~~, ~~142~~, ~~143~~, ~~144~~, ~~145~~, ~~146~~, ~~147~~, ~~148~~, 149, ~~150~~, 151, ~~152~~, ~~153~~, ~~154~~, ~~155~~, ~~156~~, 157, ~~158~~, ~~159~~, ~~160~~, ~~161~~, ~~162~~, 163, ~~164~~, ~~165~~, ~~166~~, 167, ~~168~~, ~~169~~, ~~170~~, ~~171~~, ~~172~~, 173, ~~174~~, ~~175~~, ~~176~~, ~~177~~, ~~178~~, 179, ~~180~~, 181, ~~182~~, ~~183~~, ~~184~~, ~~185~~, ~~186~~, ~~187~~, ~~188~~, ~~189~~, ~~190~~, 191, ~~192~~, 193, ~~194~~, ~~195~~, ~~196~~, 197, ~~198~~, 199, ~~200~~.

Liczby pierwsze nie większe od 200:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

Zadanie 22.30. Załóżmy, że n jest liczbą naturalną większą od 1 i $n \mid (n-1)! + 1$ oraz n nie jest liczbą pierwszą. Wtedy n jest liczbą złożoną, więc istnieją liczby naturalne $a, b > 1$ takie, że $n = ab$. Stąd $a \leqslant n - 1$ oraz $a \mid (n-1)!$, bo $(n-1)! = 1 \cdot \ldots \cdot a \cdot \ldots \cdot (n-1)$ i $1 < a \leqslant n-1$, ale $a \mid n$ i $n \mid (n-1)!+1$, więc z przechodniości relacji podzielności, $a \mid (n-1)!+1$. Ponadto $a \mid (n-1)!$, więc $a \mid 1$, skąd $a = 1$ i mamy sprzeczność. Wobec tego n jest liczbą pierwszą.

Zadanie 22.31. Badamy pierwszość liczby 437. Ponieważ $20^2 = = 400 \leqslant 437 < 441 = 21^2$, więc wypisujemy wszystkie liczby pierwsze $\leqslant 20$: 2, 3, 5, 7, 11, 13, 17, 19 i badamy podzielność liczby 437 przez każdą z nich. Oczywiście, $2 \nmid 437$, bo cyfra 7 jest nieparzysta; $3 \nmid 437$, bo suma cyfr liczby 437 wynosi $4 + 3 + 7 = 14$ i nie dzieli się przez 3; $5 \nmid 437$, bo $7 \neq 0$ i $7 \neq 5$; $[437]_7 = 3 \neq 0$, więc $7 \nmid 437$; naprzemienna suma cyfr liczby 437 wynosi $7 - 3 + 4 = 8$ i nie dzieli się przez 11, więc

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$11 \nmid 437$; $[437]_{13} = 8 \neq 0$, więc $13 \nmid 437$; $[437]_{17} = 12 \neq 0$, więc $17 \nmid 437$; w końcu $437 = 19 \cdot 23$, więc 437 nie jest liczbą pierwszą.

Badamy pierwszość liczby 1997. Ponieważ $44^2 = 1936 \leqslant 1997 < 2025 = 45^2$, więc należy wypisać wszystkie liczby pierwsze $\leqslant 44$: 2,3,5,7,11,13,17,19,23,29,31,37,41,43 i badać, czy któraś z nich dzieli liczbę 1997. Podobnie jak dla liczby 437 pokazujemy, że $2 \nmid 1997$, $3 \nmid 1997$, $5 \nmid 1997$ oraz $11 \nmid 1997$. Ponadto: $[1997]_7 = 2 \neq 0$, $[1997]_{13} = 8 \neq 0$, $[1997]_{17} = 8 \neq 0$, $[1997]_{19} = 2 \neq 0$, $[1997]_{23} = 19 \neq 0$, $[1997]_{29} = 25 \neq 0$, $[1997]_{31} = 13 \neq 0$, $[1997]_{37} = 26 \neq 0$, $[1997]_{41} = 29 \neq 0$, $[1997]_{43} = 19 \neq 0$, więc z twierdzenia 9.10 liczba 1997 jest liczbą pierwszą.

Zadanie 22.32. Mamy: $112 = 2 \cdot 56 = 2 \cdot 2^3 \cdot 7 = 2^4 \cdot 7^1$, czyli postacią kanoniczną liczby 112 jest $2^4 \cdot 7^1$.

Postacią kanoniczną liczby 143 jest $11^1 \cdot 13^1$.

Mamy: $201 = 3 \cdot 67$, więc postacią kanoniczną liczby 201 jest $3^1 \cdot 67^1$.

Mamy: $2001 = 3 \cdot 667 = 3 \cdot 23 \cdot 29$, więc rozkładem kanonicznym liczby 2001 jest $3^1 \cdot 23^1 \cdot 29^1$.

Zadanie 22.33. Jeśli $a = b = 1$, to $a^3 + b^3 = 2$ jest liczbą pierwszą. Załóżmy, że $a > 1$ lub $b > 1$. Wtedy $a + b < a^3 + b^3$ i $a + b > 1$ oraz $a + b \mid a^3 + b^3$, bo $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$ i $a^2 - ab + b^2 \in \mathbb{Z}$. Zatem $1, a + b, a^3 + b^3$ są trzema różnymi dzielnikami liczby $a^3 + b^3$, więc jest ona liczbą złożoną.

Wobec tego dla $a, b \in \mathbb{N}$ liczba $a^3 + b^3$ jest liczbą pierwszą wtedy i tylko wtedy, gdy $a = b = 1$.

Zadanie 22.34. Ponieważ $25 = 5^2$, więc z twierdzenia o jednoznaczności rozkładu $p = 5$ i $q = 2$. Stąd $2^1 \cdot 5^n = 5^2 \cdot 2^m$, więc znowu z twierdzenia o jednoznaczności rozkładu, $n = 2$ i $m = 1$.

Zadanie 22.35. Załóżmy, że liczby $a + b$ i ab nie są względnie pierwsze. Wtedy ze stwierdzenia 9.20 istnieje liczba pierwsza p taka, że $p \mid a+b$ i $p \mid ab$. Z twierdzenia 9.14 mamy, że $p \mid a$ lub $p \mid b$. Jeśli $p \mid a$, to ponieważ $p \mid a+b$, więc też $p \mid b$, skąd $\mathrm{NWD}(a, b) \geqslant p > 1$, co prowadzi do sprzeczności. Podobnie, gdy $p \mid b$, to ponieważ $p \mid a + b$, więc $p \mid a$, skąd $\mathrm{NWD}(a, b) \geqslant p > 1$ i też mamy sprzeczność. Przypuszczenie, że

liczby $a+b$ i ab nie są względnie pierwsze doprowadziło nas zatem do sprzeczności. Wobec tego te liczby są względnie pierwsze.

Zadanie 22.36. Ogólna postać dwóch kolejnych liczb całkowitych to: $n, n+1$, gdzie $n \in \mathbb{Z}$. Jeśli $d \in \mathbb{N}$ jest wspólnym dzielnikiem tych liczb, to d dzieli też ich różnicę, czyli $d \mid 1$, skąd $d = 1$. Wobec tego $\mathrm{NWD}(n, n+1) = 1$, czyli liczby n i $n+1$ są względnie pierwsze.

Zadanie 22.37. Jeśli $a > 1$, to z twierdzenia 9.8 istnieje liczba pierwsza p taka, że $p|a$. Z przechodniości relacji podzielności mamy zatem, że $p|b^n$. Stąd na mocy twierdzenia 9.14, $p|b$. Zatem $\mathrm{NWD}(a,b) \geqslant \geqslant p > 1$ i mamy sprzeczność. Wobec tego $a = 1$.

Zadanie 22.38. Ponieważ $168 = 2^3 \cdot 3 \cdot 7$ i $396 = 2^2 \cdot 3^2 \cdot 11$, więc z twierdzenia 9.30, $\mathrm{NWD}(168, 396) = 2^2 \cdot 3 = 12$ i $\mathrm{NWW}(168, 396) = = 2^3 \cdot 3^2 \cdot 7 \cdot 11 = 5544$.

Dalej, $1115 = 5 \cdot 223$ i 223 jest liczbą pierwszą, bo $14^2 = 196 \leqslant \leqslant 223 < 225 = 15^2$ i żadna z liczb $2, 3, 5, 7, 11, 13$ nie dzieli liczby 223. Ponadto $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$, więc z twierdzenia 9.30, $\mathrm{NWD}(1115, 630) = 5$ i $\mathrm{NWW}(1115, 630) = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 223 = 140490$.

$2516 = 2^2 \cdot 17 \cdot 37$ i $3655 = 5 \cdot 17 \cdot 43$, więc z twierdzenia 9.30, $\mathrm{NWD}(2516, 3655) = 17$ i $\mathrm{NWW}(2516, 3655) = 2^2 \cdot 17 \cdot 37 \cdot 5 \cdot 43 = 540940$.

Zadanie 22.39. Z twierdzenia 9.32 mamy, że $\mathrm{NWD}(a,b,c) = r$ oraz $\mathrm{NWW}(a,b,c) = p^2q^3r^3$. Ponadto $ab = p^2q^4r^5$, więc z twierdzenia 9.32, $\mathrm{NWD}(ab, c) = p^2qr^3$.

Zadanie 22.40. Ponieważ $98 = 2 \cdot 7^2$, więc liczba całkowita a jest względnie pierwsza z liczbą 98 wtedy i tylko wtedy, gdy $2 \nmid a$ i $7 \nmid a$. Stąd mamy, że $n \in \{1, 3, 5, 9, 11, 13, 15, 17, 19\}$.

Zadanie 22.41. Ponieważ $330 = 2 \cdot 3 \cdot 5 \cdot 11$, więc na mocy stwierdzenia 9.21 mamy dokładnie $2^4 = 16$ takich rozkładów: $330 = 1 \cdot 330 = = 330 \cdot 1, 330 = 2 \cdot 165 = 165 \cdot 2, 330 = 3 \cdot 110 = 110 \cdot 3, 330 = 5 \cdot 66 = 66 \cdot 5$, $330 = 11 \cdot 30 = 30 \cdot 11$, $330 = 6 \cdot 55 = 55 \cdot 6$, $10 \cdot 33 = 33 \cdot 10$, $330 = 22 \cdot 15 = 15 \cdot 22$.

Zadanie 22.42. Szukamy wszystkich par (x, y) liczb naturalnych

takich, że $x+y=22$ i $\mathrm{NWD}(x,y)=1$, ale $y=22-x$, więc z algorytmu Euklidesa:
$\mathrm{NWD}(x,22-x)=\mathrm{NWD}(x,22-x+x)=\mathrm{NWD}(x,22)$. Zatem $\mathrm{NWD}(x,y)=1 \iff \mathrm{NWD}(x,22)=1$, ale $22=2\cdot 11$, więc na mocy stwierdzenia 9.21, $\mathrm{NWD}(x,22)=1$ wtedy i tylko wtedy, gdy $2\nmid x$ i $11\nmid x$. Stąd $x\in\{1,3,5,7,9,13,15,17,19\}$ i wobec tego $(x,y)\in\{(1,19),(3,17),(5,15),(7,13),(9,11),(15,5),(17,3),(19,1)\}$.

Zadanie 22.43. Mamy $15=3\cdot 5$, $21=3\cdot 7$ i $35=5\cdot 7$, więc z twierdzenia 9.32 mamy, że $\mathrm{NWD}(15,21,35)=1$, a zatem liczby 15, 21, 35 są względnie pierwsze.

Zadanie 22.44. Ponieważ $48=2^4\cdot 3$, więc na mocy wniosku 8.51 wystarczy pokazać, że $3\mid n^3+3n^2-n-3$ i $16\mid n^3+3n^2-n-3$, ale $n^3+3n^2-n-3=(n^3-n)+3(n^2-1)$ i z zadania 22.11, $3\mid n^3-n$, więc $3\mid n^3+3n^2-n-3$. Ponadto $n^3+3n^2-n-3=n^2(n+3)-(n+3)=$ $=(n+3)(n^2-1)$ i z zadania 22.13, $n^2-1=8t$ dla pewnego $t\in\mathbb{Z}$ oraz $n=2k+1$ dla pewnego $k\in\mathbb{Z}$, gdyż n jest nieparzyste, więc $n+3=2(k+2)$ i $n^3+3n^2-n-3=16[(k+2)t]$ i oczywiście $(k+2)t\in\mathbb{Z}$, więc $16\mid n^3+3n^2-n-3$, co kończy dowód.

Zadanie 22.45. Ponieważ p jest liczbą pierwszą większą od 5, więc p jest liczbą nieparzystą, $3\nmid p$ i $5\nmid p$. Z małego twierdzenia Fermata mamy, że $5\mid p^5-p$ i $p^5-p=p(p^4-1)$, skąd $5\mid p^4-1$. Z zadania 22.8, $3\mid p^2-1$ i $p^4-1=(p^2-1)(p^2+1)$, więc $3\mid p^4-1$. Dalej, $p^4-1=$ $=(p-1)(p+1)(p^2+1)$, przy czym $(p-1)(p+1)$ jest iloczynem dwóch kolejnych liczb parzystych, więc z zadania 22.12, $8\mid(p-1)(p+1)$ i liczba p^2+1 jest parzysta, a zatem $16\mid p^4-1$. Z wniosku 8.51 wynika, że $16\cdot 3\cdot 5\mid p^4-1$, ale $16\cdot 3\cdot 5=240$, więc $240\mid p^4-1$.

Zadanie 22.46. Mamy, że $\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}=\frac{3n^5+5n^3+7n}{15}\in\mathbb{Z}$ wtedy i tylko wtedy, gdy $15\mid 3n^5+5n^3+7n$. Ponadto $15=3\cdot 5$, więc z wniosku 8.51, $15\mid 3n^5+5n^3+7n \iff [3\mid 3n^5+5n^3+7n$ i $5\mid 3n^5+5n^3+7n]$. Dalej, $3n^5+5n^3+7n-2(n^3-n)=3(n^5+n^3+3n)$ i $n^5+n^3+3n\in\mathbb{Z}$, więc stąd i z zadania 22.11, $3\mid 3n^5+5n^3+7n$. Dodatkowo, $3n^5+5n^3+7n-3(n^5-+n)=5(n^3+2n)$ i $n^3+2n\in\mathbb{Z}$, więc stąd i z małego twierdze-

nia Fermata dla $p = 5$ mamy, że $5 \mid 3n^5 + 5n^3 + 7n$]. Kończy to nasz dowód.

Zadanie 22.47. Na mocy twierdzenia 8.36 szukane liczby są postaci $\mathrm{NWW}(18, 24, 45) \cdot k$, gdzie $k \in \mathbb{N}$, ale $18 = 2 \cdot 3^2$, $24 = 2^3 \cdot 3$ i $45 = 3^2 \cdot 5$, więc z twierdzenia 9.32, $\mathrm{NWW}(18, 24, 45) = 2^3 \cdot 3^2 \cdot 5 = 360$. W takim razie ogólną postacią omawianych liczb jest $360k$ dla $k \in \mathbb{N}$.

Zadanie 22.48. Oznaczmy przez x cyfrę setek naszej liczby, a przez y jej cyfrę jedności. Ponieważ $72 = 2^3 \cdot 3^2$, więc z wniosku 8.51 liczba $a = (42x4y)_{10}$ jest podzielna przez 72 wtedy i tylko wtedy, gdy jest ona podzielna przez 8 i jest podzielna przez 9. Dalej, $a = 42 \cdot 1000 + (x4y)_{10}$ i $1000 = 125 \cdot 8$, więc $8 \mid a \iff 8 \mid 100x + 40 + y \iff 8 \mid 4x + y$. Stąd w szczególności $4 \mid y$, czyli $y = 4t$, gdzie $t \in \{0, 1, 2\}$ oraz $8 \mid 4x + y$ wtedy i tylko wtedy, gdy $8 \mid 4x + 4t \iff 2 \mid x + t$. Zatem $8 \mid a$ wtedy i tylko wtedy, gdy $y = 4t$, gdzie $t \in \{0, 1, 2\}$ i $2 \mid x + t$ oraz $x \in \{0, 1, \ldots, 9\}$.

Ponadto, z cechy podzielności przez 9 mamy, że $9 \mid a$ wtedy i tylko wtedy, gdy $9 \mid 4 + 2 + x + 4 + y \iff 9 \mid x + y + 1$, ale $1 \leqslant x + y + 1 \leqslant 9 + 9 + 1 = 19$, więc $x + y + 1 = 9$ lub $x + y + 1 = 18$. Zatem $9 \mid a$ wtedy i tylko wtedy, gdy $x + y + 1 = 9$ lub $x + y + 1 = 18$ oraz $x, y \in \{0, 1, \ldots, 9\}$.

Rozważmy najpierw przypadek, gdy $x + y + 1 = 9$. Stąd $x + 4t = 8$, więc x jest parzyste, skąd t też jest parzyste, bo $2 \mid x + t$. Jeśli $t = 0$, to $y = 0$ i $x = 8$. Jeśli $t = 2$, to $y = 8$ i $x = 0$.

Niech teraz $x + y + 1 = 18$. Wtedy $x + 4t = 17$ i $t \in \{0, 1, 2\}$, skąd $x \in \{17, 13, 9\}$, czyli $x = 9$ i $t = 2$, co przeczy temu, że $2 \mid x + t$.

Ostatecznie mamy zatem, że $(x, y) \in \{(8, 0), (0, 8)\}$, czyli są tylko dwie takie liczby: 42048 i 42840.

Zadanie 22.49. Niech $x, y \in \mathbb{Z}$ będą takie, że $3 \mid x^2 + y^2$. Jeśli $3 \mid x$, to stąd $3 \mid y^2$, skąd z twierdzenia 9.14, $3 \mid y$. Podobnie pokazujemy, że jeśli $3 \mid y$, to $3 \mid x$. Załóżmy teraz, że $3 \nmid x$. Wtedy także $3 \nmid y$. Zatem z zadania 22.8 istnieją $k, l \in \mathbb{N}_0$ takie, że $x^2 = 3k + 1$ i $y^2 = 3l + 1$. Stąd $x^2 + y^2 = 3(k + l) + 2$, co przeczy temu, że $3 \mid x^2 + y^2$. Wobec tego $3 \mid x$ i $3 \mid y$, co należało wykazać.

Zadanie 22.50. a). Szukane liczby są postaci $7t$ dla $t \in \mathbb{Z}$ takich, że $100 \leqslant 7t \leqslant 1000$, skąd $14\frac{2}{7} \leqslant t \leqslant 142\frac{6}{7}$, czyli $t = 15, 16, \ldots, 142$, a więc tych liczb jest dokładnie $142 - 14 = 128$.

b). Niech $A = \{n \in \mathbb{N} : n \in [100, 1000] \text{ i } 8 \mid n\}$ i niech $B = \{n \in \mathbb{N} : n \in [100, 1000] \text{ i } 5 \mid n\}$. Wtedy $A = \{8t : t \in \mathbb{Z} \text{ i } 100 \leqslant 8t \leqslant 1000\}$ i $B = \{5s : s \in \mathbb{Z} \text{ i } 100 \leqslant 5s \leqslant 1000\}$. Stąd $t = 13, 14, \ldots, 125$ oraz $s = 20, 21, \ldots, 200$, a zatem $|A| = 125 - 12 = 113$ i $|B| = 200 - 19 = 181$. Z wniosku 8.51 mamy, że $A \cap B = \{n \in [100, 1000] : n \in \mathbb{N} \text{ i } 40 \mid n\} = \{40t : t = 3, 4, \ldots, 25\}$, skąd $|A \cap B| = 25 - 2 = 23$. Dalej, $|A \cup B| = |A| + |B| - |A \cap B|$, więc $|A \cup B| = 113 + 181 - 23 = 271$. Zatem jest dokładnie 271 liczb naturalnych $n \in [100, 1000]$ takich, że $8 \mid n$ lub $5 \mid n$.

c). Niech $A = \{n \in \mathbb{N} : n \in [100, 1000] \text{ i } 3 \mid n\}$ i niech $B = \{n \in \mathbb{N} : n \in [100, 1000] \text{ i } 4 \mid n\}$. Wtedy $A = \{3t : t \in \mathbb{Z} \text{ i } 100 \leqslant 3t \leqslant 1000\}$ i $B = \{4s : s \in \mathbb{Z} \text{ i } 100 \leqslant 4s \leqslant 1000\}$. Stąd $t = 34, 14, \ldots, 333$ oraz $s = 25, 21, \ldots, 250$, a zatem $|A| = 333 - 33 = 300$ i $|B| = 250 - 24 = 226$. Z wniosku 8.51 mamy, że $A \cap B = \{n \in [100, 1000] : n \in \mathbb{N} \text{ i } 12 \mid n\} = \{12t : t = 9, 4, \ldots, 83\}$, skąd $|A \cap B| = 83 - 8 = 75$. Zatem $|A \setminus B| = |A| - |A \cap B| = 300 - 75 = 225$. Wobec tego jest dokładnie 225 liczb naturalnych $n \in [100, 1000]$ takich, że $3 \mid n$ i $4 \nmid n$.

Zadanie 22.51. Jeżeli $n \geqslant 4$, to prawa strona danego równania jest dodatnia, a lewa nie. Żadna więc liczba całkowita $n \geqslant 4$ nie spełnia tego równania. Podobnie wnioskujemy, że żadna liczba całkowita $n \leqslant -2$ również nie jest rozwiązaniem tego równania. Przez bezpośrednie sprawdzenie stwierdzamy, że spośród liczb: -1, 0, 1, 2, 3 dane równanie spełniają jedynie liczby: 0, 1 i 2.

Zadanie 22.52. Załóżmy, że $49 \mid n^2 - n + 9$ dla pewnego $n \in \mathbb{N}$. Wtedy $n^2 - n + 9 = 49k$ dla pewnego $k \in \mathbb{Z}$. Stąd $4(n^2 - n + 9) = 4 \cdot 49k$, czyli $(2k-1)^2 + 35 = 4 \cdot 49k$, ale $7 \mid 35$, więc $7 \mid (2k-1)^2$, skąd $7 \mid 2k-1$. Wobec tego $49 \mid (2k-1)^2$, ale $(2k-1)^2 + 35 = 4 \cdot 49k$, więc $49 \mid 35$, co jest niemożliwe.

Przypuszczenie, że istnieje liczba naturalna n taka, że $49 \mid n^2 - n + 9$

doprowadziło nas zatem do sprzeczności. Wobec tego taka liczba n nie istnieje.

Zadanie 22.53. Zauważmy, że $n(n+1)(n+2)(n+3)+1 = [n(n+3)]\cdot[(n+1)(n+2)]+1 = (n^2+3n)[(n^2+3n)+2]+1 = (n^2+3n)^2+2(n^2+3n)+1 = [(n^2+3n)+1]^2$. Stąd otrzymujemy, że $n(n+1)(n+2)(n+3)+1 = (n^2+3n+1)^2$, a ponieważ $n^2+3n+1 \in \mathbb{N}$, więc nasza teza jest udowodniona.

Zadanie 22.54. Niech x i y będą odpowiednio cyfrą dziesiątek i cyfrą jedności liczby dwucyfrowej A. Wtedy $x \in \{1,2,\ldots,9\}$ oraz $y \in \{0,1,\ldots,9\}$ i $a = 10x+y$. Ponadto z warunków zadania $a = x+y^2$. Zatem $10x+y = x+y^2$, czyli $9x = y^2-y$, a zatem $9x = y(y-1)$, ale $x \neq 0$, więc $y \geqslant 2$. Stąd $3 \mid y$ lub $3 \mid y-1$ i liczby y, $y-1$ są względnie pierwsze, więc $9 \mid y$ lub $9 \mid y-1$, skąd $y = 9$, bo $y \in \{2,3,\ldots,9\}$. Wobec tego $9x = 9\cdot 8$ i $x = 8$. Zatem szukaną liczbą jest 89.

Zadanie 22.55. Niech a,b,c będą różnymi liczbami naturalnymi takimi, że $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} = 1$. Bez zmniejszania ogólności możemy zakładać, że $a < b < c$. Wtedy $\frac{1}{a} > \frac{1}{b} > \frac{1}{c}$, skąd $1 < 3\cdot\frac{1}{a}$, a zatem $a < 3$, ale $a \neq 1$, bo inaczej $\frac{1}{b}+\frac{1}{c} = 0$, więc $a = 2$. Wobec tego $\frac{1}{b}+\frac{1}{c} = \frac{1}{2}$ i $\frac{1}{2} < 2\cdot\frac{1}{b}$, więc $b < 4$, ale $b > a = 2$, więc $b = 3$ i $\frac{1}{c} = \frac{1}{2}-\frac{1}{3} = \frac{3}{6}-\frac{2}{6} = \frac{1}{6}$, skąd $c = 6$.

Zadanie 22.56. Z twierdzenia o dzieleniu z resztą wynika, że $p = 3k$ lub $p = 3k+1$ lub $p = 3k+2$ dla pewnego $k \in \mathbb{N}_0$. Ponieważ $p \in \mathbb{P}$ i $p > 3$, więc pierwsza możliwość odpada. Jeżeli $p = 3k+2$, to $10p+1 = 30k+21 = 3(10k+7)$ i $10k+7 \geqslant 7$, więc otrzymujemy sprzeczność z pierwszością liczby $10p+1$. Wobec tego $p = 3k+1$ i $5p+1 = 15k+6 \geqslant 6$ oraz $3 \mid 5p+1$, czyli liczba $5p+1$ nie jest pierwsza.

Zadanie 22.57. Wśród czterech kolejnych liczb całkowitych k, $k+1, k+2, k+3$ istnieją dwie kolejne liczby parzyste, których iloczyn zgodnie z zadaniem 22.12 jest podzielny przez 8. Wobec tego $8 \mid k(k+1)(k+2)(k+3)$. Ponadto $k, k+1, k+2$ są trzema kolejnymi liczbami całkowitymi, więc dokładnie jedna z nich jest podzielna przez 3, a stąd $3 \mid k(k+1)(k+2)(k+3)$. Ponadto, liczby 8 i 3 są względnie

pierwsze i $24 = 3 \cdot 8$, więc $24 \mid k(k+1)(k+2)(k+3)$, co było do wykazania.

Zadanie 22.58. Jeżeli $[n+a]_3 = [n]_3$, to $3 \mid (n+a)-n$, czyli $3 \mid a$, wbrew założeniu o a. Zatem $[n+a]_3 \neq [n]_3$. Jeżeli $[n+b]_3 = [n]_3$, to $3 \mid (n+b)-n$, czyli $3 \mid b$, wbrew założeniu o b. Zatem $[n+b]_3 \neq [n]_3$. Jeżeli $[n+a]_3 = [n+b]_3$, to $3 \mid (n+a)-(n+b)$, czyli $3 \mid a-b$, skąd $[a]_3 = [b]_3$, wbrew założeniu o a i b. Zatem $[n+a]_3 \neq [n+b]_3$.

W ten sposób wykazaliśmy, że liczby: $n, n+a, n+b$ dają parami różne reszty z dzielenia przez 3, ale są dokładnie 3 reszty z dzielenia przez 3 (mianowicie $0, 1$ i 2), więc dokładnie jedna z tych liczb daje resztę 0 z dzielenia przez 3, czyli dokładnie jedna z nich jest podzielna przez 3.

Zadanie 22.59. Ogólna postać dwóch kolejnych liczb całkowitych nieparzystych: $2k+1, 2k+3$, gdzie $k \in \mathbb{Z}$. Weźmy dowolny naturalny wspólny dzielnik d tych liczb. Wtedy dzieli on ich różnicę równą 2, skąd $d = 1$ lub $d = 2$, ale $d \mid 2k+1$, więc $d \neq 2$. Stąd $d = 1$ i wobec tego $\mathrm{NWD}(2k+1, 2k+3) = 1$.

Zadanie 22.60. Z założenia wynika, że $\mathrm{NWD}(a, b) = 1$. Niech liczba naturalna d będzie wspólnym dzielnikiem liczb $a+b$ i b. Wtedy d dzieli ich różnicę, czyli $d \mid a$. Zatem d jest wspólnym dzielnikiem liczb względnie pierwszych a i b, skąd $d = 1$ i wobec tego $\mathrm{NWD}(a+b, b) = 1$.

Podobnie, niech liczba naturalna d będzie wspólnym dzielnikiem liczb $b-a$ i b. Wtedy $d \mid b-(b-a)$, czyli $d \mid a$. Zatem $d \mid a$ i $d \mid b$, skąd $d = 1$, bo $\mathrm{NWD}(a, b) = 1$. Wobec tego $\mathrm{NWD}(b-a, b) = 1$.

Zadanie 22.61. Bez zmniejszania ogólności rozważań możemy zakładać, że $x \leqslant y \leqslant z$. Wtedy $3 \cdot \frac{1}{x} \geqslant \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, skąd $\frac{3}{x} \geqslant \frac{13}{12}$, więc $13x \leqslant 36$ i $x \leqslant 2$, czyli $x \in \{1, 2\}$.

Niech $x = 1$. Wtedy $\frac{1}{y} + \frac{1}{z} = \frac{1}{12}$, skąd $y, z > 12$ oraz $yz = 12(y+z)$, czyli $(y-12)(z-12) = 144$. Teraz uwzględniając fakt, że

$$D_{144} = \{1, 144; 2, 72; 3, 48; 4, 36; 6, 24; 8, 18; 9, 16; 12\}$$

oraz to, że $0 < y-12 \leqslant z-12$ uzyskujemy następujące możliwości: $y-12 = 1$ i $z-12 = 144$ lub $y-12 = 2$ i $z-12 = 72$ lub $y-12 = 3$

i $z-12=48$ lub $y-12=4$ i $z-12=36$ lub $y-12=6$ i $z-12=24$ lub $y-12=8$ i $z-12=18$ lub $y-12=9$ i $z-12=16$ lub $y-12=z-12=12$, skąd $y=13$ i $z=156$ lub $y=14$ i $z=84$ lub $y=15$ i $z=60$ lub $y=16$ i $z=48$ lub $y=18$ i $z=36$ lub $y=20$ i $z=30$ lub $y=21$ i $z=28$ lub $y=z=24$.

Niech $x=2$. Wtedy $\frac{1}{y}+\frac{1}{z}=\frac{13}{12}-\frac{6}{12}=\frac{7}{12}$, ale $2\cdot\frac{1}{y}\geqslant\frac{1}{y}+\frac{1}{z}$, więc $\frac{2}{y}\geqslant\frac{7}{12}$, skąd $7y\leqslant 24$, czyli $y\leqslant 3$. Ponadto $y\geqslant 2$, bo $y\geqslant x$, więc $y=2$ lub $y=3$. Jeśli $y=2$, to $\frac{1}{z}=\frac{7}{12}-\frac{6}{12}=\frac{1}{12}$, czyli $z=12$. Jeśli $y=3$, to $\frac{1}{z}=\frac{7}{12}-\frac{4}{12}=\frac{3}{12}=\frac{1}{4}$, skąd $z=4$.

Zadanie 22.62. Z zadania 22.57 wynika, że licznik tego ułamka jest podzielny przez 24. Ponadto iloczyn trzech kolejnych liczb naturalnych parzystych jest postaci $2k\cdot(2k+2)\cdot(2k+4)=4k(k+1)(k+2)$ i jak wiemy $2\mid k(k+1)$ oraz $3\mid k(k+1)(k+2)$, więc mianownik naszego ułamka też jest podzielny przez 24. Zatem ten ułamek można skrócić przez 24.

Zadanie 22.63. Liczba $(n-1)n(n+1)$ jest iloczynem trzech kolejnych liczb całkowitych, więc dzieli się przez 3, gdyż dokładnie jedna z liczb $n-1, n, n+1$ jest podzielna przez 3 oraz jedna z liczb n, $n+1$ dzieli się przez 2. Zatem $6\mid n^3-n$. Ponadto $(n^3+5n)-(n^3-n)=6n$, $(n^3+11n)-(n^3-n)=12n$ i $n^3-19n=(n^3-n)-18n$, więc wypisane dwie różnice i suma też są podzielne przez 6. Wobec tego liczby n^3+5n, n^3+11n i n^3-19n są podzielne przez 6.

Zadanie 22.64. Liczba $(n-1)n(n+1)$ jest iloczynem trzech kolejnych liczb całkowitych, więc dzieli się przez 3, gdyż dokładnie jedna z liczb $n-1, n, n+1$ jest podzielna przez 3. Ponadto jedna z liczb n, $n+1$ jest parzysta, więc liczba $(n-1)n(n+1)$ jest podzielna przez 2. Zatem $6\mid(n-1)n(n+1)$. Ponadto $n(n+1)(2n+1)+n(n+1)(n-1)=$ $=n(n+1)[2n+1+(n-1)]=3n^2(n+1)$, więc ta suma dzieli się przez 6. Zatem $6\mid n(n+1)(2n+1)$.

Zadanie 22.65. Jeżeli liczby a i b dają tę samą resztę z dzielenia przez 3, to $3\mid a-b$. Niech dalej a i b dają różne reszty z dzielenia przez 3. Jeżeli $[a]_3=0$ lub $[b]_3=0$, to $3\mid a$ lub $3\mid b$. Niech zatem $[a]_3\neq[b]_3$ i niech $[a]_3\neq 0$ i $[b]_3\neq 0$. Wtedy $[a]_3=1$ i $[b]_3=2$ lub $[a]_3=2$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

i $[b]_3 = 1$. W pierwszym przypadku $a = 3k+1$ i $b = 3l+2$ dla pewnych $k, l \in \mathbb{Z}$, skąd $a + b = 3(k + l + 1)$ i $3 \mid a + b$. Podobnie w przypadku drugim $3 \mid a + b$.

Zadanie 22.66. Niech $a \in \mathbb{Z}$. Zauważmy, że $(a + 2)^4 - a^4 = [(a+2)^2-a^2]\cdot[(a+2)^2+a^2] = [(a+2)-a]\cdot[(a+2)+a]\cdot[a^2+4a+4+a^2] = 2 \cdot (2a+2) \cdot (2a^2+4a+4) = 8a(a+1)(a^2+2a+2)$. Ponadto $a(a+1)$ jest iloczynem dwóch kolejnych liczb całkowitych, więc jest podzielne przez 2. Stąd $16 \mid (a + 2)^4 - a^4$.

Zadanie 22.67. Z dzielenia przez 10 mamy dokładnie 10 różnych reszt: $0, 1, \ldots, 9$, a liczb jest 11, więc pewne dwie z nich, powiedzmy a i b dają tę samą resztę r z dzielenia przez 10. Wtedy $a = 10k + r$ i $b = 10l+r$ dla pewnych $k, l \in \mathbb{Z}$, skąd $a-b = 10(k-l)$, czyli $10 \mid a-b$.

Zadanie 22.68. Niech a będzie dowolną liczbą naturalną dwucyfrową. Wtedy $a = \overline{xy} = 10x + y$ dla pewnych cyfr x, y. Liczba po przestawieniu cyfr jest równa $b = \overline{yx} = 10y + x$. Zatem $a+b = 11x+11y = 11(x + y)$, skąd $11 \mid a + b$, co należało wykazać.

Zadanie 22.69. Niech a będzie liczbą naturalną trzycyfrową. Wtedy $a = \overline{xyz} = 100x + 10y + z$ dla pewnych cyfr x, y, z. Liczba po przestawieniu cyfr jest równa $b = \overline{zyx} = 100z + 10y + x$. Stąd $a - b = 99x - 99z = 99(x - z)$, a zatem $99 \mid a - b$, co należało wykazać.

Zadanie 22.70. Załóżmy, że tak nie jest. Wtedy istnieje trzycyfrowa liczba naturalna $a = \overline{xyz}$ taka, że $\overline{xyz} - \overline{zyx} = A^2$ dla pewnego naturalnego A. Stąd $99(x - z) = A^2$. Zatem $11 \mid A^2$ i $3 \mid A^2$, więc $11 \mid A$ i $3 \mid A$, skąd $99 \mid A$. Zatem $A = 99B$ dla pewnego $B \in \mathbb{N}$ oraz $99(x-z) = 99^2B^2$. Stąd $x-z = 99B^2$, czyli $x = 99B^2+z \geqslant 99B^2 \geqslant 99$ i mamy sprzeczność, bo $x \leqslant 9$.

Przypuszczenie, że istnieje taka liczba trzycyfrowa doprowadziło nas do sprzeczności. Wobec tego takiej liczby nie ma.

Zadanie 22.71. Mamy, że $\overline{xy} - \overline{yx} = (10x + y) - (10y + x) = 9x - 9y = 9(x - y)$. Jeśli $9(x - y) = a^2$ dla pewnego $a \in \mathbb{N}$, to $3 \mid a^2$, skąd $3 \mid a$, więc $a = 3b$ dla pewnego $b \in \mathbb{N}$. Stąd $9(x - y) = 9b^2$

i $x - y = b^2$, czyli $x = b^2 + y$, ale $x \leqslant 9$, więc $b^2 \leqslant 9$, skąd $b = 1, 2, 3$. Dla $b = 1$ jest $x = y + 1$ i mamy liczby: $10, 21, 32, 43, 54, 65, 76, 87, 98$. Dla $b = 2$: $x = y + 4$, więc mamy liczby: $40, 51, 62, 73, 84, 95$. Dla $b = 3$, $x = 9 + z$, więc mamy liczbę 90.

Zatem wszystkimi szukanymi liczbami są:
$10, 21, 32, 40, 43, 51, 54, 62, 65, 73, 76, 84, 87, 90, 95, 98$.

Zadanie 22.72. Zauważmy, że $\overline{xyz} = 100x + 10y + z \leqslant 100x + 100y + 100z$, skąd $\frac{\overline{xyz}}{x+y+z} \leqslant 100$. Ponadto $\frac{100}{1+0+0} = 100$, więc szukana największa wartość wyrażenia $\frac{\overline{xyz}}{x+y+z}$ jest równa 100.

Zadanie 22.73. Zauważmy, że dla $k, l \in \mathbb{Z}$ zachodzi wzór: $(2k)^2 + (2l)^2 = 4(k^2 + l^2)$, więc suma kwadratów dwóch liczb parzystych daje resztę 0 z dzielenia przez 4. Ponadto, $(2k)^2 + (2l + 1)^2 = 4(k^2 + l^2 + l) + 1$, więc suma kwadratów dwóch liczb całkowitych różnej parzystości daje resztę 1 z dzielenia przez 4. W końcu, $(2k + 1)^2 + (2l + 1)^2 = 4(k^2 + k + l^2 + l) + 2$, czyli suma kwadratów dwóch liczb całkowitych nieparzystych daje resztę 2 z dzielenia przez 4. Ponieważ nie ma innych przypadków, więc teza została udowodniona.

Zadanie 22.74. Dane liczby można zapisać tak: $2n, 2n+1, 2n+2$, gdzie $n \in \mathbb{N}$. Zatem iloczyn tych liczb wynosi $2n(2n + 1)(2n + 2) = 4n(n + 1)(2n + 1)$. Z zadania 22.64, $n(n + 1)(2n + 1) = 6k$ dla pewnego $k \in \mathbb{N}$, więc $2n(2n + 1)(2n + 2) = 24k$, czyli 24 dzieli liczbę $2n(2n + 1)(2n + 2)$.

Zadanie 22.75. Dwie kolejne liczby całkowite to k i $k + 1$ dla $k \in \mathbb{Z}$. Stąd różnica ich kwadratów wynosi $(k+1)^2 - k^2 = 2k+1$, czyli jest liczbą nieparzystą.

Zadanie 22.76. Ponieważ $308 = 4 \cdot 77$, więc $4 \mid 308$ i $8 \nmid 308$, ale $4 \mid 8x$ i $4 \mid 24y$ oraz $8 \mid 8x$ i $8 \mid 24y$, więc $4 \mid 5z$ i $8 \nmid 5z$, skąd $4 \mid z$ i $8 \nmid z$. Ponieważ $z \in \{0, 1, \ldots, 9\}$, więc $z = 4$ i $8x + 24y = 288$, co jest równoważne temu, że $x + 3y = 36$. Jeśli $x < 9$, to $x + 3y < 9 + 3 \cdot 9 = 36$ i mamy sprzeczność. Zatem $x = 9$, skąd $3y = 27$ i $y = 9$.

Wobec tego $x = y = 9$ i $z = 4$ jest jedynym rozwiązaniem spełniającym podane warunki.

Zadanie 22.77. Ponieważ $2x+5y = 2(x+2y)+y$, więc $k = x+2y \in \mathbb{N}$ i $y = 2001-2k$. Stąd $x = k-2\cdot(2001-2k) = 5k-4002$. Zatem $2001-2k > 0$ i $5k-4002 > 0$, skąd $801 \leqslant k \leqslant 1000$. Ostatecznie $x = 5k-4002$ i $y = 2001-2k$, gdzie $k \in \{801, 802, \ldots, 1000\}$.

Zadanie 22.78. Trzy kolejne liczby całkowite można zapisać jako: $k-1, k, k+1$, gdzie $k \in \mathbb{Z}$. Zatem suma sześcianów tych liczb jest równa $s = (k-1)^3+k^3+(k+1)^3 = k^3-3k^2+3k-1+k^3+k^3+3k^2+3k+1 = 3k^3+6k = 3k(k^2+2)$. Stąd, jeśli $3 \mid k$, to $9 \mid s$, a jeżeli $3 \nmid k$, to z zadania 22.8, $k^2 = 3t+1$ dla pewnego $t \in \mathbb{N}_0$, więc $3 \mid k^2+2$ i też $9 \mid s$.

Zadanie 22.79. Szukamy $a, b \in \{0, 1, \ldots, 9\}$, $a \neq 0$ takich, że $\overline{aabb} = K^2$ dla pewnego $K \in \mathbb{N}$. Dalej, $\overline{aabb} = a\cdot 1000+a\cdot 100+b\cdot 10+b = 100\cdot(10a+a)+11b = 100\cdot 11a+11b = 11\cdot\overline{a0b}$, więc $11 \mid K^2$, skąd $K = 11k$ dla pewnego $k \in \mathbb{N}$. Zatem $11\cdot\overline{a0b} = 11^2\cdot k^2$, skąd $\overline{a0b} = 11k^2$. Ponadto $\overline{a0b} = 99a+(a+b)$, więc $11 \mid a+b$, ale $0 < a+b \leqslant 9+9 = 18$, więc $a+b = 11$. Stąd $a \geqslant 2$ i $9a+1 = k^2$. Jeśli $a = 2$, to $19 = k^2$ i mamy sprzeczność. Jeśli $a = 3$, to $28 = k^2$ i też mamy sprzeczność. Jeśli $a = 4$, to $37 = k^2$, co prowadzi do sprzeczności. Jeśli $a = 5$, to $46 = k^2$ i też mamy sprzeczność. Jeśli $a = 6$, to $55 = k^2$, co jest niemożliwe. Dla $a = 7$, $64 = k^2$, skąd $k = 8$ i $b = 4$, przy czym $7744 = 88^2$. Dla $a = 8$, $73 = k^2$, co jest niemożliwe. Dla $a = 9$, $82 = k^2$ i też mamy sprzeczność.

Podsumowując, tylko liczba 7744 spełnia warunki zadania.

Zadanie 22.80. Jeżeli n jest liczbą naturalną złożoną, to istnieją liczby naturalne $a, b > 1$ takie, że $n = ab$ i wtedy $1 < a < n$ oraz $1, a, n$ są dzielnikami n oraz $1+a+n > n+1$, a zatem suma naturalnych dzielników liczby n jest większa niż $n+1$.

Na odwrót, załóżmy, że suma wszystkich naturalnych dzielników liczby naturalnej n jest większa niż n. Ponieważ $D_1 = \{1\}$ i $1 < 1+1$, więc $n > 1$. Jeśli n jest liczbą pierwszą, to n ma dokładnie dwa dzielniki: 1 i n i ich suma jest równa $n+1$. Wobec tego $n > 1$ i n nie jest liczbą pierwszą, a zatem n jest liczbą złożoną.

Zadanie 22.81. Z warunków zadania i cechy podzielności przez 9

wynika, że nieznana liczba trzycyfrowa $a = \overline{xyz}$ jest podzielna przez 9. Ponadto $a = \frac{47}{36} \cdot \overline{zyx}$, skąd $36 \cdot a = 47 \cdot \overline{zyx}$, ale $\mathrm{NWD}(47, 36) = 1$, więc z zasadniczego twierdzenia arytmetyki, $47 \mid a$. Ponadto $\mathrm{NWD}(9, 47) = 1$, więc $9 \cdot 47 \mid a$, czyli $423 \mid a$, ale liczba a jest trzycyfrowa, więc $a = 423$ lub $a = 2 \cdot 423 = 846$, bo $3 \cdot 423 > 999$. Ponadto $8 + 4 + 6 > 9$ i $4 + 2 + 3 = 9$, więc $a = 423$. Pozostaje sprawdzić, czy $423 = \frac{47}{36} \cdot 324$, co jest równoważne temu, że $423 \cdot 36 = 47 \cdot 324$, czyli po skróceniu przez 47, $9 \cdot 36 = 324$, a to jest prawdą. Wobec tego jedyną liczbą spełniającą warunki zadania jest liczba 423.

Zadanie 22.82. Niech $x, y \in \mathbb{N}$ i $x(y+1)^2 = 243y$. Wtedy mamy, że $y \mid x(y+1)^2$. Ponieważ $\mathrm{NWD}(y, y+1) = \mathrm{NWD}(y, 1) = 1$, więc też $\mathrm{NWD}(y, (y+1)^2) = 1$ i z zasadniczego twierdzenia arytmetyki $y \mid x$. Zatem $x = ty$ dla pewnego $t \in \mathbb{N}$ oraz $t(y+1)^2 = 243$. Ponadto $243 = 3^5$ i spośród dzielników naturalnych większych od 1 liczby 3^5 kwadratami liczb naturalnych są jedynie 3^2 i 3^4 oraz $y + 1 > 1$, więc $(y+1)^2 = 3^2$ i $t = 3^3$ lub $(y+1)^2 = 3^4$ i $t = 3$. Wobec tego $y = 2$ i $t = 27$ lub $y = 8$ i $t = 3$. Zatem $x = 54$ i $y = 2$ lub $x = 24$ i $y = 8$. Proste sprawdzenie pokazuje, że podane liczby spełniają równanie $x(y+1)^2 = 243y$.

Zadanie 22.83. Niech $x, y \in \mathbb{N}$. Wtedy $x^4 - y^4 = (x^2 - y^2)(x^2 + y^2)$ oraz $D_{65} = \{1, 5, 13, 65\}$ i $x^2 + y^2 > x^2 - y^2$, więc $x^2 + y^2 = 13$ i $x^2 - y^2 = 5$ lub $x^2 + y^2 = 65$ i $x^2 - y^2 = 1$.

W pierwszym przypadku po odjęciu stronami $2y^2 = 8$, skąd $y^2 = 4$ oraz $x^2 = 9$, więc $y = 2$ i $x = 3$.

W drugim przypadku po odjęciu stronami $2y^2 = 64$, skąd $y^2 = 32$ oraz $x^2 = 33$, ale $5^2 < 33 < 6^2$, więc mamy sprzeczność.

Ostatecznie zatem: $x = 3$ i $y = 2$.

Zadanie 22.84. Niech $x, y \in \mathbb{Z}$ i $2xy + 3y^2 = 24$. Wtedy $2 \mid 3y^2$, skąd $2 \mid y$, czyli $y = 2t$ dla pewnego $t \in \mathbb{Z}$ oraz równanie przybiera postać: $4xt + 12t^2 = 24$. Zatem $t(x + 3t) = 6$, skąd $t = 1$ i $x + 3t = 6$ lub $t = -1$ i $x + 3t = -6$ lub $t = 2$ i $x + 3t = 3$ lub $t = -2$ i $x + 3t = -3$ lub $t = 3$ i $x + 3t = 2$ lub $t = -3$ i $x + 3t = -2$ lub $t = 6$ i $x + 3t = 1$ lub $t = -6$ i $x + 3t = -1$. Stąd otrzymujemy wszystkie rozwiązania naszego równania: $x = 3$ i $y = 2$ lub $x = -3$

i $y = -2$ lub $x = -3$ i $y = 4$ lub $x = 3$ i $y = -4$ lub $x = -7$ i $y = 6$ lub $x = 7$ i $y = -6$ lub $x = -17$ i $y = 12$ lub $x = 17$ i $y = -12$.

Zadanie 22.85. Z założenia $a^2 = (a+b) \cdot t$ dla pewnego $t \in \mathbb{Z}$. Ponadto $b^2 - a^2 = (b-a)(a+b)$, więc $b^2 = (a+b)t + (b-a)(a+b) = (a+b)(t+b-a)$ i $t+b-a \in \mathbb{Z}$, więc $a+b \mid b^2$.

Zadanie 22.86. a). Ponieważ $x^2 - y^2 = (x-y) \cdot (x+y)$, więc $x^2 - y^2 = 24 \iff (x-y)(x+y) = 24$. Jeśli $x, y \in \mathbb{N}$ i $(x-y)(x+y) = 24$, to $x+y > 0$, więc $x-y > 0$, skąd $x-y \in \mathbb{N}$. Zatem $x-y$ jest dzielnikiem liczby 24, zaś $x+y$ jest jego dzielnikiem dopełniającym. Ponadto $x-y < x+y$ i $(x-y)+(x+y) = 2x$ - liczba parzysta. Ponieważ $D_{24} = \{1, 12; 3, 8; 4, 6\}$, więc $x-y = 4$ i $x+y = 6$, skąd po dodaniu stronami $2x = 10$. Zatem $x = 5$ i $y = 1$.

b) Rozumując podobnie jak w a) uzyskujemy, że $x-y$ jest dzielnikiem liczby 18, zaś $x+y$ jest jego dzielnikiem dopełniającym, przy czym suma tych dzielników jest liczbą parzystą, ale $D_{18} = \{1, 18; 2, 9; 3, 6\}$ i $1+18$, $2+9$, $3+6$ są liczbami nieparzystymi, więc nasze równanie nie posiada rozwiązania w liczbach naturalnych x i y.

c). Zauważmy, że $xy = x+y \iff (x-1)(y-1) = 1$. Stąd $x-1 = y-1 = 1$ lub $x-1 = y-1 = -1$, ale $x, y \in \mathbb{N}$, więc $x = y = 2$.

d). Zauważmy, że $xy = 3x + 2y + 1 \iff (x-2)(y-3) = 18$. Ponieważ $D_{18} = \{1, 18; 2, 9; 3, 6\}$ oraz $x, y \in \mathbb{N}$, więc $x-2 \geqslant -1$ i $y-3 \geqslant -2$. Stąd $x-2, y-3 \in \mathbb{N}$ i $x-2 = 1$ oraz $y-3 = 18$ lub $x-2 = 2$ i $y-3 = 9$ lub $x-2 = 3$ i $y-3 = 6$ lub $x-2 = 18$ i $y-3 = 1$ lub $x-2 = 9$ i $y-3 = 2$ lub $x-2 = 6$ i $y-3 = 3$. Zatem ostatecznie: $(x, y) \in \{(3, 21), (4, 12), (5, 9), (20, 4), (11, 5), (8, 6)\}$.

Zadanie 22.87. Oznaczmy prawą stronę naszego wzoru przez P i niech $A = x(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$ oraz niech $B = y(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$. Wtedy $P = A - B$. Ponadto $A = x^n + C$, gdzie $C = x^{n-1}y + x^{n-2}y^2 + \ldots + x^2y^{n-2} + xy^{n-1}$ oraz $B = y^{n+1} + C$. Wobec tego $P = x^n + C - y^n - C = x^n - y^n$, co kończy nasz dowód.

Zadanie 22.88. Na mocy wzoru (22.1), $x^n - y^n = k \cdot (x-y)$, gdzie $k = x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1} \in \mathbb{Z}$. Stąd $x-y \mid x^n - y^n$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.89. a). Wystarczy w zadaniu 22.88 podstawić $x = 10$ i $y = 1$. b). Ponieważ $3 \mid 9$ i na mocy a), $9 \mid 10^n - 1$, więc z przechodniości relacji podzielności, $3 \mid 10^n - 1$.

c). Wystarczy w zadaniu 22.88 podstawić $x = 10$ i $y = -1$. d). Podstawiając w zadaniu 22.88 $x = 4$ i $y = 1$ mamy, że $3 \mid 4^n - 1$. Stąd i na mocy b), $3 \mid (10^n - 1) + (4^n - 1)$, czyli $3 \mid 10^n + 4^n - 2$.

e). Wystarczy w zadaniu 22.88 podstawić $x = 9$ i $y = 1$.

Zadanie 22.90. Podstawmy w tożsamości (22.1) w miejsce y liczbę $(-y)$ i w miejsce n liczbę $2k + 1$. Pamiętając o tym, że $(-y)^{2t} = y^{2t}$ i $(-y)^{2t-1} = -y^{2t-1}$ dla każdego $t \in \mathbb{N}$ oraz $x-(-y) = x+y$ uzyskujemy stąd od razu wzór (22.2).

Zadanie 22.91. Na mocy wzoru (22.2), $x^{2k+1} + y^{2k+1} = t \cdot (x + y)$ dla $t = x^{2k} - x^{2k-1}y + \ldots - xy^{2k-1} + y^{2k} \in \mathbb{Z}$. Zatem $x+y \mid x^{2k+1}+y^{2k+1}$. Ponadto oczywiście $x + y \mid x + y$, więc $x + y \mid x^{2k-1} + y^{2k-1}$ dla każdego $k \in \mathbb{N}$.

Zadanie 22.92. a). Ponieważ $4 = 5 - 1$, więc z zadania 22.88, $4 \mid 5^k - 1$ dla każdego $k \in \mathbb{N}$, skąd $4 \mid 5^{5n-2} - 1$, ale $4 \mid 4$ i $5^{5n-2} + 3 = (5^{5n-2} - 1) + 4$, więc $4 \mid 5^{5n-2} + 3$.

b). Ponieważ $10 = 9 + 1$, więc z zadania 22.91, $10 \mid 9^{2n+1} + 1$, ale $9^{2n+1} + 1 = (3^2)^{2n+1} + 1 = 3^{4n+2} + 1$, więc $10 \mid 3^{4n+2} + 1$.

c). Zauważmy, że $133 = 12^2 - 11$, więc z zadania 22.88 mamy, że $133|(12^2)^n - 11^n$, czyli $133|12^{2n} - 11^n$, skąd $133|12(12^{2n} - 11^n)$. Zatem $133|12^{2n+1} - 12 \cdot 11^n$, ale $133|133 \cdot 11^n$ i $(12^{2n+1} - 12 \cdot 11^n) + 133 \cdot 11^n = 12^{2n+1} + (133 - 12) \cdot 11^n = 12^{2n+1} + 121 \cdot 11^n = 12^{2n+1} + 11^2 \cdot 11^n = 12^{2n+1} + 11^{n+2}$, więc $133|12^{2n+1} + 11^{n+2}$.

Zadanie 22.93. Po opuszczeniu nawiasów prawa strona dowodzonego wzoru przybiera postać $P = a^3 + ab^2 + ac^2 - a^2b - a^2c - abc + a^2b + b^3 + bc^2 - ab^2 - abc - b^2c + a^2c + b^2c + c^3 - abc - ac^2 - bc^2$, więc po skróceniu wyrazów podobnych uzyskamy tezę.

Zadanie 22.94. Ponieważ $8 = 2^3$ i $6 = 2 \cdot 3$, więc nasze równanie możemy zapisać w postaci $\frac{2^{3x}-2^x}{2^x \cdot 3^x - 3^x} = 2$, którą można zapisać też jak $\frac{2^x \cdot (2^{2x}-1)}{3^x \cdot (2^x-1)} = 2$. Ponadto $2^{2x} - 1 = (2^x - 1) \cdot (2^x + 1)$, więc po skró-

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

ceniu przez $2^x - 1$ uzyskujemy równanie $\frac{2^x \cdot (2^x+1)}{3^x} = 2$, czyli równanie $2^x \cdot (2^x + 1) = 2 \cdot 3^x$. Stąd dla $x > 1$ lewa strona jest podzielna przez 4, a prawa strona nie jest podzielna przez 4. Zatem $x = 1$ i wtedy $\frac{8^x - 2^x}{6^x - 3^x} = \frac{8-2}{6-3} = 2$. Stąd ostatecznie $x = 1$.

Zadanie 22.95. Niech $x, y \in \mathbb{N}$ i $\frac{1}{x} + \frac{1}{y} = \frac{2}{35}$. Wtedy $\frac{2}{35} > \frac{1}{x}$, skąd $x > \frac{35}{2}$, czyli $2x - 35 > 0$. Podobnie pokazujemy, że $2y - 35 > 0$. Dalej, $\frac{x+y}{xy} = \frac{2}{35}$, więc $2xy = 35(x + y)$, czyli po pomnożeniu obu stron przez 2, $4xy - 70x - 70y = 0$. Zatem $(2x - 35) \cdot (2y - 35) = 35^2$. Ponadto $35 = 5 \cdot 7$, skąd $35^2 = 5^2 \cdot 7^2$ i $\tau(35^2) = 3 \cdot 3 = 9$ oraz $D_{35^2} = \{1, 5, 25, 7, 49, 35, 245, 175, 1225\}$. Mamy następujące przypadki:

1. $2x - 35 = 1$ i $2y - 35 = 1225$. Wtedy $x = 18$ i $y = 630$.
2. $2x - 35 = 5$ i $2y - 35 = 245$. Wtedy $x = 20$ i $y = 140$.
3. $2x - 35 = 25$ i $2y - 35 = 49$. Wtedy $x = 30$ i $y = 42$.
4. $2x - 35 = 7$ i $2y - 35 = 175$. Wtedy $x = 21$ i $y = 105$.
5. $2x - 35 = 49$ i $2y - 35 = 25$. Wtedy $x = 42$ i $y = 30$.
6. $2x - 35 = 35$ i $2y - 35 = 35$. Wtedy $x = y = 35$.
7. $2x - 35 = 245$ i $2y - 35 = 5$. Wtedy $x = 140$ i $y = 20$.
8. $2x - 35 = 175$ i $2y - 35 = 7$. Wtedy $x = 105$ i $y = 21$.
9. $2x - 35 = 1225$ i $2y - 35 = 1$. Wtedy $x = 630$ i $y = 18$.

Zadanie 22.96. Niech $d \in \mathbb{N}$ oraz niech $d \mid c$. Jeśli $k = \mathrm{NWD}(a, d)$, to $k \mid d$ i $k \mid a$. Zatem $k \mid c$, bo $d \mid c$, ale $\mathrm{NWD}(a, c) = 1$, więc $k = 1$, skąd $\mathrm{NWD}(a, d) = 1$.

Niech $d = \mathrm{NWD}(a \cdot b, c)$. Wtedy $d \mid a \cdot b$ i $d \mid c$ oraz, jak pokazaliśmy, $\mathrm{NWD}(a, d) = 1$. Zatem z zasadniczego twierdzenia arytmetyki mamy, że $d \mid b$. Wobec tego $d \leqslant D = \mathrm{NWD}(b, c)$. Ponadto, $D \mid b$ i $D \mid c$, więc $D \mid a \cdot b$, skąd $D \leqslant d$ i ostatecznie $D = d$, co należało udowodnić.

Zadanie 22.97. Zastosujemy indukcję ze względu na $k \in \mathbb{N}$. Dla $k = 1$ teza wynika z małego twierdzenia Fermata. Przypuśćmy, że $p \mid a^{p^k} - a$ dla pewnego $k \in \mathbb{N}$. Wtedy $a^{p^k} \equiv a \pmod{p}$, więc po podniesieniu tej kongruencji stronami do potęgi p uzyskamy, że $a^{p^{k+1}} \equiv a^p \pmod{p}$. Ponadto, $a^p \equiv a \pmod{p}$, więc $a^{p^{k+1}} \equiv a \pmod{p}$, czyli $p \mid a^{p^{k+1}} - a$. Wobec tego na mocy zasady indukcji nasza teza zachodzi dla dowolnego $k \in \mathbb{N}$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.98. Teza wynika od razu ze wzorów:
$2b+a=7(2x+y+2z)$, $3a+c=7(x+2y+2z)$ i $b+c=7(x+y+z)$.

Zadanie 22.99. Przypuśćmy, że istnieją liczby naturalne x, y, a, b takie, że $x^2+y=a^2$ i $x+y^2=b^2$. Wtedy $a^2>x^2$, skąd $a>x$, czyli $a\geqslant x+1$. Zatem $x^2+y=a^2\geqslant x^2+2x+1$, skąd $y\geqslant 2x+1>x$. Podobnie, $b^2>y^2$, skąd $b\geqslant y+1$ i $x+y^2=b^2\geqslant y^2+2y+1$, czyli $x\geqslant 2y+1>y$. Wobec tego $y>x$ i $x>y$, co prowadzi do sprzeczności. Wobec tego takie liczby x i y nie istnieją.

Zadanie 22.100. Załóżmy, że istnieją różne liczby pierwsze p, q i r oraz liczba całkowita k takie, że $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}=k$. Wtedy po pomnożeniu tej równości przez pqr dostaniemy, że $qr+pr+pq=kpqr$. Stąd $qr=$ $=p(kqr-q-r)$, czyli $p\mid qr$. Zatem z pierwszości liczby p jest $p\mid q$ lub $p\mid r$ i dalej z pierwszości liczb q i r uzyskujemy, że $p=q$ lub $p=r$, co prowadzi do sprzeczności. Wobec tego takie liczby pierwsze p, q, r nie istnieją.

Zadanie 22.101. Z twierdzenia o dzieleniu z resztą wynika, że $n=3k$ lub $n=3k+1$ lub $n=3k+2$ dla pewnego $k\in\mathbb{Z}$. W pierwszym przypadku $2n^2+n+1=3(6k^2+k)+1$, więc $3\nmid 2n^2+n+1$. W drugim przypadku $2n^2+n+1=3(6k^2+5k+1)+1$, więc $3\nmid 2n^2+n+1$. W trzecim przypadku $2n^2+n+1=3(6k^2+9k+3)+2$, więc też $3\nmid 2n^2+n+1$.

Zadanie 22.102. Z założenia wynika, że $3\mid m^2+mn+n^2$, więc też $3\mid (m^2+mn+n^2)-3mn$, czyli $3\mid (m-n)^2$. Ponadto $3\in\mathbb{P}$, więc $3\mid m-n$, skąd $m=n+3k$ dla pewnego $k\in\mathbb{Z}$. Zatem $m^2+mn+n^2=$ $=3n^2+9kn+9k^2$ i ponieważ $9\mid m^2+mn+n^2$, to $9\mid 3n^2$, skąd $3\mid n^2$, czyli $3\mid n$. Dodatkowo $m=n+3k$, a zatem $3\mid m$.

Zadanie 22.103. Warunki zadania można zapisać w postaci: $c\mid a-b$ i $a\mid b-c$ i $b\mid c-a$. Stąd bez zmniejszania ogólności możemy zakładać, że $a\leqslant b\leqslant c$. Wtedy $c\mid b-a$ i $0\leqslant b-a<b\leqslant c$, skąd $b-a=0$, czyli $a=b$. Ponadto $a\mid b-c$, więc $a\mid c$, skąd $c=ak$ dla pewnego $k\in\mathbb{N}$. Na odwrót, jeśli $a=b$ i $c=ak$, to $c\mid a-b$ i $a\mid b-c$ i $b\mid c-a$. Wobec tego wszystkie szukane trójki (a,b,c) liczb na-

turalnych są następującej postaci $(n, n, mn), (n, mn, n), (mn, n, n)$ dla $m, n \in \mathbb{N}$.

Zadanie 22.104. a). Weźmy dowolne $x, y \in \mathbb{N}$ takie, że $x \mid y+1$ i $y \mid x+1$. Wtedy $x \leqslant y+1$ i $y \leqslant x+1$, skąd $x-1 \leqslant y \leqslant x+1$. Zatem mogą zajść tylko następujące przypadki: 1) $y = x-1$, 2) $y = x$, 3) $y = x+1$.

W przypadku 1) $x \geqslant 2$ i $y+1 = x$, więc $x \mid y+1$ oraz $y \mid x+1$ wtedy i tylko wtedy, gdy $x-1 \mid x+1$. Ponadto $x+1 = (x-1)+2$, więc $x-1 \mid x+1 \iff x-1 \mid 2 \iff x \in \{2, 3\}$. Zatem $x = 2$ i $y = 1$ lub $x = 3$ i $y = 2$.

W przypadku 2), $x \mid x+1 \iff x \mid 1 \iff x = 1$, więc $x = y = 1$.

W przypadku 3), $y = x+1$, więc $y \mid x+1$. Ponadto $x \mid y+1$ wtedy i tylko wtedy, gdy $x \mid x+2 \iff x \mid 2 \iff x \in \{1, 2\}$. Zatem $x = 1$ i $y = 2$ lub $x = 2$ i $y = 3$.

Ostatecznie: $(x, y) \in \{(1,1), (1,2), (2,1), (2,3), (3,2)\}$.

b). Weźmy dowolne $x, y \in \mathbb{N}$ takie, że $x \mid 2y+1$ i $y \mid 2x+1$. Ze względu na symetrię warunków nałożonych na x i y możemy zakładać, że $x \leqslant y$. Ponadto $2x+1 = ky$ dla pewnego $k \in \mathbb{N}$, ale $2x+1 \leqslant 3x \leqslant 3y$, więc $ky \leqslant 3y$, skąd $k = 1$ lub $k = 2$ lub $k = 3$.

Jeśli $k = 1$, to $y = 2x+1$, więc $2y+1 = 4x+3$, skąd $x \mid 2y+1$ wtedy i tylko wtedy, gdy $x \mid 3 \iff x \in \{1, 3\}$. Zatem wtedy $x = 1$ i $y = 3$ lub $x = 3$ i $y = 7$. Dla takich x i y jest oczywiście, że $x \mid 2y+1$ i $y \mid 2x+1$.

Jeśli $k = 2$, to $1 = 2(y-x)$, co prowadzi do sprzeczności.

Jeśli $k = 3$, to $2x+1 = 3y$, więc jeśli $x < y$, to $2x < 2y$, skąd $2x+1 < 2y+1 \leqslant 3y$, czyli $2x+1 < 3y$ i mamy sprzeczność. Zatem $x = y$ i $2x+1 = 3x$, skąd $x = y = 1$. Dla takich x i y oczywiście $x \mid 2y+1$ i $y \mid 2x+1$.

Ostatecznie: $(x, y) \in \{(1,1), (1,3), (3,1), (3,7), (7,3)\}$.

Zadanie 22.105. Ułamek $\frac{a}{b}$, gdzie $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ jest nieskracalny, gdy $\mathrm{NWD}(a, b) = 1$.

Badamy nieskracalność ułamka: $\frac{12n+1}{30n+2}$. Korzystamy z algorytmu Euklidesa, $\mathrm{NWD}(12n+1, 30n+2) = \mathrm{NWD}(12n+1, 30n+2-2(12n+$

1)) = NWD(12n+1, 6n) = NWD(6n, 12n+1−2·6n) = NWD(1, 6n) = = 1, bo 1 | 6n. Zatem ten ułamek jest nieskracalny.

Badamy nieskracalność ułamka: $\frac{19n+7}{7n+11}$. Korzystamy z algorytmu Euklidesa, NWD($7n+11, 19n+7$) = NWD($7n+11, 19n+7-2(7n+$ $+11)$) = NWD($7n$+11, $5n$−15) = NWD($5n$−15, $7n$+11−($5n$−15)) = = NWD($5n-15, 2n+36$) = NWD($2n+36, 5n-15-2(2n+36)$) = = NWD($n-87, 2n+36$) = NWD($n-87, 2n+36-2(n-87)$) = = NWD($n-87, 210$), ale $210 = 2\cdot 3\cdot 5\cdot 7$, więc nie zawsze ten ułamek jest nieskracalny, na przykład dla $n = 1$ jest on skracalny przez 2.

Badamy nieskracalność ułamka: $\frac{2n+1}{9n+4}$. Korzystamy z algorytmu Euklidesa, NWD($2n+1, 9n+4$) = NWD($2n+1, 9n+4-4(2n+1)$) = = NWD($2n+1, n$) = NWD($n, 2n+1-2\cdot n$) = NWD($n, 1$) = 1, bo 1 | n. Zatem ten ułamek jest nieskracalny.

Badamy nieskracalność ułamka: $\frac{8n+3}{13n+5}$. Korzystamy z algorytmu Euklidesa, NWD($8n+3, 13n+5$) = NWD($8n+3, 13n+5-(8n+$ $+3)$) = NWD($8n+3, 5n+2$) = NWD($5n+2, 8n+3-(5n+2)$) = = NWD($5n+2, 3n+1$) = NWD($3n+1, 5n+2-(3n+1)$) = = NWD($3n+1, 2n+1$) = NWD($2n+1, 3n+1-(2n+1)$) = = NWD($2n+1, n$) = NWD($n, 2n+1-2\cdot n$) = NWD($n, 1$) = 1, bo 1 | n. Zatem ten ułamek jest nieskracalny.

Badamy nieskracalność ułamka: $\frac{2n-1}{9n+4}$. Korzystamy z algorytmu Euklidesa, NWD($2n-1, 9n+4$) = NWD($2n-1, 9n+4-4(2n-1)$) = = NWD($2n-1, n+8$) = NWD($n+8, 2n-1-2(n+8)$) = = NWD($n+8, -17$) = NWD($17, n+8$), skąd wynika, że ten ułamek nie zawsze jest nieskracalny, na przykład dla $n = 9$ można go skrócić przez 17.

Badamy nieskracalność ułamka: $\frac{14n+3}{21n+4}$. Korzystamy z algorytmu Euklidesa, NWD($14n+3, 21n+4$) = NWD($14n+3, 21n+4-(14n+$ $+3)$) = NWD($14n+3, 7n+1$) = NWD($7n+1, 14n+3-2(7n+1)$) = = NWD($7n+1, 1$) = 1, bo 1 | $7n+1$. Zatem ten ułamek jest nieskracalny.

Zadanie 22.106. Oznaczmy szukaną liczbę naturalną przez a. Ponieważ reszta z dzielenia przez a jest mniejsza od a, więc $a > 8$. Ponadto $4373 = xa+8$ i $826 = ya+7$ dla pewnych $x, y \in \mathbb{Z}$, więc $4365 = = xa$ i $819 = ya$. Z twierdzenia 8.39 wynika, że a | NWD(4365, 819).

Przy pomocy algorytmu Euklidesa obliczamy:
$\mathrm{NWD}(819, 4365) = \mathrm{NWD}(819, 270) = \mathrm{NWD}(270, 9) = 9$, bo $9 \mid 270$. Stąd $a > 8$ i $a \mid 9$, a zatem $a = 9$. Ponadto, $[4373]_9 = [4+3+7+3]_9 = [17]_9 = 8$ i $[826]_9 = [8+2+6]_9 = [16]_9 = 7$. Wobec tego szukaną liczbą jest $a = 9$.

Zadanie 22.107. Jeżeli $n \in \{1, 2, 3\}$, to $k = 1$ i oczywiście $1 \mid n$. Jeżeli $n \in \{4, 6, 8\}$, to $k = 2$ i oczywiście wtedy $1 \mid n$ i $2 \mid n$. Jeżeli $n = 12$, to $k = 3$ i wtedy $1 \mid n$, $2 \mid n$ i $3 \mid n$. Jeżeli $n = 24$, to $k = 4$ i oczywiście $1 \mid n$, $2 \mid n$, $3 \mid n$ oraz $4 \mid n$.

Na odwrót, załóżmy, że $n > 4$ i n jest podzielne przez wszystkie liczby naturalne k takie, że $k^2 \leqslant n$. Istnieje największa liczba naturalna s taka, że $s^2 \leqslant n$. Wtedy $s \geqslant 2$, bo $n > 4$ i $n < (s+1)^2$, więc $n = s^2 + l$ dla pewnego $l \in \{0, 1, \ldots, 2s\}$, ale $s \mid n$, więc $s \mid l$, skąd $l = 0$ lub $l = s$ lub $l = 2s$.

Niech $l = 0$. Wtedy $n = s^2$ i $s - 1 \in \mathbb{N}$, więc $s - 1 \mid s^2$, ale $s^2 = (s-1)(s+1) + 1$, więc $s - 1 \mid 1$, skąd $s - 1 = 1$ i $s = 2$ oraz $n = 4$.

Niech $l = s$. Wtedy $n = s^2 + s$ i $s - 1 \in \mathbb{N}$, więc $s - 1 \mid s^2 + s$, ale $s^2 + s = (s-1)(s+2) + 2$, więc $s - 1 \mid 2$, skąd $s - 1 = 1$ lub $s - 1 = 2$, czyli $s = 2$ lub $s = 3$, skąd $n = 6$ lub $n = 12$.

Niech $l = 2s$. Wtedy $n = s^2 + 2s$ $s - 1 \in \mathbb{N}$, więc $s - 1 \mid s^2 + 2s$, ale $s^2 + 2s = (s-1)(s+3) + 3$, więc $s - 1 \mid 3$, skąd $s - 1 = 1$ lub $s - 1 = 3$, czyli $s = 2$ lub $s = 4$ oraz $n = 8$ lub $n = 24$.

Wobec tego wszystkimi liczbami naturalnymi n, które są podzielne przez każdą liczbę naturalną k taką, że $k^2 \leqslant n$ są jedynie liczby: 1, 2, 3, 4, 6, 8, 12 i 24.

Zadanie 22.108. Niech n będzie liczbą naturalną posiadającą dokładnie 4 dzielniki. Wtedy $n > 1$, więc istnieją różne liczby pierwsze $p_1, \ldots, p_s$ oraz liczby naturalne $a_1, \ldots, a_s$ takie, że $n = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$. Ze stwierdzenia 9.23 liczba wszystkich dzielników liczby n wynosi $\tau(n) = (a_1 + 1) \cdot \ldots \cdot (a_s + 1)$, a ponieważ $a_i \geqslant 1$ dla każdego $i = 1, \ldots, s$, więc $\tau(n) \geqslant 2^s$. Stąd $4 \geqslant 2^s$, czyli $s = 1$ lub $s = 2$. Jeśli $s = 1$, to $n = p_1^{a_1}$ i $4 = a_1 + 1$, skąd $a_1 = 3$ i $n = p_1^3$. Jeśli $s = 2$, to $n = p_1^{a_1} \cdot p_2^{a_2}$ i $(a_1+1)(a_2+1) = 4$, a ponieważ $a_1+1, a_2+1 \geqslant 2$, to $a_1+1 = a_2+1 = 2$, skąd $a_1 = a_2 = 1$. Wobec tego $n = p_1 \cdot p_2$.

Podsumowując, liczba naturalna ma dokładnie 4 dzielniki wtedy i tylko wtedy, gdy jest sześcianem pewnej liczby pierwszej lub gdy jest iloczynem dwóch różnych liczb pierwszych.

Zadanie 22.109. a). Niech n będzie liczbą naturalną taką, że $\tau(n) = 18$. Wtedy $n > 1$, więc istnieją różne liczby pierwsze $p_1, \ldots, p_s$ oraz liczby naturalne $a_1, \ldots, a_s$ takie, że $n = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$ oraz $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_s$. Ze stwierdzenia 9.23, $\tau(n) = (a_1 + 1) \cdot \ldots \cdot (a_s + 1)$, więc $(a_1 + 1) \cdot \ldots \cdot (a_s + 1) = 18$, ale $a_i \geqslant 1$ dla każdego $i = 1, \ldots, s$, więc $\tau(n) \geqslant 2^s$. Stąd $18 \geqslant 2^s$, czyli $s = 1$ lub $s = 2$ lub $s = 3$ lub $s = 4$.

Jeśli $s = 4$, to $(a_1 + 1)^4 \leqslant (a_1 + 1)(a_2 + 1)(a_3 + 1)(a_4 + 1) = 18$, skąd $a_1 + 1 \leqslant 2$, a zatem $a_1 + 1 = 2$ i $(a_2 + 1)(a_3 + 1)(a_4 + 1) = 9$. Wobec tego $(a_2 + 1)^3 \leqslant (a_2 + 1)(a_3 + 1)(a_4 + 1) = 9$, skąd $a_2 + 1 \leqslant 2$, czyli $a_2 + 1 = 2$ i $2(a_3 + 1)(a_4 + 1) = 9$, skąd $2 \mid 9$, co prowadzi do sprzeczności. Zatem $s \neq 4$.

Załóżmy, że $s = 3$. Wtedy $(a_1+1)^3 \leqslant (a_1+1)(a_2+1)(a_3+1) = 18$, skąd $a_1 + 1 \leqslant 2$, a zatem $a_1 + 1 = 2$ i $(a_2 + 1)(a_3 + 1) = 9$, ale $a + 2 + 1, a_3 + 1 \geqslant 2$ i $D_9 = \{1, 3, 9\}$, więc $a_2 + 1 = a_3 + 1 = 3$. Stąd $a_1 = 1$ i $a_2 = a_3 = 2$ oraz $n = p_1 \cdot p_2^2 \cdot p_3^2$. Na odwrót, dla takiego n na mocy stwierdzenia 9.23, $\tau(n) = 2 \cdot 3 \cdot 3 = 18$.

Załóżmy, że $s = 2$. Wtedy $(a_1+1)(a_2+1) = 18$ i $2 \leqslant a_1+1 \leqslant a_2+1$ oraz $D_{18} = \{1, 2, 3, 6, 9, 18\}$, więc $a_1+1 = 2$ i $a_2+1 = 9$ lub $a_1+1 = 3$ i $a_2 + 1 = 6$, skąd $a_1 = 1$ i $a_2 = 8$ lub $a_1 = 2$ i $a_2 = 5$ oraz $n = p_1 \cdot p_2^8$ lub $n = p_1^2 \cdot p_2^5$. Na odwrót, dla takiego n na mocy stwierdzenia 9.23 mamy, że $\tau(n) = 2 \cdot 9 = 18$ lub $\tau(n) = 3 \cdot 6 = 18$.

Niech w końcu $s = 1$. Wtedy $n = p_1^{a_1}$ i na mocy stwierdzenia 9.23, $\tau(n) = 18 \iff a_1 + 1 = 18 \iff a_1 = 17$. Zatem w tym przypadku $n = p_1^{17}$.

b). Niech n będzie liczbą naturalną taką, że $\tau(n) = 24$. Wtedy $n > 1$, więc istnieją różne liczby pierwsze $p_1, \ldots, p_s$ oraz liczby naturalne $a_1, \ldots, a_s$ takie, że $n = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$ oraz $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_s$. Ze stwierdzenia 9.23, $\tau(n) = (a_1+1)\cdot\ldots\cdot(a_s+1)$, więc $(a_1+1)\cdot\ldots\cdot(a_s+1) = 24$, ale $a_i \geqslant 1$ dla każdego $i = 1, \ldots, s$, więc $\tau(n) \geqslant 2^s$. Stąd $18 \geqslant 2^s$, czyli $s = 1$ lub $s = 2$ lub $s = 3$ lub $s = 4$.

Jeśli $s = 4$, to $(a_1 + 1)^4 \leqslant (a_1 + 1)(a_2 + 1)(a_3 + 1)(a_4 + 1) = 24$,

skąd $a_1+1 \leqslant 2$, a zatem $a_1+1=2$ i $(a_2+1)(a_3+1)(a_4+1)=12$. Wobec tego $(a_2+1)^3 \leqslant (a_2+1)(a_3+1)(a_4+1)=12$, skąd $a_2+1 \leqslant 2$, czyli $a_2+1=2$ i $(a_3+1)(a_4+1)=6$, ale $a_3 \leqslant a_4$ i $D_6=\{1,2,3,6\}$, więc $a_3+1=2$ i $a_4+1=3$. Wobec tego $a_1=a_2=a_3=1$ i $a_4=2$ oraz $n=p_1\cdot p_2\cdot p_3\cdot p_4^2$.

Załóżmy, że $s=3$. Wtedy $(a_1+1)^3 \leqslant (a_1+1)(a_2+1)(a_3+1)=24$, skąd $a_1+1 \leqslant 2$, a zatem $a_1+1=2$ i $(a_2+1)(a_3+1)=12$, ale $a_2+1, a_3+1 \geqslant 2$ i $D_{12}=\{1,2,3,4,6,12\}$, więc $a_2+1=2$ i $a_3+1=6$ lub $a_2+1=3$ i $a_3+1=4$. Wobec tego $a_1=1$, $a_2=1$ i $a_3=5$ lub $a_1=1$, $a_2=2$ i $a_3=3$ oraz $n=p_1\cdot p_2\cdot p_3^5$ lub $n=p_1\cdot p_2^2\cdot p_3^3$.

Załóżmy, że $s=2$. Wtedy $(a_1+1)(a_2+1)=24$ i $2 \leqslant a_1+1 \leqslant a_2+1$ oraz $D_{24}=\{1,2,3,4,6,8,12,24\}$, więc $a_1+1=2$ i $a_2+1=12$ lub $a_1+1=3$ i $a_2+1=8$ lub $a_1+1=4$ i $a_2+1=6$, skąd $a_1=1$ i $a_2=11$ lub $a_1=2$ i $a_2=7$ lub $a_1=3$ i $a_2=5$ oraz $n=p_1\cdot p_2^{11}$ lub $n=p_1^2\cdot p_2^7$ lub $n=p_1^3\cdot p_2^5$.

Niech w końcu $s=1$. Wtedy $n=p_1^{a_1}$ i na mocy stwierdzenia 9.23, $\tau(n)=18 \iff a_1+1=24 \iff a_1=23$. Zatem w tym przypadku $n=p_1^{23}$.

Zadanie 22.110. Niech $n\in\mathbb{N}$ będzie takie, że $12 \mid n$. Wtedy $n>1$, więc istnieją różne liczby pierwsze $p_1,\ldots,p_s$ oraz liczby naturalne $a_1,\ldots,a_s$ takie, że $n=p_1^{a_1}\cdot\ldots\cdot p_s^{a_s}$ oraz $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_s$, ale $12=2^2\cdot 3$, więc $s \geqslant 2$. Z rozwiązania zadania 22.109 a) wynika dodatkowo, że $s=2$ lub $s=3$, przy czym dla $s=2$, $n=p_1\cdot p_2^8$ lub $n=p_1^2\cdot p_2^5$ dla pewnych różnych liczb pierwszych p_1 i p_2, ale $2^2\cdot 3 \mid n$, więc stąd dla $s=2$: $n=3\cdot 2^8$ lub $n=2^2\cdot 3^5$ lub $n=3^2\cdot 2^5$.

Jeśli zaś $s=3$, to na mocy rozwiązania zadania 22.109 a) istnieją różne liczby pierwsze p_1,p_2,p_3 takie, że $n=p_1\cdot p_2^2\cdot p_3^2$, ale $2^2\cdot 3 \mid n$, więc stąd $n=2^2\cdot 3^2\cdot p$ lub $n=2^2\cdot 3\cdot p^2$ dla pewnej liczby pierwszej $p>3$.

Zadanie 22.111. Niech n będzie liczbą naturalną podzielną przez 10. Wtedy $n>1$, więc istnieją różne liczby pierwsze $p_1,\ldots,p_s$ oraz liczby naturalne $a_1,\ldots,a_s$ takie, że $n=p_1^{a_1}\cdot\ldots\cdot p_s^{a_s}$ oraz $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_s$, ale $10=2\cdot 5$, więc $s \geqslant 2$ i $2,5\in\{p_1,\ldots,p_s\}$. Ze stwierdzenia 9.23 mamy, że $\tau(n)=6 \iff (a_1+1)\cdot\ldots\cdot(a_s+1)=6$, ale

$a_i + 1 \geqslant 2$ dla $i = 1, \ldots, s$, więc $2^s \leqslant 6$, skąd $s \leqslant 2$. Ponadto, $s \geqslant 2$, więc $s = 2$. Wobec tego $\{2, 5\} = \{p_1, p_2\}$ oraz $(a_1 + 1)(a_2 + 1) = 6$, ale $D_6 = \{1, 2, 3, 6\}$ i $a_1 \leqslant a_2$, więc $a_1 + 1 = 2$ i $a_2 + 1 = 3$, skąd $a_1 = 1$ i $a_2 = 2$. Wobec tego $n = 2 \cdot 5^2 = 50$ lub $n = 2^2 \cdot 5 = 20$.

Zadanie 22.112. Należy wyznaczyć wszystkie liczby pierwsze a, b, c, d, p takie, że $p = a + b = c - d$. Ponieważ $a, b > 1$, więc $p > 2$, czyli liczba pierwsza p jest nieparzysta. Stąd liczby a i b są różnej parzystości, a ponieważ jedyną parzystą liczbą pierwszą jest liczba 2, więc $a = 2$ lub $b = 2$. Bez zmniejszania ogólności możemy dalej zakładać, że $b = 2$.

Podobnie, ponieważ $c - d$ jest liczbą nieparzystą, więc liczby c i d są różnej parzystości, ale c i d są liczbami pierwszymi i jedyną parzystą liczbą pierwszą jest liczba 2, więc $c = 2$ lub $d = 2$. Jeśli $c = 2$, to $p < 2$, co prowadzi do sprzeczności. Zatem $d = 2$.

Stąd $p - 2, p$ i $p + 2$ są liczbami pierwszymi. Jeśli $p - 2 = 3$, to $p = 5$ i $p + 2 = 7$, przy czym $5 = 3 + 2 = 7 - 2$, czyli liczba pierwsza 5 jest sumą i różnicą dwóch liczb pierwszych. Niech dalej $p - 2 \neq 3$. Ponieważ $p - 2$ jest liczbą pierwszą, więc stąd $3 \nmid p - 2$, ale $p - 2 \geqslant 2$ i $p - 2 \neq 2$, więc z twierdzenia o dzieleniu z resztą wynika, że $p - 2 = 3k + 1$ lub $p - 2 = 3k + 2$ dla pewnego $k \in \mathbb{N}$. W pierwszym przypadku, $p = 3(k + 1)$, więc p jest liczbą złożoną i mamy sprzeczność. Natomiast w drugim przypadku, $p + 2 = 3(k + 2)$ jest liczbą złożoną i też mamy sprzeczność.

Podsumowując, jedyną liczbą pierwszą, która jest sumą i różnicą dwóch liczb pierwszych jest liczba 5.

Zadanie 22.113. *a*) $\Rightarrow$ *b*). Oczywiste, bo każda liczba pierwsza jest większa od 1.

b) $\Rightarrow$ *c*). Załóżmy, że $b \neq 1$. Wtedy $b > 1$, więc z twierdzenia o jednoznaczności rozkładu istnieją różne liczby pierwsze $p_1, \ldots, p_s$ i istnieją liczby naturalne $a_1, \ldots, a_s$ takie, że $b = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$. Jeżeli dla pewnego $i = 1, \ldots, s$ jest $a_i \geqslant 2$, to $p_i^2 \mid b$ wbrew założeniu. Zatem $a_1 = \ldots = a_s = 1$, czyli b jest iloczynem różnych liczb pierwszych.

c) $\Rightarrow$ *a*). Teza jest oczywista dla $b > 1$. Niech dalej $b = p_1 \cdot \ldots \cdot p_s$, gdzie $p_1, \ldots, p_s$ są różnymi liczbami pierwszymi. Załóżmy, że istnieje

liczba naturalna $d > 1$ taka, że $d^2 \mid b$. Wtedy z twierdzenia 9.8 istnieje liczba pierwsza p taka, że $p \mid d$. Zatem $d = tp$ dla pewnego $t \in \mathbb{Z}$, skąd $d^2 = t^2p^2$, a ponieważ $t^2 \in \mathbb{Z}$, więc $p^2 \mid d^2$ i z przechodniości relacji podzielności, $p^2 \mid b$. Stąd $p^2 \mid p_1 \cdot \ldots \cdot p_s$, co przeczy twierdzeniu 9.22. Wobec tego nie istnieje liczba naturalna $d > 1$ taka, że $d^2 \mid b$.

Zadanie 22.114. Oczywiście liczba $a = 1$ spełnia podany warunek. Pokażemy, że jeżeli a jest iloczynem różnych liczb pierwszych $p_1, \ldots, p_s$, to też spełnia ten warunek. Niech zatem $b, n \in \mathbb{N}$ będą takie, że $a \mid b^n$. Wtedy dla $i = 1, \ldots, s$ mamy, że $p_i \mid a$, więc $p_i \mid b^n$ i z twierdzenia 9.14, $p_i \mid b$, ale liczby $p_1, \ldots, p_s$ są parami względnie pierwsze, więc z twierdzenia 8.50, $\mathrm{NWW}(p_1, \ldots, p_s) = p_1 \cdot \ldots \cdot p_s$. Stąd i z twierdzenia 8.36, $p_1 \cdot \ldots \cdot p_s \mid b$, czyli $a \mid b$.

Załóżmy teraz, że $a > 1$ i a nie jest iloczynem różnych liczb pierwszych. Wtedy z zadania 22.113 istnieje liczba pierwsza p taka, że $p^2 \mid a$. Zatem $a = p^2c$ dla pewnego $c \in \mathbb{N}$. Niech $b = pc$ i $n = 2$. Wtedy $b^n = p^2c^2 = ac$, skąd $a \mid b^n$, ale $a = p^2c > pc = b$, więc $a \nmid b$.

Podsumowując możemy powiedzieć, że warunki zadania spełnia jedynie liczba $a = 1$ i liczby a będące iloczynami różnych liczb pierwszych.

Zadanie 22.115. Jeśli a jest liczbą złożoną, to $a = xy$ dla pewnych liczb naturalnych x, y takich, że $1 < x < a$ i $1 < y < a$. Wtedy $a \mid xy$, ale $a \nmid x$ i $a \nmid y$, gdyż $x < a$ i $y < a$ oraz $a, x, y \in \mathbb{N}$.

Ponadto liczba 1 jest dzielnikiem każdej liczby naturalnej, więc dla dowolnych $x, y \in \mathbb{N}$: jeśli $1 \mid xy$, to $1 \mid x$ lub $1 \mid y$. Ponadto na mocy twierdzenia 9.14, jeśli a jest liczbą pierwszą to dla dowolnych liczb naturalnych x, y: jeśli $a \mid xy$, to $a \mid x$ lub $a \mid y$.

Podsumowując mamy, że $a = 1$ lub a jest liczbą pierwszą.

Zadanie 22.116. Weźmy dowolne $x, y \in \mathbb{N}$. Wówczas istnieją różne liczby pierwsze $p_1, \ldots, p_s$ i istnieją nieujemne liczby całkowite a_i, b_i dla $i = 1, 2, \ldots, s$ takie, że $x = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$ oraz $y = p_1^{b_1} \cdot \ldots \cdot p_s^{b_s}$. Stąd $x^k = p_1^{ka_1} \cdot \ldots \cdot p_s^{ka_s}$ i $y^l = p_1^{lb_1} \cdot \ldots \cdot p_s^{lb_s}$. Z twierdzenia 9.17 mamy, że $x^k = y^l$ wtedy i tylko wtedy, gdy $ka_i = lb_i$ dla każdego $i = 1, \ldots, s$. Z zasadniczego twierdzenia arytmetyki wynika, że $k | b_i$, a zatem $b_i = kc_i$

dla pewnego $c_i \in \mathbb{N}_0$, skąd $a_i = lc_i$ dla każdego $i = 1, \ldots, s$. Stąd $x = n^l$ i $y = n^k$ dla $n = p_1^{c_1} \cdot \ldots \cdot p_s^{c_s}$.

Stąd wynika, że $x^k = y^l$ wtedy i tylko wtedy, gdy istnieje $n \in \mathbb{N}$ takie, że $x = n^l$ i $y = n^k$.

Zadanie 22.117. Niech $n \in \mathbb{N}$. Jeśli $n = 1$, to wystarczy wziąć $a = b = 1$. Niech dalej $n > 1$. Wtedy z twierdzenia o jednoznaczności rozkładu istnieją różne liczby pierwsze $p_1, \ldots, p_s$ i istnieją liczby naturalne $\alpha_1, \ldots, \alpha_s$ takie, że $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Dla $i = 1, \ldots, s$ na mocy twierdzenia o dzieleniu z resztą istnieją nieujemne liczby całkowite q_i, r_i takie, że $r_i \in \{0, 1\}$ oraz $\alpha_i = 2q_i + r_i$. Niech $a = p_1^{q_1} \cdot \ldots \cdot p_s^{q_s}$ i $b = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$. Wtedy $n = a^2 b$ oraz na mocy zadania 22.113 liczba b nie dzieli się przez kwadrat liczby pierwszej.

Niech $c, d \in \mathbb{N}$ będą takie, że $n = c^2 d$ i liczba d jest bezkwadratowa. Jeśli $n = 1$, to $c = d = 1$, czyli $c = a$ i $d = b$. Natomiast dla $n > 1$ i dla liczby pierwszej p takiej, że $p \mid c$ lub $p \mid d$ mamy, że $p \mid n$, skąd $p \in \{p_1, \ldots, p_s\}$. Oznacza to, że $c = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ i $d = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$ dla pewnych nieujemnych liczb całkowitych $k_1, e_1, \ldots, k_s, e_s$, przy czym na mocy zadania 22.113, $e_i \in \{0, 1\}$. Stąd $n = p_1^{2k_1+e_1} \cdot \ldots \cdot p_s^{2k_s+e_s}$ i z twierdzenia 9.17 wynika, że $2q_i + r_i = 2k_i + e_i$, skąd na mocy twierdzenia o dzieleniu z resztą $q_i = k_i$ oraz $r_i = e_i$ dla każdego $i = 1, \ldots, s$. Stąd $c = a$ i $d = b$.

Zadanie 22.118. Weźmy dowolne $n \in \mathbb{N}$. Jeżeli n jest nieparzyste, to $n = 2k - 1$ dla pewnego $k \in \mathbb{N}$, skąd $n = 2^{1-1} \cdot (2k - 1)$. Jeżeli zaś n jest parzyste, to z twierdzenia o jednoznaczności rozkładu $n = 2^a \cdot p_1^{b_1} \cdot \ldots \cdot p_s^{b_s}$ dla pewnego $a \in \mathbb{N}$ i dla pewnych nieparzystych liczb pierwszych $p_s > \ldots > p_1 > 2$ oraz dla pewnych $b_1, \ldots, b_s \in \mathbb{N}_0$. Stąd liczba $p_1^{b_1} \cdot \ldots \cdot p_s^{b_s}$ jest nieparzysta, więc jest ona równa $2k - 1$ dla pewnego $k \in \mathbb{N}$ i wystarczy wziąć $l = a + 1$.

Pozostaje wykazać jednoznaczność takiego zapisu. W tym celu weźmy dowolne $a, b, k, l \in \mathbb{N}$ takie, że $2^{l-1}(2k-1) = 2^{a-1}(2b-1)$. Załóżmy, że $l \neq a$. Bez zmniejszania ogólności można zakładać, że $a < l$. Po podzieleniu obu stron równości przez 2^{a-1} otrzymujemy, że $2b - 1 = 2^{l-a}(2k - 1)$, skąd $2 \mid 1$, gdyż liczba 2^{l-a} jest parzysta i mamy sprzeczność. Wobec tego $a = l$ i po skróceniu przez 2^{a-1} uzyskujemy,

że $2b-1=2k-1$, skąd $2b=2k$, a zatem $b=k$. Wobec tego $a=l$ i $b=k$.

Zadanie 22.119. Z założenia wynika, że $35 \mid 6\cdot(6x+13y)$, ale $6\cdot(6x+13y)=36x+78y=35(x+2y)+(x+8y)$, więc stąd $35 \mid x+8y$.

Zadanie 22.120. Liczba naturalna a daje z dzielenia przez liczbę naturalną k resztę $k-1$ wtedy i tylko wtedy, gdy $k \mid a+1$. Ponadto z twierdzenia 8.36 liczba $a+1$ jest podzielna przez k dla każdego $k=2,3,\ldots,10$ wtedy i tylko wtedy, gdy $\mathrm{NWW}(2,3,\ldots,10) \mid a+1$. Wobec tego najmniejszą liczbą spełniającą warunki zadania jest liczba $a=\mathrm{NWW}(2,3,\ldots,10)-1$, ale $4=4^2$, $6=2\cdot 3$, $8=^3$, $9=3^2$ i $10=2\cdot 5$, więc z twierdzenia 9.32, $a=2^3\cdot 3^2\cdot 5\cdot 7-1=2519$.

Zadanie 22.121. Jeżeli $3|p$, to z pierwszości p mamy, że $p=3$ i wtedy $p^2+2=11$ też jest liczbą pierwszą. Jeżeli zaś $3 \nmid p$, to z zadania 22.8 liczba p^2 daje resztę 1 z dzielenia przez 3, a ponieważ ta liczba jest większa od 1, więc $p^2=3k+1$ dla pewnego $k\in\mathbb{N}$. Stąd $p^2+2=3(k+1)$ i $k+1>1$, więc p^2+2 nie jest wtedy liczbą pierwszą.

Wobec tego jedyną liczbą spełniającą warunki zadania jest $p=3$.

Zadanie 22.122. Niech p,q,r będą liczbami pierwszymi takimi, że $p\cdot q\cdot r=5\cdot(p+q+r)$. Wtedy $5 \mid p\cdot q\cdot r$, skąd $5\in\{p,q,r\}$. Bez zmniejszania ogólności możemy zakładać, że $r=5$. Wtedy po skróceniu przez 5 uzyskamy, że $pq=p+q+5$, skąd $(p-1)(q-1)=6$. Ponadto $D_6=\{1,2,3,6\}$, więc $p-1=1$ i $q-1=6$ lub $p-1=2$ i $q-1=3$ lub $p-1=3$ i $q-1=2$ lub $p-1=6$ i $q-1=1$. Dodatkowo p i q są liczbami pierwszymi, więc $p=2$ i $q=7$ lub $p=7$ i $q=2$.

Stąd wszystkimi rozwiązaniami naszego zadania są trójki $(p,q,r)\in\{(2,7,5),(7,2,5),(2,5,7),(7,5,2),(5,2,7),(5,7,2)\}$.

Zadanie 22.123. Dla $n=1$ mamy, że $n^4+4=5$ jest liczbą pierwszą. Pokażemy, że dla naturalnych $n>1$ liczba n^4+4 jest złożona. W tym celu zauważmy, że $n^4+4=n^4+4n^2+4-4n^2=(n^2+2)^2-+(2n)^2=[(n^2+2)-2n][(n^2+2)+2n]=(n^2-2n+2)(n^2+2n+2)$,

ale $n^2+2n+2>2$, bo $n>0$ oraz $n^2-2n+2=(n-1)^2+1>1$, bo $n>1$. Zatem n^4+4 jest liczbą złożoną.

Podsumowując mamy, że dla $n\in\mathbb{N}$, n^4+4 jest liczbą pierwszą wtedy i tylko wtedy, gdy $n=1$. Warto przypomnieć, że rezultat ten został po raz pierwszy udowodniony przez Sophie Germain.

Zadanie 22.124. Dla $n=1$ liczba $n^4+n^2+1=3$ jest liczbą pierwszą. Pokażemy, że dla naturalnych $n>1$ liczba n^4+n^2+1 jest złożona. W tym celu zauważmy, że $n^4+n^2+1=n^4+2n^2+1-n^2=$ $=(n^2+1)^2-n^2=[(n^2+1)-n][(n^2+1)+n]=(n^2-n+1)(n^2+n+1)$, ale $n^2+n+1>n^2-n+1=n(n-1)+1>1$, gdyż $n>1$, więc liczba n^4+n^2+1 jest złożona.

Wobec tego jedyną liczbą naturalną n, dla której n^4+n^2+1 jest liczbą pierwszą jest $n=1$.

Zadanie 22.125. Niech liczby pierwsze p,q,r spełniają warunek $p=q^3-r^3$. Wtedy $p=(q-r)(q^2+qr+r^2)$, skąd $q-r>0$ i $q-r\in\mathbb{Z}$, więc $q-r\in\mathbb{N}$, ale $q^2+qr+r^2>1$ i jest dzielnikiem liczby pierwszej p, więc $q^2+qr+r^2=p$. Stąd $q-r=1$, więc liczby q i r są różnej parzystości, ale $r>1$ i jedyną parzystą liczbą pierwszą jest 2, więc $r=2$, skąd $q=3$ i $p=3^2+3\cdot 2+2^2=19$ i 19 jest liczbą pierwszą.

Wobec tego zadanie ma dokładnie jedno rozwiązanie: $p=19$, $q=3$ i $r=2$.

Zadanie 22.126. Niech p i q będą liczbami pierwszymi takimi, że $p^2-2q^2=1$. Jeżeli $3\mid q$, to $q=3$ i $p^2=19$, co prowadzi do sprzeczności. Zatem $3\nmid q$ i na mocy zadania 22.8 i tego, że $q>1$ mamy, że $q^2=3k+1$ dla pewnego $k\in\mathbb{N}$. Stąd $p^2=2(3k+1)+1=3(2k+1)$, więc $3\mid p^2$, skąd $3\mid p$ i $p=3$ oraz $2q^2=3^2-1=8$, skąd $q=2$.

Wobec tego zadanie ma dokładnie jedno rozwiązanie: $p=3$ i $q=2$.

Zadanie 22.127. Niech p i q będą liczbami pierwszymi takimi, że $6p-22q=12$. Wtedy $3p-11q=6$, więc $11q=3(p-2)$, skąd $3\mid 11q$ i z zasadniczego twierdzenia arytmetyki $3\mid q$. Zatem $q=3$ i $11=p-2$, skąd $p=13$. Ponieważ 13 jest liczbą pierwszą, więc nasze zadanie ma dokładnie jedno rozwiązanie: $p=13$ i $q=3$.

Zadanie 22.128. Zauważmy, że $[0^3]_7 = 0$, $[1^3]_7 = 1$, $[2^3]_7 = [8]_7 = 1$, $[3^3]_7 = [27]_7 = 6$, $[4^3]_7 = [64]_7 = 1$, $[5^5]_7 = [125]_7 = 6$, $[6^3]_7 = [216]_7 = 6$ oraz $x - r \mid x^3 - r^3$ dla $x, r \in \mathbb{Z}$. Stąd wynika, że $[x^3]_7 \in \{0, 1, 6\}$ dla każdego $x \in \mathbb{Z}$, przy czym $[x^3]_7 = 0$ wtedy i tylko wtedy, gdy $7 \mid x$. Weźmy dowolne $a, b, c \in \mathbb{Z}$. Jeśli 7 dzieli jedną z liczb a, b, c, to oczywiście $7 \mid a^3b^3c^3(a^3 - b^3)(b^3 - c^3)(c^3 - a^3) = K$. W przeciwnym przypadku $[a^3]_7, [b^3]_7, [c^3]_7 \in \{1, 6\}$, więc pewne dwie spośród liczb a^3, b^3, c^3 dają tę samą resztę z dzielenia przez 7, skąd ich różnica jest podzielna przez 7. Stąd $7 \mid (a^3 - b^3)(b^3 - c^3)(c^3 - a^3)$, a zatem $7 \mid K$.

Zadanie 22.129. Teza jest oczywista dla $m = 1$ (możemy wtedy wziąć na przykład liczbę 4). Niech dalej $m > 1$. Niech $a = m \cdot (m+1) \cdot \ldots \cdot [m + (m-1)]$. Wtedy $a + m, a + (m+1), \ldots, a + (m + (m-1))$ jest ciągiem m kolejnych liczb naturalnych, przy czym i-ta liczba tego ciągu ma postać $a + [m + (i-1)] > m + (i-1) > 1$ oraz $[m + (i-1)] \mid a$, więc $[m + (i-1)] \mid a + [m + (i-1)]$, co oznacza, że $a + [m + (i-1)]$ jest liczbą złożoną dla każdego $i = 1, 2, \ldots, m$.

Zadanie 22.130. Ponieważ $n > 2$, więc $a = n! - 1 \in \mathbb{N}$ i $a \in (n, n!)$, bo $n! \geqslant 2n > n + 1$. Z twierdzenia 9.8 istnieje liczba pierwsza p taka, że $p \mid a$. Stąd $p \leqslant a$, czyli $p < n!$. Ponadto każda liczba pierwsza $q \leqslant n$ dzieli liczbę $n! = a + 1$, a zatem nie dzieli liczby a. Stąd $p > n$ i $p \in (n, n!)$.

W ten sposób wykazaliśmy, że dla każdej liczby naturalnej $n > 2$ istnieje liczba pierwsza p_n taka, że $n < p_n < n!$. Niech $q_3 = p_3 = 5$ oraz $q_{n+1} = p_{q_n}$ dla $n = 3, 4, \ldots$. Wtedy $q_{n+1} > q_n$ dla $n = 3, 4, \ldots$, więc (q_n) jest rosnącym ciągiem liczb pierwszych. Wobec tego zbiór wszystkich liczb pierwszych jest nieskończony.

Zadanie 22.131. Załóżmy, że $a, n \in \mathbb{N}$, $a, n > 1$ i $a^n - 1$ jest liczbą pierwszą. Z zadania 22.88, $a - 1 \mid a^n - 1$, a ponieważ $a - 1 < a^n - 1$, więc $a - 1 = 1$, skąd $a = 2$. Załóżmy, że n nie jest liczbą pierwszą. Ponieważ $n > 1$, więc n jest liczbą złożoną i istnieją liczby naturalne $r, s > 1$ takie, że $n = rs$. Stąd $s < n$ i z zadania 22.88, $2^s - 1 \mid 2^n - 1$, przy czym $2^s - 1 > 1$, bo $s > 1$ oraz $2^s - 1 < 2^n - 1$, bo $s < n$. Przeczy to pierwszości liczby $2^n - 1$. Wobec tego n jest liczbą pierwszą.

Zadanie 22.132. Zbadamy najpierw, kiedy p i $8p^2+1$ są jednocześnie liczbami pierwszymi. Z twierdzenia o dzieleniu z resztą wynika, że możliwe są tylko następujące przypadki:

1. $p=3k$ dla pewnego $k\in\mathbb{N}$. Wtedy z pierwszości p, $k=1$ i $p=3$ oraz $8p^2-1=71$ jest liczbą pierwszą.

2. $p=3k+1$ dla pewnego $k\in\mathbb{N}$. Wtedy $8p^2+1=8(9k^2+6k+$ $+1)+1=3(24k^2+16k+3)$, więc $8p^2+1$ nie jest liczbą pierwszą.

3. $p=3k+2$ dla pewnego $k\in\mathbb{N}_0$. Wtedy $8p^2+1=8(9k^2+12k+$ $+4)+1=3(24k^2+32k+11)$, więc $8p^2+1$ jest liczbą złożoną.

Wobec tego liczby p i $8p^2+1$ są liczbami pierwszymi wtedy i tylko wtedy, gdy $p=3$. Wówczas $8p^2-1=71$ jest liczbą pierwszą, co kończy dowód.

Zadanie 22.133. Zbadamy najpierw, kiedy p i $5p^2-2$ są jednocześnie liczbami pierwszymi. Z twierdzenia o dzieleniu z resztą wynika, że możliwe są tylko następujące przypadki:

1. $p=3k$ dla pewnego $k\in\mathbb{N}$. Wtedy z pierwszości p, $k=1$ i $p=3$ oraz $5p^2-2=43$ jest liczbą pierwszą.

2. $p=3k+1$ dla pewnego $k\in\mathbb{N}$. Wtedy $5p^2-2=5(9k^2+6k+$ $+1)-2=3(15k^2+10k+1)$, więc $5p^2-2$ nie jest liczbą pierwszą.

3. $p=3k+2$ dla pewnego $k\in\mathbb{N}_0$. Wtedy $5p^2-2=5(9k^2+12k+$ $+4)-2=3(15k^2+20k+6)$, więc $5p^2-2$ jest liczbą złożoną.

Wobec tego liczby p i $5p^2-2$ są liczbami pierwszymi wtedy i tylko wtedy, gdy $p=3$. Wówczas $5p^2-4=41$ i $5p^2+2=47$ są liczbami pierwszymi, co kończy dowód.

Zadanie 22.134. Dla $n,x,y\in\mathbb{N}$ mamy, że:

$$\frac{1}{x}-\frac{1}{y}=\frac{1}{n}\iff ny-nx=xy\iff (y+n)(n-x)=n^2.$$

Załóżmy, że n jest liczbą pierwszą. Wtedy $D_n=\{1,n,n^2\}$ i $n+y|n^2$ oraz $n+y>n$, więc $n+y=n^2$ i $n-x=1$, skąd $y=n^2-n$ i $x=n-1$. Wobec tego w tym przypadku równanie $\frac{1}{x}-\frac{1}{y}=\frac{1}{n}$ posiada dokładnie jedno rozwiązanie w liczbach naturalnych x i y: $x=n-1$ i $y=n^2-n$.

Na odwrót, załóżmy, że równanie $\frac{1}{x}-\frac{1}{y}=\frac{1}{n}$ posiada dokładnie jedno rozwiązanie w liczbach naturalnych x i y. Jeśli $n=1$, to $(y+1)(1-x)=$

$= 1$, skąd $y + 1 = 1$ i $y = 0$, co prowadzi do sprzeczności. Zatem $n > 1$. Załóżmy, że n nie jest liczbą pierwszą. Wtedy istnieją liczby naturalne $a, b > 1$ takie, że $ab = n$. Stąd $a, b < n$. Stąd $l = ab - a > 0$ i $k = b - 1 > 0$, czyli $k, l \in \mathbb{N}$ oraz $(bl + ab)(ab - ak) = ab^2a = n^2$, skąd $x_1 = ak$ i $y_1 = bl$ są liczbami naturalnymi i $\frac{1}{x_1} - \frac{1}{y_1} = \frac{1}{n}$, ale $x_1 = ab - a = n - a < n - 1$, więc równanie $\frac{1}{x} - \frac{1}{y} = \frac{1}{n}$ posiada co najmniej dwa rozwiązania w liczbach naturalnych x i y (drugim rozwiązaniem jest $x = n - 1$, $y = n^2 - n$), co prowadzi do sprzeczności. Wobec tego n jest liczbą pierwszą.

Zadanie 22.135. Niech x, y, z będą liczbami pierwszymi takimi, że $2x - y = 1$ i $2x - z = -1$. Wtedy $y = 2x - 1$ i $z = 2x + 1$, czyli liczby $x, 2x - 1$ i $2x + 1$ są liczbami pierwszymi. Z twierdzenia o dzieleniu z resztą wynika, że możliwe są teraz tylko 3 przypadki: 1) $3 \mid x$, 2) $x = 3k + 1$ dla pewnego $k \in \mathbb{N}$, 3) $x = 3k + 2$ dla pewnego $k \in \mathbb{N}_0$.

W przypadku 1), $x = 3$, więc $y = 6 - 1 = 5$ i $z = 6 + 1 = 7$.

W przypadku 2), $2x + 1 = 6k + 2 + 1 = 3(2k + 1)$ i $2k + 1 > 1$, bo $k \geqslant 1$, więc mamy sprzeczność z pierwszością liczby $2x + 1$.

W przypadku 3), $2x - 1 = 6k + 4 - 1 = 3(2k + 1)$ i z pierwszości $2x - 1$ jest $2x - 1 = 3$, skąd $x = 2$ i $2x + 1 = 5$.

Podsumowując, $x = 3$, $y = 5$ i $z = 7$ lub $x = 2$, $y = 3$ i $z = 5$.

Zadanie 22.136. Ponieważ różnica liczb $11p$ i $5q$ jest nieparzysta, więc te liczby są różnej parzystości. Jeśli liczba $11p$ jest parzysta, to liczba pierwsza p jest parzysta, skąd $p = 2$ i $5q = 22 - 7 = 15$ oraz $q = 3$. Jeśli zaś liczba $5q$ jest parzysta, to liczba pierwsza q jest parzysta, czyli $q = 2$ i $11p = 10 + 7 = 17$, co prowadzi do sprzeczności.

Wobec tego: $p = 2$ i $q = 3$.

Zadanie 22.137. Zauważmy, że $1 \in S$, bo $1 = 4 \cdot 0 + 1$. Ponadto $st \in S$ dla dowolnych $s, t \in S$, gdyż $s = 4k + 1$ i $t = 4l + 1$ dla pewnych $k, l \in \mathbb{N}_0$, więc $st = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1$ i $4kl + k + l \in \mathbb{N}_0$.

Jeżeli $a, b \in \mathbb{N}$ i $[a]_4 = [b]_4 = 3$, to $[ab]_4 = 1$, bo $a = 4k + 3$ i $b = 4l + 3$ dla pewnych $k, l \in \mathbb{N}_0$, skąd $ab = 16kl + 12k + 12l + 9 =$

$= 4(4kl + 3k + 3l + 2) + 1$ i $4kl + 3k + 3l + 2 \in \mathbb{N}_0$. Zatem, jeśli $[a]_4 = [b]_4 = 3$ i $a, b \in \mathbb{N}$, to $ab \in S$.

Pokażemy, że $s \in S$ jest liczbą „pierwszą w S"wtedy i tylko wtedy, gdy s jest liczbą pierwszą lub s jest iloczynem dwóch liczb pierwszych dających resztę 3 z dzielenia przez 4. Jeżeli s jest liczbą pierwszą i $[s]_4 = 1$, to $s \in S$ i $s > 1$ oraz s nie jest iloczynem dwóch liczb naturalnych większych od 1, czyli s jest liczbą „pierwszą w S". Załóżmy, że $s = p^2$ lub $s = pq$, gdzie p i q są różnymi liczbami pierwszymi takimi, że $[p]_4 = [q]_4 = 3$, wtedy jak wiemy $s \in S$ i $s > 1$. Ponadto $D_{p^2} = \{1, p, p^2\}$ i $D_{pq} = \{1, p, q, pq\}$, więc s jest liczbą „pierwszą w S". Na odwrót, niech $s \in S$ będzie liczbą „pierwszą w S". Wtedy $s > 1$ i s jest nieparzyste. Załóżmy, że s ma dzielnik pierwszy p taki, że $[p]_4 = 1$. Wtedy $s = p \cdot t$ dla pewnego $t \in \mathbb{N}$, ale $[s]_4 = [p]_4 = 1$, więc też $[t]_4 = 1$, skąd $t \in S$ i z „pierwszości w S"liczby s mamy, że $t = 1$ i $s = p$. Niech dalej s nie posiada dzielnika pierwszego dającego resztę 1 z dzielenia przez 4. Wtedy istnieje liczba pierwsza q taka, że $q \mid s$ i $[q]_4 = 3$. Zatem $s = qt$ dla pewnego $t \in \mathbb{N}$, przy czym $[t]_4 = 3$, więc $t > 1$ i liczba t posiada dzielnik pierwszy r, przy czym $r \mid s$, więc $[r]_4 = 3$. Stąd $s = (qr) \cdot u$ dla pewnego $u \in \mathbb{N}$, skąd $[u]_4 = 1$, czyli $u \in S$ i z „pierwszości s w S"mamy, że $u = 1$, więc $s = qr$.

Z katalogu liczb pierwszych podanego w zadaniu 22.29 wynika, że liczbami „pierwszymi w S", które są liczbami pierwszymi $\leqslant 101$ są jedynie liczby: 5, 13, 17, 29, 37, 41, 53, 61, 73, 89 i 101. Natomiast liczby „pierwsze w S", które są iloczynami dwóch liczb pierwszych dających resztę 3 z dzielenia przez 4, to jedynie: $3^2 = 9$, $7^2 = 49$, $3 \cdot 7 = 21$, $3 \cdot 11 = 33$, $3 \cdot 19 = 57$, $3 \cdot 23 = 69$, $3 \cdot 31 = 93$, $7 \cdot 11 = 77$.

Zauważmy, że $441 = 9 \cdot 49 = 21 \cdot 21$, a to oznacza, że liczba 441 nie posiada jednoznacznego rozkładu na iloczyn liczb „pierwszych w S".

Przypuśćmy, że pewna liczba $s > 1$ należąca do S nie jest iloczynem liczb „pierwszych w S". Wtedy z zasady minimum istnieje najmniejsza liczba s_0 o tej własności. Oczywiście $s_0 > 1$ i s_0 nie jest „pierwsza w S". Zatem $s_0 = a \cdot b$ dla pewnych $a, b \in S$ takich, że $a, b > 1$. Stąd $a, b < s_0$, więc z minimalności s_0 zarówno a jak i b są iloczynami liczb „pierwszych w S", skąd $s_0 = ab$ też jest takim iloczynem

i mamy sprzeczność. Wobec tego każda liczba $s > 1$ należąca do S jest iloczynem liczb „pierwszych w S".

Uwaga. Powyższy przykład został po raz pierwszy odkryty przez Dawida Hilberta - wielkiego matematyka niemieckiego. Pokazuje on, że przy dowodzeniu twierdzenia o jednoznaczności rozkładu nie wystarczy ograniczać się tylko do mnożenia, lecz musimy korzystać też z innych działań na liczbach naturalnych (na przykład dodawania).

Zadanie 22.138. Niech $a = 4$ i $b = 2$ oraz $n = 1$, $m = 5$, $k = 2$ i $l = 3$. Wtedy $a \neq b$, $n \neq k$ i $m \neq l$, ale $a^n \cdot b^m = 2^7$ i $a^k \cdot b^l = 2^7$, czyli $a^n \cdot b^m = a^k \cdot b^l$.

Zadanie 22.139. Oznaczmy $d = \mathrm{NWD}(a, b)$. Wtedy $a = dx$ i $b = dy$ dla pewnych $x, y \in \mathbb{N}$ oraz $\mathrm{NWW}(a, b) = dxy$. Należy zatem pokazać, że $d + dxy \geqslant dx + dy$, co jest równoważne nierówności $1 + xy \geqslant x + y$, ale $1 + xy - (x + y) = (x - 1)(y - 1) \geqslant 0$, bo $x, y \geqslant 1$, więc nasza nierówność została wykazana. Ponadto równość zachodzi wtedy i tylko wtedy, gdy $x = 1$ lub $y = 1$, a więc gdy $a \mid b$ lub $b \mid a$.

Zadanie 22.140. Niech $x, y \in \mathbb{N}$ będą takie, że $\mathrm{NWD}(x, y) = 15$. Wtedy $x = 15a$ i $y = 15b$ dla pewnych $a, b \in \mathbb{N}$, przy czym na mocy twierdzenia 8.32, $\mathrm{NWD}(a, b) = 1$. Na odwrót, niech $a, b \in \mathbb{N}$ będą względnie pierwsze i niech $x = 15a$ i $y = 15b$. Wtedy z twierdzenia 8.46, $\mathrm{NWD}(x, y) = \mathrm{NWD}(15a, 15b) = 15 \cdot \mathrm{NWD}(a, b) = 15 \cdot 1 = 15$. Ponadto wówczas na mocy twierdzenia 8.44, $\mathrm{NWW}(x, y) = \frac{xy}{15} = \frac{15a \cdot 15b}{15} = 15ab$. W takim razie zadanie sprowadza się do znalezienia wszystkich względnie pierwszych liczb naturalnych a i b takich, że $15ab = 24360$, czyli $ab = 1624$, ale $1624 = 2^3 \cdot 203 = 2^3 \cdot 7 \cdot 29$, więc na parę (a, b) mamy dokładnie 8 możliwości: $(1, 1624), (1624, 1), (8, 203), (203, 8), (7, 232), (232, 7), (29, 56), (56, 29)$ i ostatecznie (x, y) to: $(15, 24360), (24360, 15), (120, 3045), (3045, 120), (435, 840), (840, 435)$.

Zadanie 22.141. Bez zmniejszania ogólności możemy zakładać, że $a \leqslant b \leqslant c$. Ponieważ $a + b + c = 12$, więc $3a \leqslant 12$, skąd $a \leqslant 4$, czyli $a \in \{1, 2, 3, 4\}$.

1. Niech $a = 1$. Wtedy $b + c = 11$, więc (a, b, c) to: $(1, 1, 10), (1, 2, 9), (1, 3, 8), (1, 4, 7), (1, 5, 6)$ oraz $\mathrm{NWW}(1, 1, 10) = 10$, $\mathrm{NWW}(1, 2, 9) =$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$= 2 \cdot 9 = 18$, $\mathrm{NWW}(1,3,8) = 3 \cdot 8 = 24$, $\mathrm{NWW}(1,4,7) = 4 \cdot 7 = 28$, $\mathrm{NWW}(1,5,6) = 5 \cdot 6 = 30$.

2. Niech $a = 2$. Wtedy $b + c = 10$, więc (a,b,c) to: $(2,2,8)$, $(2,3,7)$, $(2,4,6)$, $(2,5,5)$ oraz $\mathrm{NWW}(2,2,8) = 8$, $\mathrm{NWW}(2,3,7) = 2 \cdot 3 \cdot 7 = 42$, $\mathrm{NWW}(2,4,6) = 12$, $\mathrm{NWW}(2,5,5) = 2 \cdot 5 = 10$.

3. Niech $a = 3$. Wtedy $b + c = 9$, więc $(a,b,c) \in \{(3,3,6),(3,4,5)\}$ oraz $\mathrm{NWW}(3,3,6) = 6$ i $\mathrm{NWW}(3,4,5) = 3 \cdot 4 \cdot 5 = 60$.

4. Niech $a = 4$. Wtedy $b+c = 8$, więc $b = c = 4$ i $\mathrm{NWW}(4,4,4) = 4$.

Ostatecznie więc zbiorem wszystkich wartości $\mathrm{NWW}(a,b,c)$ jest zbiór: $\{4,6,8,10,12,18,24,28,30,42,60\}$.

Zadanie 22.142. Bez zmniejszania ogólności możemy zakładać, że $a \leqslant b \leqslant c$, ale $a + b + c = 12$, więc $3a \leqslant 12$, skąd $a \leqslant 4$, więc $\mathrm{NWD}(a,b,c) \leqslant 4$. Ponadto $\mathrm{NWD}(a,b,c)$ jest dzielnikiem wspólnym liczb a,b,c, więc też dzieli ich sumę, czyli $\mathrm{NWD}(a,b,c) \mid 12$. Stąd $\mathrm{NWD}(a,b,c) \in \{1,2,3,4\}$, ale $\mathrm{NWD}(1,1,10) = 1$ i $1+1+10 = 12$, $\mathrm{NWD}(2,2,8) = 2$ i $2+2+2+8 = 12$, $\mathrm{NWD}(3,3,6) = 3$ i $3+3+6 = 12$ oraz $\mathrm{NWD}(4,4,4) = 4$ i $4+4+4 = 12$, więc zbiór wszystkich wartości $\mathrm{NWD}(a,b,c)$ jest równy $\{1,2,3,4\}$.

Zadanie 22.143. Niech $a = 10^{80} \cdot 6^{60} \cdot 15^{40}$. Wtedy $a = 2^{80} \cdot 5^{80} \cdot 2^{60} \cdot 3^{60} \cdot 3^{40} \cdot 5^{40} = 2^{140} \cdot 3^{100} \cdot 5^{120}$. Z twierdzenia 8.53 wynika, że $\sqrt[n]{a}$ jest liczbą wymierną wtedy i tylko wtedy, gdy a jest n-tą potęgą liczby naturalnej, a to zgodnie z twierdzeniem 9.27 zachodzi wtedy i tylko wtedy, gdy n jest wspólnym dzielnikiem liczb 140, 100 i 120. Ta ostatnia własność zgodnie z twierdzeniem 8.41 jest równoważne temu, że $n \mid \mathrm{NWD}(140,100,120)$. Z algorytmu Euklidesa: $\mathrm{NWD}(100,120,140) = \mathrm{NWD}(100,20,40) = \mathrm{NWD}(20,0,0) = 20$ i $D_{20} = \{1,2,4,5,10,20\}$, więc ostatecznie $n \in \{2,4,5,10,20\}$.

Zadanie 22.144. Istnieją różne liczby pierwsze $p_1, \ldots, p_s$ oraz nieujemne liczby całkowite $\alpha_i, \beta_i, \gamma_i$ dla $i = 1, \ldots, s$ takie, że

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}, \quad b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s} \text{ i } c = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}.$$

a). Korzystając z twierdzenia 9.30 mamy, że

$$\mathrm{NWW}(a,b) = p_1^{\max\{\beta_1,\gamma_1\}} \cdot \ldots \cdot p_s^{\max\{\beta_s,\gamma_s\}}.$$

Zatem znowu z tego twierdzenia

$$\mathrm{NWD}(a, \mathrm{NWW}(b,c)) = p_1^{\min\{\alpha_1, \max\{\beta_1,\gamma_1\}\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s, \max\{\beta_s,\gamma_s\}\}}.$$

Ponadto z twierdzenia 9.30:

$$\mathrm{NWD}(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s,\beta_s\}},$$

$$\mathrm{NWD}(a,c) = p_1^{\min\{\alpha_1,\gamma_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s,\gamma_s\}},$$

więc

$$\mathrm{NWW}(\mathrm{NWD}(a,b), \mathrm{NWD}(a,c)) =$$

$$= p_1^{\max\{\min\{\alpha_1,\beta_1\}, \min\{\alpha_1,\gamma_1\}\}} \cdot \ldots \cdot p_s^{\max\{\min\{\alpha_s,\beta_s\}, \min\{\alpha_s,\gamma_s\}\}}.$$

Wystarczy zatem wykazać, że dla dowolnych $x, y, z \in \mathbb{N}_0$ zachodzi wzór:

$$\min\{x, \max\{y,z\}\} = \max\{\min\{x,y\}, \min\{x,z\}\}. \tag{23.1}$$

Możliwe są tylko następujące przypadki: (1) $x \leqslant y \leqslant z$, (2) $x \leqslant z \leqslant y$, (3) $y \leqslant x \leqslant z$, (4) $y \leqslant z \leqslant x$, (5) $z \leqslant x \leqslant y$, (6) $z \leqslant y \leqslant x$.

W przypadku (1):
$\min\{x, \max\{y,z\}\} = \min\{x,z\} = x$ i $\max\{\min\{x,y\}, \min\{x,z\}\} = \max\{x,x\} = x$, więc wzór (23.1) jest wtedy spełniony.

W przypadku (2):
$\min\{x, \max\{y,z\}\} = \min\{x,y\} = x$ i $\max\{\min\{x,y\}, \min\{x,z\}\} = \max\{x,x\} = x$, więc wzór (2.1) jest wtedy spełniony.

W przypadku (3):
$\min\{x, \max\{y,z\}\} = \min\{x,z\} = x$ i $\max\{\min\{x,y\}, \min\{x,z\}\} = \max\{y,x\} = x$, więc wzór (2.1) jest wtedy spełniony.

W przypadku (4):
$\min\{x, \max\{y,z\}\} = \min\{x,z\} = z$ i $\max\{\min\{x,y\}, \min\{x,z\}\} = \max\{y,z\} = z$, więc wzór (2.1) jest wtedy spełniony.

W przypadku (5):
$\min\{x, \max\{y,z\}\} = \min\{x,y\} = x$ i $\max\{\min\{x,y\}, \min\{x,z\}\} = \max\{x,z\} = x$, więc wzór (2.1) jest wtedy spełniony.

W przypadku (6):
$\min\{x, \max\{y, z\}\} = \min\{x, y\} = y$ i $\max\{\min\{x, y\}, \min\{x, z\}\} = \max\{y, z\} = y$, więc wzór (2.1) jest wtedy spełniony.

Kończy to dowód a).

b). Korzystając z twierdzenia 9.30 mamy, że

$$\mathrm{NWD}(a, b) = p_1^{\min\{\beta_1, \gamma_1\}} \cdot \ldots \cdot p_s^{\min\{\beta_s, \gamma_s\}}.$$

Zatem znowu z tego twierdzenia

$$\mathrm{NWW}(a, \mathrm{NWD}(b, c)) = p_1^{\max\{\alpha_1, \min\{\beta_1, \gamma_1\}\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s, \min\{\beta_s, \gamma_s\}\}}.$$

Ponadto z twierdzenia 9.30:

$$\mathrm{NWW}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s, \beta_s\}},$$

$$\mathrm{NWW}(a, c) = p_1^{\max\{\alpha_1, \gamma_1\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s, \gamma_s\}},$$

więc

$$\mathrm{NWD}(\mathrm{NWW}(a, b), \mathrm{NWW}(a, c)) =$$
$$= p_1^{\min\{\max\{\alpha_1, \beta_1\}, \max\{\alpha_1, \gamma_1\}\}} \cdot \ldots p_s^{\min\{\max\{\alpha_s, \beta_s\}, \max\{\alpha_s, \gamma_s\}\}}.$$

Wystarczy zatem wykazać, że dla dowolnych $x, y, z \in \mathbb{N}_0$ zachodzi wzór:

$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\}. \tag{23.2}$$

Możliwe są tylko następujące przypadki: (1) $x \leqslant y \leqslant z$, (2) $x \leqslant z \leqslant y$, (3) $y \leqslant x \leqslant z$, (4) $y \leqslant z \leqslant x$, (5) $z \leqslant x \leqslant y$, (6) $z \leqslant y \leqslant x$.

W przypadku (1):
$\max\{x, \min\{y, z\}\} = \max\{x, y\} = y$ i $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, z\} = y$, więc wzór (23.2) jest wtedy spełniony.

W przypadku (2):
$\max\{x, \min\{y, z\}\} = \max\{x, z\} = z$ i $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, z\} = z$, więc wzór (23.2) jest wtedy spełniony.

W przypadku (3):
$\max\{x, \min\{y, z\}\} = \max\{x, y\} = x$ i $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{x, z\} = x$, więc wzór (23.2) jest wtedy spełniony.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

W przypadku (4):
$\max\{x, \min\{y, z\}\} = \max\{x, y\} = x$ i $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{x, x\} = x$, więc wzór (23.2) jest wtedy spełniony.

W przypadku (5):
$\max\{x, \min\{y, z\}\} = \max\{x, z\} = x$ i $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, x\} = x$, więc wzór (23.2) jest wtedy spełniony.

W przypadku (6):
$\max\{x, \min\{y, z\}\} = \max\{x, z\} = x$ i $\min\{\max\{x, y\}, \max\{x, z\}\} = \min\{x, x\} = x$, więc wzór (23.2) jest wtedy spełniony.

Kończy to dowód b).

c). Na mocy twierdzenia 9.32 mamy, że:
$\mathrm{NWD}(a, b, c) = p_1^{\min\{\alpha_1, \beta_1, \gamma_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s, \beta_s, \gamma_s\}}$ oraz $\mathrm{NWW}(a, b, c) = p_1^{\max\{\alpha_1, \beta_1, \gamma_1\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s, \beta_s, \gamma_s\}}$. Wobec tego:

$$\mathrm{NWD}(a, b, c) \cdot \mathrm{NWW}(a, b, c) =$$

$$= p_1^{\min\{\alpha_1, \beta_1, \gamma_1\} + \max\{\alpha_1, \beta_1, \gamma_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s, \beta_s, \gamma_s\} + \max\{\alpha_s, \beta_s, \gamma_s\}}.$$

Ponadto:
$abc = p_1^{\alpha_1 + \beta_1 + \gamma_1} \cdot \ldots \cdot p_s^{\alpha_s + \beta_s + \gamma_s}$. Wystarczy zatem wykazać, że dla dowolnych $x, y, z \in \mathbb{N}_0$ zachodzi nierówność:

$$\min\{x, y, z\} + \max\{x, y, z\} \leqslant x + y + z. \tag{23.3}$$

Ze względu na symetrię wzoru (23.3) możemy bez zmniejszania ogólności zakładać, że $x \leqslant y \leqslant z$. Wtedy lewa strona wzoru (23.3) jest równa $x + z \leqslant x + y + z$, bo $y \geqslant 0$. Kończy to dowód c).

Zadanie 22.145. a). Załóżmy, że $\mathrm{NWD}(x, y) = \mathrm{NWW}(x, y)$. Ponieważ $x \mid \mathrm{NWW}(x, y)$, więc stąd $x \mid \mathrm{NWD}(x, y)$. Dalej, $\mathrm{NWD}(x, y) \mid x$, więc $x = \mathrm{NWD}(x, y)$. Podobnie dowodzimy, że $y = \mathrm{NWD}(x, y)$. Wobec tego $x = y$. Na odwrót, jeśli $x = y$, to $\mathrm{NWD}(x, y) = \mathrm{NWW}(x, y) = x$.

Wobec tego: $x = y$.

b). Załóżmy, że $\mathrm{NWD}(x, y) = xy$. Ponieważ zawsze $\mathrm{NWD}(x, y) \mid x$, więc $xy \mid x$, skąd $y \mid 1$, czyli $y = 1$. Podobnie pokazujemy, że $x = 1$. Ponadto $\mathrm{NWD}(1, 1) = 1 = 1 \cdot 1$.

Wobec tego $x = y = 1$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

c). Załóżmy, że $\mathrm{NWD}(x,y) = x+y$. Ponieważ zawsze $\mathrm{NWD}(x,y) \leqslant x$, więc $x+y \leqslant x$, skąd $y \leqslant 0$ i mamy sprzeczność.

Wobec tego takie x i y nie istnieją.

d). Załóżmy, że $\mathrm{NWD}(x,y) = x-y$. Wtedy istnieją $a, b \in \mathbb{N}$ takie, że $x = (x-y)a$ i $y = (x-y)b$ oraz $\mathrm{NWD}(a,b) = 1$. Stąd $x - y = (x-y)a - (x-y)b = (x-y)(a-b)$, a zatem $a - b = 1$, czyli $a = b+1$. Oznaczmy $t = x - y$. Wtedy $t \in \mathbb{N}$ i $x = t(b+1)$ i $y = tb$.

Na odwrót, niech $t, b \in \mathbb{N}$ i $x = t(b+1)$ i $y = tb$. Wtedy z twierdzenia 8.46, $\mathrm{NWD}(x,y) = t \cdot \mathrm{NWD}(b+1, b) = t \cdot \mathrm{NWD}(b,1) = t \cdot 1 = t$ oraz $x - y = tb + t - tb = t$.

Wobec tego $x = t(b+1)$ i $y = tb$, gdzie $t, b \in \mathbb{N}$.

e). Załóżmy, że $\mathrm{NWD}(x,y) = \frac{x}{y}$. Wtedy $y \mid x$, więc $x = ty$ dla pewnego $t \in \mathbb{N}$. Stąd $\mathrm{NWD}(x,y) = \mathrm{NWD}(ty, y) = y$, a zatem $y = \frac{x}{y}$, czyli $y = t$ oraz $x = t^2$.

Na odwrót, niech $t \in \mathbb{N}$ oraz $x = t^2$ i $y = t$. Wtedy $\frac{x}{y} = t$ i $t \mid t^2$, więc $\mathrm{NWD}(x,y) = t = \frac{x}{y}$.

Wobec tego $x = t^2$ i $y = t$ dla pewnego $t \in \mathbb{N}$.

f). Załóżmy, że $\mathrm{NWW}(x,y) = xy$. Wtedy z twierdzenia 8.44, $\mathrm{NWD}(x,y) = \frac{xy}{xy} = 1$. Jeśli zaś $\mathrm{NWD}(x,y) = 1$, to z twierdzenia 8.44, $\mathrm{NWW}(x,y) = xy$.

Wobec tego x i y są dowolnymi liczbami względnie pierwszymi.

g). Załóżmy, że $\mathrm{NWW}(x,y) = x+y$. Ponieważ zawsze $x|\mathrm{NWW}(x,y)$ i $y|\mathrm{NWW}(x,y)$, więc $x|x+y$ i $y|x+y$, skąd $x|y$ i $y|x$, więc $x = y$. Stąd $\mathrm{NWW}(x,y) = \mathrm{NWW}(x,x) = x < 2x = x+y$.

Wobec tego takie liczby x i y nie istnieją.

h). Niech $\mathrm{NWW}(x,y) = x-y$. Ponieważ zawsze $x \mid \mathrm{NWW}(x,y)$, więc $x \leqslant \mathrm{NWW}(x,y)$, skąd $x \leqslant x-y$ i mamy sprzeczność.

Wobec tego takie liczby x i y nie istnieją.

i). Załóżmy, że $\mathrm{NWW}(x,y) = \frac{x}{y}$. Wtedy $y \mid x$, więc $\mathrm{NWW}(x,y) = x$, skąd $x = \frac{x}{y}$, czyli $y = 1$. Na odwrót, dla $x \in \mathbb{N}$: $\mathrm{NWW}(x,1) = x = \frac{x}{1}$.

Wobec tego $y = 1$ i x jest dowolną liczbą naturalną.

j). Niech $\mathrm{NWW}(x,y) = x$. Ponieważ zawsze $y \mid \mathrm{NWW}(x,y)$, więc $y \mid x$. Na odwrót, jeśli $y \mid x$, to $\mathrm{NWW}(x,y) = x$.

Wobec tego $x = yt$, gdzie $t, y \in \mathbb{N}$.

k). Załóżmy, że $\mathrm{NWD}(x, y) = x$. Ponieważ zawsze $\mathrm{NWD}(x, y) \mid y$, więc $x \mid y$. Na odwrót, jeśli $x \mid y$, to $\mathrm{NWD}(x, y) = x$.

Wobec tego $y = xt$ i $x, t \in \mathbb{N}$.

Zadanie 22.146. a). Niech $x, y \in \mathbb{N}$. Jeśli $\mathrm{NWD}(x, y) = 30$, to istnieją $a, b \in \mathbb{N}$ takie, że $x = 30a$ i $y = 30b$, przy czym na mocy twierdzenia 8.32, $\mathrm{NWD}(a, b) = 1$. Na odwrót, niech $a, b \in \mathbb{N}$ będą takie, że $\mathrm{NWD}(a, b) = 1$. Wtedy na mocy twierdzenia 8.46, $\mathrm{NWD}(30a, 30b) = 30 \cdot \mathrm{NWD}(a, b) = 30 \cdot 1 = 30$. W takim razie $x = 30a$ i $y = 30b$, gdzie $a, b \in \mathbb{N}$ i $\mathrm{NWD}(a, b) = 1$ oraz $30a + 30b = 180$, czyli $a + b = 6$, skąd wobec warunku $\mathrm{NWD}(a, b) = 1$: $a = 1$ i $b = 5$ lub $a = 5$ i $b = 1$ oraz $x = 30$ i $y = 150$ lub $x = 150$ i $y = 30$.

b). Podobnie jak w punkcie a) dowodzimy, że $x = 45a$ i $y = 45b$ dla pewnych względnie pierwszych $a, b \in \mathbb{N}$, ale $7x = 11y$, więc $7 \cdot 45a = 11 \cdot 45b$, czyli $7a = 11b$. Z zasadniczego twierdzenia arytmetyki $7 \mid b$, więc $b = 7t$ dla pewnego $t \in \mathbb{N}$ i $7a = 11 \cdot 7t$, czyli $a = 11t$. Z twierdzenia 8.46, $\mathrm{NWD}(11t, 7t) = t \cdot \mathrm{NWD}(11, 7) = t \cdot 1 = t$, więc $t = 1$ i $a = 11$, $b = 7$ oraz $x = 495$ oraz $y = 315$.

c). Podobnie jak w punkcie a) dowodzimy, że $x = 4a$ i $y = 4b$ dla pewnych względnie pierwszych $a, b \in \mathbb{N}$. Stąd $4a \cdot 4b = 720$, czyli $ab = 45$. Ponadto $45 = 3^2 \cdot 5$ i $\mathrm{NWD}(a, b) = 1$, więc $a = 1$ i $b = 45$ lub $a = 9$ i $b = 5$ lub $a = 5$ i $b = 9$ lub $a = 45$ i $b = 1$ oraz $x = 4$ i $y = 180$ lub $x = 180$ i $y = 4$ lub $x = 36$ i $y = 20$ lub $x = 20$ i $y = 36$.

d). Podobnie jak w punkcie a) dowodzimy, że $x = 15a$ i $y = 15b$ dla pewnych względnie pierwszych $a, b \in \mathbb{N}$. Z twierdzenia 8.44, $\mathrm{NWW}(x, y) = 15ab$, więc $15ab = 420$, czyli $ab = 28$, ale $28 = 2^2 \cdot 7$ i $\mathrm{NWD}(a, b) = 1$, więc $a = 1$ i $b = 28$ lub $a = 28$ i $b = 1$ lub $a = 4$ i $b = 7$ lub $a = 7$ i $b = 4$. Stąd $x = 15$ i $b = 420$ lub $a = 420$ i $b = 15$ lub $a = 60$ i $b = 105$ lub $a = 105$ i $b = 60$.

e). Niech $x, y \in \mathbb{N}$. Załóżmy, że $x + y = 667$ i $\mathrm{NWW}(x, y) = 120 \cdot \mathrm{NWD}(x, y)$. Ponieważ $\mathrm{NWD}(x, y) \mid x$ i $\mathrm{NWD}(x, y) \mid y$, więc $\mathrm{NWD}(x, y) \mid x + y$, czyli $\mathrm{NWD}(x, y) \mid 667$, ale $667 = 23 \cdot 29$, więc $\mathrm{NWD}(x, y) \in \{1, 23, 29, 667\}$. Jeśli $\mathrm{NWD}(x, y) = 667$, to $x = 667a$ i $y = 667b$ dla pewnych $a, b \in \mathbb{N}$ takich, że $\mathrm{NWD}(a, b) = 1$, więc

$667a + 667b = 667$, skąd $a + b = 1$ i mamy sprzeczność, bo $a + b \geqslant 2$, gdyż $a, b \geqslant 1$.

Załóżmy, że $\mathrm{NWD}(x, y) = 1$. Wtedy $\mathrm{NWW}(x, y) = 120$ i $120 = 2^3 \cdot 3 \cdot 5$, więc $x = 1$ i $y = 120$ lub $x = 120$ i $y = 1$ lub $x = 8$ i $y = 15$ lub $x = 15$ i $y = 8$ lub $x = 3$ i $y = 40$ lub $x = 40$ i $y = 3$ lub $x = 5$ i $y = 24$ lub $x = 24$ i $y = 5$, ale w żadnym przypadku nie mamy spełnionego warunku $x + y = 667$, więc ten przypadek też nie może zajść.

Załóżmy, że $\mathrm{NWD}(x, y) = 23$. Wtedy podobnie jak w a) istnieją względnie pierwsze liczby naturalne a i b takie, że $x = 23a$ i $y = 23b$. Wtedy z twierdzenia 8.44, $\mathrm{NWW}(x, y) = 23ab$, więc $23ab = 120 \cdot 23$, a zatem $ab = 120$ i $23a+23b = 667$, czyli $a+b = 29$, ale $\mathrm{NWD}(a, b) = 1$, więc $a = 1$ i $b = 120$ lub $a = 120$ i $b = 1$ lub $a = 8$ i $b = 15$ lub $a = 15$ i $b = 8$ lub $a = 3$ i $b = 40$ lub $a = 40$ i $b = 3$ lub $a = 5$ i $b = 24$ lub $a = 24$ i $b = 5$, skąd $x = 23 \cdot 5 = 115$ i $y = 23 \cdot 24 = 552$ lub $x = 552$ i $y = 115$. Proste sprawdzenie pokazuje, że takie x i y spełniają warunki zadania.

Załóżmy, że $\mathrm{NWD}(x, y) = 29$. Wtedy podobnie jak w a) istnieją względnie pierwsze liczby naturalne a i b takie, że $x = 29a$ i $y = 29b$. Wtedy z twierdzenia 8.44, $\mathrm{NWW}(x, y) = 29ab$, więc $29ab = 120 \cdot 29$, a zatem $ab = 120$ i $29a+29b = 667$, czyli $a+b = 23$, ale $\mathrm{NWD}(a, b) = 1$, więc $a = 1$ i $b = 120$ lub $a = 120$ i $b = 1$ lub $a = 8$ i $b = 15$ lub $a = 15$ i $b = 8$ lub $a = 3$ i $b = 40$ lub $a = 40$ i $b = 3$ lub $a = 5$ i $b = 24$ lub $a = 24$ i $b = 5$, skąd $x = 29 \cdot 8 = 232$ i $y = 29 \cdot 15 = 435$ lub $x = 435$ i $y = 232$. Proste sprawdzenie pokazuje, że takie x i y spełniają warunki zadania.

Wobec tego nasze zadanie posiada dokładnie cztery rozwiązania: $x = 23 \cdot 5 = 115$ i $y = 23 \cdot 24 = 552$ lub $x = 552$ i $y = 115$ lub $x = 23 \cdot 5 = 115$ i $y = 23 \cdot 24 = 552$ lub $x = 552$ i $y = 115$.

Zadanie 22.147. Wyznaczymy najpierw wszystkie liczby naturalne a takie, że $a = 2x^2 = 3y^3 = 5z^5$ dla pewnych liczb naturalnych x, y, z. Ponieważ $2 \mid a$ i $3 \mid a$ i $5 \mid a$, więc z twierdzenia o jednoznaczności rozkładu istnieją różne liczby pierwsze $p_1, \ldots, p_s$ większe od 5 i istnieją nieujemne liczby całkowite $\alpha, \beta, \gamma, \alpha_1, \ldots, \alpha_s$ takie, że $a = 2^{1+\alpha} \cdot 3^{1+\beta} \cdot 5^{1+\gamma} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$.

Stąd $x^2 = 2^{\alpha} \cdot 3^{1+\beta} \cdot 5^{1+\gamma} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, więc z twierdzenia 9.27 takie x istnieje wtedy i tylko wtedy, gdy $2 \mid \alpha$ i $2 \mid 1+\beta$ i $2 \mid 1+\gamma$ i $2 \mid \alpha_i$ dla każdego $i = 1, \ldots, s$.

Dalej, $y^3 = 2^{1+\alpha} \cdot 3^{\beta} \cdot 5^{1+\gamma} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, więc z twierdzenia 9.27 takie y istnieje wtedy i tylko wtedy, gdy $3 \mid 1+\alpha$ i $3 \mid \beta$ i $3 \mid 1+\gamma$ i $3 \mid \alpha_i$ dla każdego $i = 1, \ldots, s$.

Ponadto, $z^5 = 2^{1+\alpha} \cdot 3^{1+\beta} \cdot 5^{\gamma} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, więc z twierdzenia 9.27 takie z istnieje wtedy i tylko wtedy, gdy $5 \mid 1+\alpha$ i $5 \mid 1+\beta$ i $5 \mid \gamma$ i $5 \mid \alpha_i$ dla każdego $i = 1, \ldots, s$.

Ponieważ liczby $2, 3, 5$ są parami względnie pierwsze, więc z wniosku 8.51 takie x, y i z istnieją wtedy i tylko wtedy, gdy $2 \mid \alpha$ i $15 \mid 1+\alpha$ i $10 \mid 1+\beta$ i $3 \mid \beta$ i $6 \mid 1+\gamma$ i $5 \mid \gamma$ i $30 \mid \alpha_i$ dla każdego $i = 1, \ldots, s$. Te warunki są równoważne temu, że $\alpha = 30k + 14$, $\beta = 30l + 9$, $\gamma = 30t + 5$ oraz $\alpha_i = 30\beta_i$, gdzie $k, l, t \in \mathbb{N}_0$ oraz $\beta_i \in \mathbb{N}_0$ dla $i = 1, \ldots, s$. Oznaczmy $n = 2^k \cdot 3^l \cdot 5^t \cdot p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$. Wtedy $a = 2^{15} \cdot 3^{10} \cdot 5^6 \cdot n^{30}$ oraz $x = 2^7 \cdot 3^5 \cdot 5^3 \cdot n^{15}$, $y = 2^5 \cdot 3^3 \cdot 5^2 \cdot n^{10}$ i $z = 2^3 \cdot 3^2 \cdot 5 \cdot n^{10}$, przy czym n jest dowolną liczbą naturalną.

Zadanie 22.148. Niech $d_1, d_2, \ldots, d_s$ będą wszystkimi różnymi dzielnikami liczby n. Wtedy $\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_s}$ też są różnymi dzielnikami liczby n, a ponieważ ma ona dokładnie s dzielników, to

$$\{d_1, \ldots, d_s\} = \left\{\frac{n}{d_1}, \ldots, \frac{n}{d_s}\right\},$$

skąd $d_1 \cdot \ldots \cdot d_s = \frac{n}{d_1} \cdot \ldots \cdot \frac{n}{d_s}$. Wobec tego $(d_1 \cdot \ldots \cdot d_s)^2 = n^s$, czyli $d_1 \cdot \ldots \cdot d_s = \sqrt{n^s}$.

Zadanie 22.149. Niech $p_1, p_2, \ldots, p_n$ będą różnymi liczbami pierwszymi, niech $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ i niech $a_i = \frac{a}{p_i}$ dla $i = 1, 2, \ldots, n$. Wtedy $a_1, a_2, \ldots, a_n$ są liczbami naturalnymi, przy czym $p_i \nmid a_i$ dla $i = 1, 2, \ldots, n$. Wynika stąd, że nie istnieje liczba pierwsza będąca wspólnym dzielnikiem tych liczb. Zatem ze stwierdzenia 9.21 liczby $a_1, a_2, \ldots, a_n$ są względnie pierwsze. Natomiast dla każdego $i = 1, \ldots, n$ wszystkie liczby ze zbioru $\{a_1, a_2, \ldots, a_n\} \setminus \{a_i\}$ są podzielne przez p_i, więc nie tworzą liczb względnie pierwszych. Zatem każde $n-1$ liczb spośród liczb $a_1, a_2, \ldots, a_n$ nie są względnie pierwsze.

Zadanie 22.150. Ponieważ $\frac{n^3}{6}+\frac{n^2}{2}+\frac{n}{3}=\frac{n^3+3n^2+2n}{6}$, więc wystarczy wykazać, że $6 \mid n^3+3n^2+2n$ dla każdego $n \in \mathbb{N}$, ale $6=2\cdot 3$, więc z wniosku 8.51 wystarczy pokazać, że $2 \mid n^3+3n^2+2n$ i $3 \mid n^3+3n^2+2n$. Dalej, $n^3+3n^2+2n=n^3+n^2+2(n^2+n)=n\cdot n(n+1)+2(n^2+n)$ i z zadania 22.9, $2 \mid n(n+1)$, więc $2 \mid n^3+3n^2+2n$. Ponadto mamy, że $n^3+3n^2+2n=(n^3-n)+3(n^2+n)$ i z zadania 22.11, $3 \mid n^3-n$, więc $3 \mid n^3+3n^2+2n$. Kończy to nasz dowód.

Zadanie 22.151. Niech x będzie dodatnią liczbą rzeczywistą. Wtedy $x:\frac{35}{396}=k\in\mathbb{Z} \iff x=k\cdot\frac{35}{396}$, a zatem jeśli $x:\frac{35}{396}$ jest liczbą całkowitą, to x jest liczbą wymierną. Ze stwierdzenia 8.33, $x=\frac{a}{b}$, gdzie $a,b\in\mathbb{N}$ i $\mathrm{NWD}(a,b)=1$. Ponadto $\frac{a}{b}:\frac{35}{396}=\frac{396a}{35b}$ i $\frac{a}{b}:\frac{28}{297}=$ $=\frac{297a}{28b}$, więc z zasadniczego twierdzenia arytmetyki $\frac{a}{b}:\frac{35}{396}\in\mathbb{Z}$ wtedy i tylko wtedy, gdy $a \mid 35$ i $396 \mid b$ oraz $\frac{a}{b}:\frac{28}{297}\in\mathbb{Z} \iff [a \mid 28$ i $297 \mid b]$. W takim razie liczby $\frac{a}{b}:\frac{35}{396}$ i $\frac{a}{b}:\frac{28}{297}$ są całkowite wtedy i tylko wtedy, gdy $a \mid 35$ i $a \mid 28$ oraz $396 \mid b$ i $297 \mid b$. Ułamek $\frac{a}{b}$ jest największy, gdy a jest największe i gdy b jest najmniejsze, czyli gdy $a=\mathrm{NWD}(35,28)=7$ oraz $b=\mathrm{NWW}(396,297)=\mathrm{NWW}(2^2\cdot 3^2\cdot 11, 3^3\cdot 11)=2^2\cdot 3^3\cdot 11=1188$.

Wobec tego szukaną liczbą jest $\frac{7}{1188}$.

Zadanie 22.152. Niech x będzie niezerową liczbą rzeczywistą. Jeżeli $\frac{8}{15}:x=k$ dla pewnego $k\in\mathbb{Z}$, to $k\neq 0$ i $x=\frac{8}{15}:k$, skąd x jest liczbą wymierną. Każda dodatnia liczba wymierna jest większa od każdej ujemnej liczby wymiernej a my szukamy największego x takiego, że liczby $\frac{8}{15}:x$ i $\frac{18}{55}:x$ są wymierne, więc wystarczy ograniczyć się do dodatnich liczb wymiernych x. Z twierdzenia 8.32, $x=\frac{a}{b}$, gdzie $a,b\in\mathbb{N}$ i $\mathrm{NWD}(a,b)=1$. Ponadto $\frac{8}{15}:\frac{a}{b}=\frac{8b}{15a}\in\mathbb{Z} \iff 15a \mid 8b$ oraz $\frac{18}{55}:\frac{a}{b}=\frac{18b}{55a}\in\mathbb{Z} \iff 55a \mid 18b$. Z zasadniczego twierdzenia arytmetyki uzyskujemy, że $15a \mid 8b \iff [15 \mid b$ i $a \mid 8]$ oraz $55a \mid 18b$ wtedy i tylko wtedy, gdy $55 \mid b$ i $a \mid 18$. Z twierdzenia 8.36, $15 \mid b$ i $55 \mid b$ wtedy i tylko wtedy, gdy $\mathrm{NWW}(15,55) \mid b \iff 165 \mid b$. Ponadto z twierdzenia 8.41, $a \mid 8$ i $a \mid 18$ wtedy i tylko wtedy, gdy $a \mid \mathrm{NWD}(8,18) \iff a \mid 2$.

Ułamek $\frac{a}{b}$ jest największy, gdy a jest największe i gdy b jest najmniejsze, czyli wtedy i tylko wtedy, gdy $a=\mathrm{NWD}(8,18)=2$ i $b=$ $=\mathrm{NWW}(15,55)=165$. Zatem szukaną liczbą jest $\frac{2}{165}$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.153. Niech $S = 1^3 + 2^3 + \ldots + 1964^3$. Wtedy $2S = [1^3+1964^3]+[2^3+1963^3]+\ldots+[k^3+(1965-k)^3]+\ldots+[1964^3+1^3]$, ale dla $k = 1, \ldots, 1964$ jest, że $1965 = k + (1965 - k)$ i na mocy zadania 22.91, $k + (1965 - k) \mid k^3 + (1965 - k)^3$, więc $1965 \mid 2S$. Ponadto $\mathrm{NWD}(1965, 2) = 1$, więc z zasadniczego twierdzenia arytmetyki 1965 dzieli S, co należało wykazać.

Zadanie 22.154. Ponieważ $11, 31$ i 61 są różnymi liczbami pierwszymi, więc na mocy wniosku 3.33 wystarczy wykazać, że $11 \mid 20^{15} - 1$ i $31 \mid 20^{15} - 1$ i $61 \mid 20^{15} - 1$.

Z zasadniczego twierdzenia arytmetyki $61 \mid 20^{15} - 1 \iff 61 \mid 3^{15} \cdot (20^{15} - 1)$, ale $3^{15} \cdot (20^{15} - 1) = [60^{15} + 1] - [3^{15} + 1]$ oraz z zadania 22.91, $61 \mid [60^{15} + 1]$, bo $61 = 60 + 1$ i $3^5 + 1 = 244 = 4 \cdot 61$ oraz $3^{15} + 1 = (3^5)^3 + 1$, więc z zadania 22.91 i z przechodniości relacji podzielności, $61 \mid 3^{15} + 1$. Wobec tego $61 \mid 20^{15} - 1$.

Dalej, $20^{15} - 1 = 2^{30} \cdot 5^{15} - 1 = 5^{15} \cdot (2^{30} - 1) + (5^{15} - 1)$ oraz $31 = 2^5 - 1$ i z zadania 22.88, $2^5 - 1 \mid 2^{30} - 1$, więc $31 \mid 5^{15} \cdot (2^{30} - 1)$. Ponadto z zadania 22.88, $5^3 - 1 \mid 5^{15} - 1$ i $5^3 - 1 = 124 = 4 \cdot 31$, więc $31 \mid 5^{15} - 1$. Wobec tego $31 \mid 20^{15} - 1$.

W końcu, $20^{15}-1 = 2^{15}\cdot 10^{15}-1 = 2^{15}\cdot(10^{15}+1)-(2^{15}+1)$ i z zadania 22.91, $11 \mid 10^{15}+1$ oraz $2^5+1 \mid 2^{15}+1$, przy czym $2^5+1 = 33 = 3 \cdot 11$, więc $11 \mid 2^{15} + 1$. Wobec tego $11 \mid 20^{15} - 1$.

Zadanie 22.155. Ponieważ n jest liczbą naturalną i $n > 2$, więc n^2-4 jest liczbą naturalną. Załóżmy, że $\sqrt{n^2 - 4}$ jest liczbą wymierną. Wtedy z twierdzenia 8.53 istnieje liczba naturalna k taka, że $n^2 - 4 = k^2$, ale $n^2 - 4 < n^2$, więc $k^2 < n^2$, skąd $k < n$, a więc $k \leqslant n - 1$. Zatem $n^2 - 4 = k^2 \leqslant (n - 1)^2 = n^2 - 2n + 1$, skąd $-4 \leqslant -2n + 1$, czyli $2n \leqslant 5$. Lecz $n \geqslant 3$, więc $2n \geqslant 6$ i mamy sprzeczność. Wobec tego liczba $\sqrt{n^2 - 4}$ jest niewymierna.

Zadanie 22.156. Mamy, że $[2222]_7 = 3$, więc $7 \mid 2222-3$ i z zadania 22.88, $7 \mid 2222^{5555}-3^{5555}$, więc liczby 2222^{5555} i 3^{5555} dają te same reszty z dzielenia przez 7. Ponadto, $[5555]_7 = 4$, więc analogicznie, liczby 5555^{2222} i 4^{2222} dają te same reszty z dzielenia przez 7. Stąd $[2222^{5555} + 5555^{2222}]_7 = [3^{5555} + 4^{2222}]_7$, ale $7 = 2^3 - 1$ i $4^{2222} - 1 = 2^{4444} - 1$, więc z zadania 22.160, $[4^{2222} - 1]_7 = 2^{[4444]_3} - 1 = 2^1 - 1 = 1$, skąd

$[4^{2222}]_7 = 2$. Ponadto z małego twierdzenia Fermata $7 \mid 3^6 - 1$, więc z zadania 22.88, $7 \mid 3^{6n} - 1$ dla każdego $n \in \mathbb{N}$. Dalej, $5555 = 925 \cdot 6 + 5$, więc $3^{5555} - 1 = 3^5 \cdot 3^{925 \cdot 6} - 1 = 3^5 \cdot (3^{925 \cdot 6} - 1) + (3^5 - 1)$, skąd $[3^{5555} - 1]_7 = [3^5 - 1]_7 = [242]_7 = 4$ i w takim razie $[3^{5555}]_7 = 5$. Stąd $[3^{5555} + 4^{2222}]_7 = [5 + 2]_7 = 0$. Zatem ostatecznie uzyskaliśmy, że liczba $2222^{5555} + 5555^{2222}$ daje resztę 0 z dzielenia przez 7.

Zadanie 22.157. Zauważmy, że iloczyn dwóch liczb naturalnych, których cyfrą jedności jest 6 ma też cyfrę jedności równą 6. Stąd ostatnią cyfrą liczby 6^{1971} jest 6.

Zauważmy, że iloczyn dwóch liczb naturalnych, których cyfrą jedności jest 1 ma też cyfrę jedności równą 1, ale $9^{1971} = (9^2)^{985} \cdot 9 = 81^{985} \cdot 9$ i liczba 81^{985} ma cyfrę jedności równą 1, więc liczba $81^{985} \cdot 9$ ma cyfrę jedności równą 9, czyli ostatnią cyfrą liczby 9^{1971} jest 9.

Ponieważ $3^4 = 81$ i $3^{1971} = (3^4)^{492} \cdot 3^3 = 81^{492} \cdot 27$, więc ostatnią cyfrą liczby 81^{492} jest 1 i ostatnią cyfrą liczby $81^{492} \cdot 27$ jest 7. Zatem ostatnią cyfrą liczby 3^{1971} jest 7.

Mamy, że $2^4 = 16$ i $2^{1971} = (2^4)^{492} \cdot 2^3 = 16^{492} \cdot 8$ oraz liczba 16^{492} kończy się na 6, więc liczba $16^{492} \cdot 8$ kończy się na 8.

Zadanie 22.158. Ponieważ $10 = 2 \cdot 5$ i na mocy ćwiczenia 9.51 jest $\alpha_5(100!) \leqslant \alpha_2(100!)$ oraz na mocy twierdzenia 9.49 mamy, że $\alpha_5(100!) = \frac{100}{5} + \frac{100}{25} = 24$, więc liczba 100! kończy się 24-oma zerami.

Zadanie 22.159. Z zasadniczego twierdzenia arytmetyki wynika, że $34 \mid 15n - 8 \iff 34 \mid 9 \cdot (15n - 8)$, ale $9 \cdot (15n - 8) = 34(4n - 2) - +(n + 4)$, więc $34 \mid 15n - 8 \iff 34 \mid n + 4 \iff 34 \mid n - 30$. Wobec tego $n = 34t + 30$ dla pewnego $t \in \mathbb{Z}$, ale liczba n jest trzycyfrowa, więc $t \leqslant 28$.

Ponadto $[3n^2 + 3n + 2]_5 = 3 \iff 5 \mid 3n^2 + 3n + 2 - 3$, czyli $[3n^2 + 3n + 2]_5 = 3 \iff 5 \mid 3n^2 + 3n - 1$. Z zasadniczego twierdzenia arytmetyki wynika, że $5 \mid 3n^2 + 3n - 1 \iff 5 \mid 2 \cdot (3n^2 + 3n - 1)$, więc $5 \mid 3n^2 + 3n - 1 \iff 5 \mid (n^2 + n - 2) + 5(n^2 + n) \iff 5 \mid n^2 + n - 2$, ale $n^2 + n - 2 = (n - 1)(n + 2)$, więc $5 \mid n^2 + n - 2 \iff [5 \mid n - 1$ lub $5 \mid n + +2] \iff [5 \mid n - 1$ lub $5 \mid n - 3]$. Wobec tego $[3n^2 + 3n + 2]_5 = 3$ wtedy i tylko wtedy, gdy $[n]_5 = 1$ lub $[n]_5 = 3$.

Szukamy teraz największego trzycyfrowego n spełniającego znale-

zione warunki. Dla $t = 28$ mamy, że $n = 982$, więc $[n]_5 = [2]_5 = 2$. Dla $t = 27$ mamy, że $n = 948$, więc $[n]_5 = [8]_5 = 3$. Wobec tego szukane $n = 948$. Mamy: $948 = 2^2 \cdot 3 \cdot 79$ i 79 jest liczbą pierwszą, więc ze stwierdzenia 9.23, $\tau(948) = 3 \cdot 2 \cdot 2 = 12$, czyli szukana liczba n ma dokładnie 12 dzielników.

Zadanie 22.160. Z twierdzenia o dzieleniu z resztą $n = qm + r$ dla pewnych $q, r \in \mathbb{N}_0$ takich, że $r < m$. Stąd $a^n - 1 = a^r \cdot a^{qm} - 1 = a^r \cdot (a^{qm} - 1) + (a^r - 1)$, ale z zadania 22.88, $a^m - 1 \mid a^{qm} - 1$, czyli $a^{qm} - 1 = t \cdot (a^m - 1)$ dla pewnego $t \in \mathbb{Z}$. Wobec tego $a^n - 1 = (a^r t)(a^m - 1) + a^r - 1$, przy czym $0 \leqslant a^r - 1 < a^m - 1$, bo $a > 1$ oraz $0 \leqslant r < m$. Oznacza to, że $a^r - 1$ jest resztą z dzielenia liczby $a^n - 1$ przez liczbę $a^m - 1$.

Korzystając z algorytmu Euklidesa otrzymujemy zatem, że $\mathrm{NWD}(a^m - 1, a^n - 1) = \mathrm{NWD}(a^r - 1, a^m - 1)$. Kontynuując ten proces po skończonej liczbie kroków uzyskamy, że $\mathrm{NWD}(a^m - 1, a^n - 1) = \mathrm{NWD}(a^d - 1, a^0 - 1) = a^d - 1$, gdzie $d = \mathrm{NWD}(m, n)$.

Na mocy wniosku 8.3 liczba $a^m - 1$ dzieli liczbę $a^n - 1$ wtedy i tylko wtedy, gdy reszta z dzielenia $a^n - 1$ przez $a^m - 1$ jest równa 0, czyli wtedy i tylko wtedy, gdy $a^{[n]_m} - 1 = 0$, ale $a^{[n]_m} - 1 = 0 \iff a^{[n]_m} = 1 \iff [n]_m = 0 \iff m \mid n$, więc rzeczywiście, $a^m - 1 \mid a^n - 1$ wtedy i tylko wtedy, gdy $m \mid n$.

Zadanie 22.161. Ponieważ $69 = 3^2 \cdot 7$ i $91 = 7 \cdot 13$, więc mamy, że $\mathrm{NWD}(69, 91) = 7$. Stąd i z zadania 22.160: $\mathrm{NWD}(2^{63} - 1, 2^{91} - 1) = 2^7 - 1 = 127$.

Zadanie 22.162. Szukamy liczb naturalnych x i y takich, że $7x - 11y = 9$. Stąd $x > y$ oraz $7(x - y) - 4y = 9$. Oznaczmy $z = x - y$. Wtedy $z \in \mathbb{N}$ oraz $7z - 4y = 9$. Stąd $4(z - y) + 3z = 9$, więc można przyjąć $y = z = 3$. Stąd $x = z + y = 6$. Rzeczywiście: $7 \cdot 6 - 11 \cdot 3 = 9$.

Należy zatem najpierw odwracać 6 razy klepsydrę 7-mio minutową i 3 razy klepsydrę 11-to minutową. Czas, który upłynie po przesypaniu piasku w klepsydrze 11-to minutowej po jej trzecim odwróceniu do przesypania się piasku w odwracanej w tym czasie klepsydry 7-mio minutowej wynosi dokładnie 9 minut.

Zadanie 22.163. a). Oznaczmy $a = \mathrm{NWW}(n+1, n+2, \ldots, 2n)$ i $A = \mathrm{NWW}(1, 2, \ldots, 2n)$. Wtedy $k \mid A$ dla każdego $k = 1, \ldots, 2n$, więc A jest wspólną wielokrotnością liczb $n+1, \ldots, 2n$ i z twierdzenia 8.36, $a \mid A$, skąd $a \leqslant A$. Weźmy teraz dowolne $k \in \{1, \ldots, n\}$. Wtedy $n+k \leqslant 2n$, więc $n+1, n+2, \ldots, n+k$ tworzą k kolejnych liczb naturalnych i wszystkie występują wśród liczb $n+1, n+2, \ldots, 2n$, więc z zadania 22.51, $k \mid n+i$ dla pewnego $i = 1, \ldots, n$, ale $n+i \mid a$, więc z przechodniości relacji podzielności $k \mid a$. Ponadto każda z liczb $n+1, \ldots, 2n$ też dzieli a, więc a jest wspólną wielokrotnością liczb $1, 2, \ldots, 2n$ i z twierdzenia 8.36, $A \mid a$, skąd $A \leqslant a$. W ten sposób wykazaliśmy, że $a \leqslant A$ i $A \leqslant a$, więc $A = a$, czyli $\mathrm{NWW}(1, 2, \ldots, 2n) = \mathrm{NWW}(n+1, n+2, \ldots, 2n)$.

b). Przyjmijmy oznaczenia: $a = \mathrm{NWW}(n+1, n+2, \ldots, 2n+1)$ i $A = \mathrm{NWW}(1, 2, \ldots, 2n+1)$. Wtedy $k|A$ dla każdego $k = 1, \ldots, 2n+1$, więc A jest wspólną wielokrotnością liczb $n+1, \ldots, 2n+1$ i z twierdzenia 8.36, $a|A$, skąd $a \leqslant A$. Weźmy teraz dowolne $k \in \{1, \ldots, n\}$. Wtedy $n+k \leqslant 2n+1$, więc $n+1, n+2, \ldots, n+k$ tworzą k kolejnych liczb naturalnych i wszystkie występują wśród liczb $n+1, n+2, \ldots, 2n+1$, więc z zadania 22.51, $k \mid n+i$ dla pewnego $i = 1, \ldots, n$. Dalej, $n+i \mid a$, więc z przechodniości relacji podzielności $k \mid a$. Ponadto każda z liczb $n+1, \ldots, 2n+1$ też dzieli a, więc a jest wspólną wielokrotnością liczb $1, 2, \ldots, 2n+1$ i z twierdzenia 8.36, $A \mid a$, skąd $A \leqslant a$. W ten sposób wykazaliśmy, że $a \leqslant A$ i $A \leqslant a$, więc $A = a$, a to oznacza, że $\mathrm{NWW}(1, 2, \ldots, 2n+1) = \mathrm{NWW}(n+1, n+2, \ldots, 2n+1)$.

Zadanie 22.164. Oznaczmy przez a liczbę całkowitą, która przy dzieleniu przez 76 jak i przez 77 ma tę samą resztę równą 46. Wtedy $76 \mid a-46$ i $77 \mid a-46$. Ponadto 76 i 77 są względnie pierwsze jako kolejne liczby naturalne, więc z twierdzenia 8.44, $\mathrm{NWW}(76, 77) = 76 \cdot 77$. Stąd i z twierdzenia 8.36, $76 \cdot 77 \mid a-46$. Zatem $a-46 = 76 \cdot 77t$ dla pewnego $t \in \mathbb{Z}$. Wobec tego $a = 77 \cdot 76t + 46 = 14 \cdot (11 \cdot 38t + 3) + 4$, skąd $[a]_{14} = 2$, bo $11 \cdot 38t + 3 \in \mathbb{Z}$.

Zadanie 22.165. Niech x_i oznacza liczbę cięć i-tego rodzaju dla $i = 1, 2, 3, 4$. Wtedy $x_i \in \mathbb{N}_0$. Smok będzie zatem zabity wtedy i tylko wtedy, gdy istnieją nieujemne liczby całkowite x_1, x_2, x_3, x_4 takie, że

$-15x_1 + 21x_2 + 3x_3 - 348x_4 = 2000$, ale liczba $-15x_1 + 21x_2 + 3x_3 - +348x_4 = 3(-5x_1 + 7x_2 + x_3 - 116x_4)$ jest podzielna przez 3 i $[2000]_3 = = [2 + 0 + 0 + 0]_3 = 2 \neq 0$, więc otrzymujemy sprzeczność. Wobec tego rycerz nie może zabić tego smoka.

Zadanie 22.166. Niech x będzie liczbą dobrych odpowiedzi tej uczennicy, y-liczbą złych jej odpowiedzi i niech z będzie liczbą pytań, na które ta uczennica nie udzieliła odpowiedzi. Wtedy $x, y, z \in \mathbb{N}_0$ i $x + y + z = 60$. Ponadto $11x - 8y + 0 \cdot z = 24$, czyli $11x - 8y = 24$ oraz $x + y \leqslant 60$. Zatem $11x = 8(y + 3)$, skąd $8 \mid x$, więc $x = 8a$ dla pewnego $a \in \mathbb{N}_0$. Stąd $11 \cdot 8a = 8(y + 3)$, czyli $y = 11a - 3$. ale $y \geqslant 0$, więc $a \geqslant 1$. Dalej, $60 \geqslant x + y = 8a + (11a - 3) = 19a - 3$, skąd $19a \leqslant 63$ i $a \leqslant 3$. Zatem $a \in \{1, 2, 3\}$, skąd $x = 8, y = 8, z = 44$ lub $x = 16, y = 19, z = 25$ lub $x = 24, y = 30, z = 6$.

Zadanie 22.167. Ponieważ $7 = 2^3 - 1$, więc dla $n \in \mathbb{N}$ na mocy zadania 22.160 mamy, że $7 \mid 2^n - 1 \iff [n]_3 = 0$. Wobec tego $7 \mid 2^n - 1$ wtedy i tylko wtedy, gdy $n = 3k$ dla pewnego $k \in \mathbb{N}$.

Zadanie 22.168. Oznaczmy $\mathrm{NWD}(a, b) = d$. Wtedy $d \in \mathbb{N}$ i istnieją względnie pierwsze liczby naturalne x, y takie, że $a = dx$ i $b = dy$ oraz na mocy twierdzenia 8.44, $\mathrm{NWW}(a, b) = dxy$. Zatem $\mathrm{NWD}(a + b, \mathrm{NWW}(a, b)) = \mathrm{NWD}(d(x + y), dxy) = d \cdot \mathrm{NWD}(x + y, xy)$ na mocy twierdzenia 8.46. Z zadania 22.35, $\mathrm{NWD}(x + y, xy) = 1$, więc $\mathrm{NWD}(a + b, \mathrm{NWW}(a, b)) = d = \mathrm{NWD}(a, b)$.

Zadanie 22.169. Niech $m, n \in \mathbb{N}$. Jeżeli $m^5 n^9 = 2^{24} \cdot 3^{45} \cdot 5^{30}$ i liczba pierwsza p jest dzielnikiem liczby m lub liczby n, to $p | 2^{24} \cdot 3^{45} \cdot 5^{30}$, więc z własności liczb pierwszych, $p \in \{2, 3, 5\}$. Z twierdzenia o jednoznaczności rozkładu mamy zatem, że $m = 2^a \cdot 3^b \cdot 5^c$ i $n = 2^x \cdot 3^y \cdot 5^z$ dla pewnych $a, b, c, x, y, z \in \mathbb{N}_0$. Stąd mamy, że $m^5 n^9 = 2^{5a+9x} \cdot 3^{5b+9y} \cdot 5^{5c+9z}$ i z twierdzenia o jednoznaczności rozkładu:

$$m^5 n^9 = 2^{24} \cdot 3^{45} \cdot 5^{30} \iff [5a + 9x = 24 \text{ i } 5b + 9y = 45 \text{ i } 5c + 9z = 30].$$

Pozostaje zatem rozwiązać w nieujemnych liczbach całkowitych równania: $5a + 9x = 24$, $5b + 9y = 45$, $5c + 9z = 30$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

1). Znajdujemy wszystkie $a, x \in \mathbb{N}_0$ takie, że $5a + 9x = 24$. Zauważmy, że $9x \leqslant 5a + 9x$, więc $9x \leqslant 24$. Stąd $x = 0$ lub $x = 1$ lub $x = 2$. Dla $x = 0$ mamy, że $5a = 24$, co prowadzi do sprzeczności. Dla $x = 1$, $5a = 15$, skąd $a = 3$. Dla $x = 2$, $5a = 6$ i mamy sprzeczność. Zatem: $a = 3$ i $x = 1$.

2) Znajdujemy wszystkie $b, y \in \mathbb{N}_0$ takie, że $5b + 9y = 45$. Zauważmy, że $9 \mid 45 - 9y$, więc $9 \mid 5b$, skąd z zasadniczego twierdzenia arytmetyki $9 \mid b$, ale $5b \leqslant 45$, więc $b \leqslant 9$, skąd $b = 0$ lub $b = 9$. Jeśli $b = 0$, to $y = 5$. Jeśli $b = 9$, to $y = 0$. Mamy zatem dwa rozwiązania: $b = 0$ i $y = 5$ oraz $b = 9$ i $y = 0$.

3). Znajdujemy wszystkie $c, z \in \mathbb{N}_0$ takie, że $5c + 9z = 30$. Zauważmy, że $5 \mid 30 - 5c$, więc $5 \mid 9z$ i z zasadniczego twierdzenia arytmetyki, $5 \mid z$, ale $9z \leqslant 30$, więc $z \leqslant 3$ i wobec tego $z = 0$ oraz $c = 6$.

Wobec tego nasze zadanie posiada dokładnie dwa rozwiązania:
$m = 2^3 \cdot 3^0 \cdot 5^6$ i $n = 2^1 \cdot 3^5 \cdot 5^0$ oraz $m = 2^3 \cdot 3^9 \cdot 5^6$ i $n = 2^1 \cdot 3^0 \cdot 5^0$.

Zadanie 22.170. Takie liczby są postaci: $n, n+1, n+2, n+3, n+4, n+5, n+6, n+7, n+8, n+9$, gdzie $n \in \mathbb{N}$ i $n > 3$. Jeśli n jest parzyste, to liczby $n, n+2, n+4, n+6, n+8$ są parzyste i większe od 2, więc są to liczby złożone, zaś pozostałe 5 liczb: $n+1, n+3, n+5, n+7, n+9$ zawiera ciąg $n+1, (n+1)+2, (n+1)+4$, przy czym $[2]_3 = 2$ i $[4]_3 = 1$, więc z zadania 22.58 wśród liczb $n+1, n+3, n+5$ istnieje liczba podzielna przez 3, ale ta liczba jest większa od 3, więc jest ona liczbą złożoną. Zatem w tym przypadku wśród naszych dziesięciu liczb nie ma pięciu liczb pierwszych.

Jeśli zaś n jest nieparzyste, to liczby $n+1, n+3, n+5, n+7, n+9$ są parzyste i większe od 2, czyli są to liczby złożone. Natomiast wśród pozostałych pięciu liczb $n, n+2, n+4, n+6, n+8$ na mocy zadania 22.58 istnieje liczba podzielna przez 3, a ponieważ jest ona większa od 3, więc jest liczbą złożoną. Wobec tego w tym przypadku też wśród naszych dziesięciu liczb nie ma pięciu liczb pierwszych.

Wobec tego odpowiedź na postawione w zadaniu pytanie brzmi: Nie może.

Zadanie 22.171. Takie liczby są postaci: $n, n+1, n+2, n+3, n+4, n+5, n+6, n+7, n+8, n+9, n+10, n+11$, gdzie $n \in \mathbb{N}$

i $n > 3$. Jeśli n jest parzyste, to liczby $n, n+2, n+4, n+6, n+8, n+10$ są parzyste i większe od 2, więc są to liczby złożone, zaś pozostałe 6 liczb: $n+1, n+3, n+5, n+7, n+9, n+11$ zawierają ciągi $n+1$, $(n+1)+2, (n+1)+4$ i $n+7, (n+7)+2, (n+7)+4$, przy czym $[2]_3 = 2$ i $[4]_3 = 1$, więc z zadania 22.58 wśród liczb $n+1, n+3, n+5$ istnieje liczba podzielna przez 3 i wśród liczb $n+7, n+9, n+11$ istnieje liczba podzielna przez 3, ale te liczby są większe od 3, więc są one liczbami złożonymi. Zatem w tym przypadku wśród naszych dwunastu liczb nie ma pięciu liczb pierwszych.

Jeśli zaś n jest nieparzyste, to liczby $n+1, n+3, n+5, n+7$, $n+9, n+11$ są parzyste i większe od 2, czyli są to liczby złożone. Natomiast wśród pozostałych sześciu liczb $n, n+2, n+4, n+6$, $n+8, n+10$ na mocy zadania 22.58 istnieją dwie liczby podzielne przez 3, a ponieważ są one większe od 3, więc są to liczby złożone. Wobec tego w tym przypadku też wśród naszych dwunastu liczb nie ma pięciu liczb pierwszych.

Wobec tego odpowiedź na postawione w zadaniu pytanie brzmi: Nie może.

Zadanie 22.172. Bez zmniejszania ogólności możemy zakładać, że $x < y$. Wtedy $2 \cdot \frac{1}{x} > \frac{1}{x} + \frac{1}{y} = \frac{2}{7}$, więc $\frac{2}{x} > \frac{2}{7}$, skąd $x < 7$, czyli $x \leqslant 6$. Ponadto $\frac{1}{x} < \frac{2}{7}$, więc $x > 3,5$, a zatem $x = 4, 5, 6$. Ponadto $2xy = 7(x+y)$, więc dla $x = 4$, $8y = 7 \cdot 4 + 7y$, skąd $y = 28$. Jeśli $x = 5$, to $10y = 35 + 7y$, więc $3y = 35$, co prowadzi do sprzeczności. Jeśli $y = 6$, to $12y = 42 + 7y$, skąd $5y = 42$ i też mamy sprzeczność.

Wobec tego ostatecznie $x = 4$ i $y = 28$ lub $x = 28$ i $y = 4$.

Zadanie 22.173. Oznaczmy nasze liczby nieparzyste przez a i b. Wtedy $2 \mid a - b$. Ponadto $5 \mid a - b$. Zatem $10 \mid a - b$, ale $a - b \mid a^3 - b^3$, bo $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$, więc $10 \mid a^3 - b^3$. Zatem różnica sześcianów tych liczb posiada cyfrę jedności równą 0.

Zadanie 22.174. Ponieważ n jest liczbą parzystą, więc $n = 2k$ dla pewnego $k \in \mathbb{Z}$. Oznaczmy $a = n^4 - 4n^3 - 4n^2 + 16n$. Wtedy $a = n^3(n-4) - 4n(n-4) = (n-4)(n^3 - 4n) = (n-4)n(n^2-4) =$ $= (n-4)n(n-2)(n+2)$, a zatem $a = (2k-4) \cdot 2k(2k-2)(2k+2) =$

$= 2^4(k-2)(k-1)k(k+1)$. Z zadania 22.57, $(k-2)(k-1)k(k+1) = 24s$ dla pewnego $s \in \mathbb{Z}$, więc $a = 2^7 \cdot 3s = 384s$. Zatem $384 \mid a$, co należało wykazać.

Zadanie 22.175. Zauważmy, że dla dowolnej liczby całkowitej k: $(k+1)^2 - k^2 = 2k+1$ i $(k+1)^2 - (k-1)^2 = 4k$. Stąd wynika, że jeśli liczba całkowita nie daje reszty 2 z dzielenia przez 4, to ta liczba jest różnicą kwadratów dwóch licz całkowitych.

Pozostaje zatem rozważyć liczby $4s+2$ dla $s \in \mathbb{Z}$. Weźmy dowolne $a, b \in \mathbb{Z}$. Wtedy $a^2 - b^2 = (a-b)(a+b)$ i $(a-b) + (a+b) = 2a$ jest liczbą parzystą. Zatem liczby $a-b$ i $a+b$ są tej samej parzystości, ale jeśli są one parzyste, to ich iloczyn dzieli się przez 4, a jeśli obie te liczby są nieparzyste, to ich iloczyn też jest liczbą nieparzystą. Wobec tego $a^2 - b^2$ nie może być równe $4s+2$.

Podsumowując mamy, że liczb całkowita jest różnicą kwadratów dwóch liczb całkowitych wtedy i tylko wtedy, gdy ta liczba nie daje reszty 2 z dzielenia przez 4.

Zadanie 22.176. Załóżmy, że istnieją liczby naturalne x, y, z takie, że $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{8}{11}$. Wtedy bez zmniejszania ogólności rozważań możemy zakładać, że $x \leqslant y \leqslant z$. Stąd $3 \cdot \frac{1}{x} \geqslant \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{8}{11}$, czyli $\frac{3}{x} \geqslant \frac{8}{11}$, a zatem $8x \leqslant 33$. Wobec tego $x \leqslant 4$. Ponieważ $x > 1$, więc $x = 2, 3, 4$.

Załóżmy, że $x = 2$. Wtedy $z \geqslant y \geqslant 2$ i $\frac{1}{y} + \frac{1}{z} = \frac{8}{11} - \frac{1}{2}$, skąd $\frac{1}{y} + \frac{1}{z} = \frac{5}{22}$, ale $2 \cdot \frac{1}{y} \geqslant \frac{1}{y} + \frac{1}{z}$, więc $\frac{2}{y} \geqslant \frac{5}{22}$, czyli $5y \leqslant 44$ i wobec tego $y = 2, 3, 4, 5, 6, 7, 8$. Dodatkowo, $\frac{y+z}{yz} = \frac{5}{22}$, więc $5yz = 22(y+z)$. Stąd $5yz > 22z$, czyli $y > 4\frac{2}{5}$, a zatem $y = 5, 6, 7, 8$. Jeśli $y = 5$, to $25z = 22(5+z)$, skąd $3z = 110$ i mamy sprzeczność, bo $3 \nmid 110$. Jeżeli $y = 6$, to $30z = 22(6+z)$, skąd $8z = 132$ i $z = 16\frac{1}{2}$, co też jest niemożliwe. Jeśli $y = 7$, to $35z = 22(7+z)$, skąd $13z = 2 \cdot 11 \cdot 7$ i też mamy sprzeczność. Jeżeli $y = 8$, to $40z = 22(8+z)$, skąd $18z = 22 \cdot 8$, czyli $9z = 11 \cdot 8$ i mamy sprzeczność. Wobec tego $x \neq 2$.

Załóżmy, że $x = 3$. Wtedy $z \geqslant y \geqslant 3$ i $\frac{1}{y} + \frac{1}{z} = \frac{8}{11} - \frac{1}{3}$, skąd $\frac{1}{y} + \frac{1}{z} = \frac{13}{33}$, ale $2 \cdot \frac{1}{y} \geqslant \frac{1}{y} + \frac{1}{z}$, więc $\frac{2}{y} \geqslant \frac{13}{33}$, czyli $13y \leqslant 66$ i wobec tego $y = 3, 4, 5$. Dodatkowo, $\frac{y+z}{yz} = \frac{13}{33}$, więc $13yz = 33(y+z)$. Jeśli $y = 3$, to $39z = 33(3+z)$, więc $6z = 99$ i mamy sprzeczność (bo $2 \nmid 99$). Jeśli

$y = 4$, to $52z = 33(4 + z)$, skąd $19z = 3 \cdot 11 \cdot 4$ i też mamy sprzeczność. Jeśli $y = 5$, to $65z = 33(5 + z)$ i $32z = 33 \cdot 5$, co też jest niemożliwe, gdyż $2 \nmid 33 \cdot 5$. Wobec tego $x \neq 3$.

Załóżmy, że $x = 4$. Wtedy $z \geqslant y \geqslant 4$ i $\frac{1}{y} + \frac{1}{z} = \frac{8}{11} - \frac{1}{4} = \frac{21}{44}$, ale $2 \cdot \frac{1}{y} \geqslant \frac{1}{y} + \frac{1}{z}$, czyli $\frac{2}{y} \geqslant \frac{21}{44}$, skąd $21y \leqslant 88$, czyli $y \leqslant 4\frac{4}{21}$. Zatem $y = 4$ i $\frac{1}{z} = \frac{21}{44} - \frac{1}{4} = \frac{5}{11}$, skąd $z = \frac{11}{5}$ i mamy sprzeczność. Zatem $x \neq 4$.

Przypuszczenie, że istnieją liczby naturalne x, y, z takie, że $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{8}{11}$ doprowadziło nas do sprzeczności. Wobec tego takie liczby x, y, z nie istnieją.

Zadanie 22.177. Załóżmy, że $2x^2 - 5y^2 = 8z \pm 1$ dla pewnych $x, y, z \in \mathbb{Z}$. Wtedy y jest nieparzyste, więc z zadania 22.13 $[y^2]_8 = 1$, czyli $y^2 = 8k + 1$ dla pewnego $k \in \mathbb{Z}$. Jeśli x jest parzyste, to $x = 2t$ dla pewnego $t \in \mathbb{Z}$ i $x^2 = 4t^2$. Zatem $2x^2 - 5y^2 = 8(t^2 - 5k) - 5$, skąd $8(t^2 - 5k - z) = 5 \pm 1$, czyli $8 \mid 6$ lub $8 \mid 4$, co prowadzi do sprzeczności. Wobec tego x jest nieparzyste i z zadania 22.13 $x^2 = 8s+1$ dla pewnego $s \in \mathbb{Z}$, ale wtedy $2x^2 - 5y^2 = 2(8s + 1) - 5(8k + 1) = 8(2s - 5k) - 3$, więc $8(2s - 5k) - 3 = 8z \pm 1$. Zatem $8(2s - 5k - z) = 3 \pm 1$, skąd $8 \mid 4$ lub $8 \mid 2$, co też prowadzi do sprzeczności.

Wobec tego nie istnieją liczby całkowite x, y, z takie, że $2x^2 - 5y^2 = 8z \pm 1$.

Zadanie 22.178. Rozważmy najpierw przypadek, gdy $x \leqslant y \leqslant z$. Wtedy $x + y + z \leqslant 3z$, więc $xyz \leqslant 3z$, skąd $xy \leqslant 3$. Stąd $x^2 \leqslant 3$, czyli $x = 1$. Wobec tego $x = 1$ i $y = 1$ lub $x = 1$ i $y = 2$ lub $x = 1$ i $y = 3$. Jeśli $x = 1$ i $y = 1$, to $z = 2 + z$, czyli $z = 0$ i mamy sprzeczność. Jeśli $x = 1$ i $y = 2$, to $2z = 3 + z$, skąd $z = 3$. Jeśli $x = 1$ i $y = 3$, to $3z = 4 + z$, skąd $z = 2 < 3$, więc mamy sprzeczność.

Wobec tego wszystkimi rozwiązaniami naszego zadania są trójki: $(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)$.

Zadanie 22.179. Ponieważ $3 \mid 6n$, więc z cechy podzielności przez 3 mamy, że $3 \mid S(6n)$, ale $S(n) = S(6n)$, więc $3 \mid S(n)$ i znowu z cechy podzielności przez 3, $3 \mid n$. Zatem $n = 3m$ dla pewnego $m \in \mathbb{N}$. Stąd $6n = 18m$, więc $9 \mid 6n$ i z cechy podzielności przez 9, $9 \mid S(6n)$, ale

$S(n) = S(6n)$, więc $9 \mid S(n)$ i z cechy podzielności przez 9, $9 \mid n$, co należało wykazać.

Zadanie 22.180. Zauważmy, że $(ad+bc)-(ab+cd) = d(a-c)-$ $+b(a-c) = (a-c)(d-b)$, skąd $a-c \mid (ad+bc)-(ab+cd)$, a ponieważ $a-c \mid ab+cd$, więc $a-c \mid ad+bc$.

Zadanie 22.181. Rozważmy ciąg n liczb naturalnych: $a, a^2, \ldots, a^n$. Jeżeli te liczby dają parami różne reszty z dzielenia przez n, to z uwagi na to, że reszt z dzielenia przez n jest dokładnie n, istnieje $i \in \{1, 2, \ldots, n\}$ takie, że $[a^i]_n = 0$, czyli $n \mid a^i$, ale $n > 1$, więc istnieje liczba pierwsza p taka, że $p \mid n$, skąd $p \mid a^i$ i z własności liczb pierwszych, $p \mid a$. Zatem $p \mid a$ i $p \mid n$, więc mamy sprzeczność. Wobec tego liczby $a, a^2, \ldots, a^n$ nie dają parami różnych reszt z dzielenia przez n. Zatem istnieją $k, l \in \{1, 2, \ldots, n\}$ takie, że $k < l$ oraz $[a^l]_n = [a^k]_n$, skąd $n \mid a^l - a^k$, ale $a^l - a^k = a^k(a^{l-k} - 1)$ i jak pokazaliśmy, $n \nmid a^k$, więc z zasadniczego twierdzenia arytmetyki, $n \mid a^d - 1$, gdzie $d = l - k$ jest liczbą naturalną mniejszą od n, bo $l > k$ i $l - k \leqslant n - k \leqslant n - 1$.

Zadanie 22.182. Z założenia istnieją liczby całkowite k, l, t, s takie, że $a = k(ab - cd)$, $b = l(ab - cd)$, $c = t(ab - cd)$ i $d = s(ab - cd)$. Stąd $ab - cd = kl(ab - cd)^2 - ts(ab - cd)^2 = (kl - ts)(ab - cd)^2$, czyli $(ab - cd)^2 \mid ab - cd$, ale $ab - cd \neq 0$, bo inaczej $a = 0$, więc $ab - cd \mid 1$, skąd $ab - cd = \pm 1$ i $|ab - cd| = 1$.

Zadanie 22.183. Ponieważ dla każdej niezerowej cyfry c jest $\overline{cc\ldots c} = c \cdot \overline{11\ldots1}$, więc tezę wystarczy udowadniać dla liczb złożonych z samych jedynek.

Zastosujemy indukcję ze względu na n. Dla $n = 1$: $3^1 = 3$ i liczba 111 jest podzielna przez 3, bo suma jej cyfr jest równa $1 + 1 + 1 = 3$ i dzieli się przez 3.

Niech teza zachodzi dla pewnej liczby naturalnej n, to znaczy $3^n \mid a$, gdzie a jest liczbą 3^n-cyfrową złożoną z samych jedynek. Wtedy 3^{n+1}-cyfrowa liczba A złożona z samych jedynek jest równa $A = a \cdot 10^{2 \cdot 3^n} +$ $+a \cdot 10^{3^n} + a = a \cdot (10^{2 \cdot 3^n} + 10^{3^n} + 1)$. Z założenia indukcyjnego $a = 3^n \cdot t$ dla pewnego $t \in \mathbb{N}$. Ponadto suma cyfr liczby $10^{2 \cdot 3^n} + 10^{3^n} + 1$ jest równa $1 + 1 + 1 = 3$, czyli jest podzielna przez 3, więc $10^{2 \cdot 3^n} + 10^{3^n} + 1 = 3k$

dla pewnego $k \in \mathbb{N}$. Wobec tego $A = 3^n \cdot 3 \cdot tk = 3^{n+1}(tk)$, więc $3^{n+1} \mid A$ i teza zachodzi dla liczby $n+1$.

Stąd na mocy zasady indukcji matematycznej teza zachodzi dla każdej liczby naturalnej n.

Zadanie 22.184. Opiszemy najpierw wszystkie liczby naturalne n takie, że $55 \mid 11n^2 + 3n + 17$. Ponieważ $55 = 5 \cdot 11$ i liczby 5 i 11 są względnie pierwsze, więc potrzeba i wystarcza aby $5 \mid 11n^2 + 3n + 17$ i $11 \mid 11n^2 + 3n + 17$. Ta druga zależność jest równoważna temu, że $11 \mid 3n + 6$, ale $3n + 6 = 3(n + 2)$, więc z zasadniczego twierdzenia arytmetyki, jest to równoważne temu, że $11 \mid n + 2$, czyli temu, że $11 \mid n - 9$. Wobec tego $n = 11s + 9$ dla pewnego $s \in \mathbb{N}$.

Ponadto $5 \mid 11n^2 + 3n + 17 \iff 5 \mid n^2 + 3n + 2$, bo liczba $(11n^2 + 3n + 17) - (n^2 + 3n + 2) = 10n^2 + 15$ jest podzielna przez 5, ale $n^2 + 3n + 2 = (n + 1)(n + 2)$, więc z własności liczb pierwszych, $5 \mid 11n^2 + 3n + 17 \iff [5 \mid n + 1 \text{ lub } 5 \mid n + 2]$. Stąd $n = 5t + 4$ lub $n = 5t + 3$ dla pewnego $t \in \mathbb{N}$.

Dalej, n jest liczbą trzycyfrową, więc $100 \leqslant 11s + 9 \leqslant 999$, skąd $9 \leqslant s \leqslant 90$. Dla $s = 9$: $n = 108$ i $[108]_5 = [8]_5 = 3$. Wobec tego $n = 108$.

Zadanie 22.185. Z założenia wynika, że $17 \mid 8(3a + 2b)$. Wobec tego $17 \mid 24a + 16b$, ale $17 \mid 34a + 17b$, więc $17 \mid (34a + 17b) - (24a + 16b)$, skąd $17 \mid 10a + b$. Ponadto $17 \mid 51$, więc $17 \mid 10a + b - 51$.

Zadanie 22.186. Ponieważ $d = \mathrm{NWD}(a, b)$, więc $a = xd$ i $b = yd$ dla pewnych $x, y \in \mathbb{N}$ takich, że $\mathrm{NWD}(x, y) = 1$. Zatem $\frac{a+1}{b} + \frac{b+1}{a} = \frac{a^2+a+b^2+b}{ab} = \frac{d^2x^2+dx+d^2y^2+dy}{d^2xy} = \frac{dx^2+x+dy^2+y}{dxy}$, a ponieważ $\frac{a+1}{b} + \frac{b+1}{a} \in \mathbb{N}$, więc $dxy \mid dx^2 + x + dy^2 + y$, skąd $d \mid d(x^2 + y^2) + (x + y)$. Wobec tego $d \mid x + y$, skąd $d \leqslant x + y$ i po pomnożeniu obu stron przez d uzyskujemy, że $d^2 \leqslant a + b$, co należało wykazać.

Zadanie 22.187. Weźmy dowolne $s \in S$. Wtedy istnieje liczba naturalna a i liczba naturalna b posiadająca dokładnie n cyfr takie, że $s = a \cdot 10^{n+2} + b$, przy czym $a \cdot 10^{n+2} + b = 76 \cdot (a \cdot 10^n + b)$, skąd $a \cdot 24 \cdot 10^n = 75b$, ale $b < 10^n$, więc $a \cdot 24 < 75$, skąd $a \leqslant 3$ i $b = 8a \cdot \frac{10^n}{25}$, skąd $n \geqslant 2$. Wobec tego $s = 10^{n+2} + 8a \cdot \frac{10^n}{25}$, gdzie

$a = 1, 2, 3$ i $n = 2, 3, \ldots$. Na odwrót, jeśli $s = a \cdot 10^{n+2} + 8a \cdot \frac{10^n}{25}$, gdzie $a = 1, 2, 3$ i $n = 2, 3, \ldots$, to $s \in \mathbb{N}$, bo $25 \mid 10^n$ i $10^{n-1} < 8a \cdot \frac{10^n}{25} < 10^n$, więc liczba $b = 8a \cdot \frac{10^n}{25}$ ma dokładnie n cyfr i po wykreśleniu w liczbie s dwóch kolejnych zer uzyskamy liczbę $c = a \cdot 10^n + b$, przy czym $76c = 76a \cdot 10^n + 76b = a \cdot 10^{n+2} - 24a \cdot 10^n + 100b - 24b = a \cdot 10^{n+2} - 24a \cdot 10^n + 32a \cdot 10^n - 24 \cdot 8a \cdot \frac{10^n}{25} = a \cdot 10^{n+2} + 10^n a \cdot (8 - \frac{24 \cdot 8}{25}) = a \cdot 10^{n+2} + 8a \cdot \frac{10^n}{25} = s$.

Wobec tego $S = \{a \cdot 10^{n+2} + 8a \cdot \frac{10^n}{25} : a = 1, 2, 3 \text{ i } n = 2, 3, \ldots\}$. Stąd do zbioru S należą liczby $s_n = 10^{n+2} + 8 \cdot \frac{10^n}{25}$ dla $n = 2, 3, 4, \ldots$, a ponieważ ciąg (s_n) jest rosnący, więc zbiór S jest nieskończony.

Zadanie 22.188. Ponieważ $23 \cdot 1 = 23$, więc $1 \notin S$. Niech $n \in \mathbb{N}$ i $n > 1$. Wówczas $n \in S$ wtedy i tylko wtedy, gdy istnieje niezerowa cyfra a i liczba naturalna s takie, że $23n = a \cdot \frac{10^s - 1}{9}$, gdyż liczba s cyfrowa złożona z samych jedynek jest równa $\frac{10^s - 1}{9}$. Ponadto $23 \mid \frac{10^s - 1}{9} \iff 23 \mid 10^s - 1$, gdyż $9 \mid 10^s - 1$ i liczby 23 oraz 9 są względnie pierwsze. Wobec tego $S = \{a \cdot \frac{10^s - 1}{23 \cdot 9} : s \in \mathbb{N} \text{ i } 23 \mid 10^s - 1\}$. Ponieważ 23 jest liczbą pierwszą i $23 \nmid 10$, więc z małego twierdzenia Fermata $23 \mid 10^{22} - 1$. Stąd zaś $23 \mid 10^{22k} - 1$ dla każdego $k \in \mathbb{N}$. Wobec tego dla $k \in \mathbb{N}$: $s_k = \frac{10^s - 1}{23 \cdot 9}$ mamy, że $s_k \in S$, a ponieważ ciąg (s_k) jest rosnący, więc zbiór S jest nieskończony.

Najmniejsza liczba należąca do S jest postaci $\frac{10^d - 1}{23 \cdot 9}$, gdzie s jest najmniejszą liczbą naturalną taką, że $23 \mid 10^d - 1$. Stąd $d > 1$ i $d \leqslant 22$, bo $23 \mid 10^{22} - 1$, ale z zadania 22.160 reszta z dzielenia liczby $10^{22} - 1$ przez liczbę $10^d - 1$ jest równa $10^{[22]_d} - 1$ i 23 dzieli tę resztę, więc z minimalności d, $[22]_d = 0$, czyli $d \mid 22$. Ponadto $d > 1$ i $22 = 2 \cdot 11$, więc $d = 2$ lub $d = 11$ lub $d = 22$, ale $10^2 - 1 = 99 = 9 \cdot 11$, więc $d = 11$ lub $d = 22$. Ponadto $[10^3]_{23} = 11$, $[10^4]_{23} = 18$ i $[10^8]_{23} = [18^2]_{23} = 2$, więc $[10^{11}]_{23} = [2 \cdot 11]_{23} = 22$, skąd $d \neq 11$ i wobec tego $d = 22$. Zatem najmniejszą liczbą w zbiorze S jest $\frac{10^{22} - 1}{9 \cdot 23}$.

Zadanie 22.189. Ponieważ $60 = 4 \cdot 3 \cdot 5$ i liczby $3, 4, 5$ są parami względnie pierwsze, więc wystarczy wykazać, że $4 \mid xyz$ i $3 \mid xyz$ i $5 \mid xyz$.

Jeśli 3 nie dzieli żadnej z liczb x, y, z, to na mocy zadania 22.8, $x^2 = 3k + 1$ i $y^2 = 3t + 1$ i $z^2 = 3s + 1$ dla pewnych $k, t, s \in \mathbb{N}_0$,

skąd $3(k+t)+2 = 3s+1$, co przeczy twierdzeniu o dzieleniu z resztą. Zatem $3 \mid x$ lub $3 \mid y$ lub $3 \mid z$, skąd $3 \mid xyz$.

Załóżmy, że 4 nie dzieli żadnej z liczb x, y, z. Jeśli $a \in \mathbb{Z}$ i $4 \nmid a$, to z twierdzenia o dzieleniu z resztą wynika, że $a = 4k+1$ lub $a = 4k+2$ lub $a = 4k+3$ dla pewnego $k \in \mathbb{Z}$, skąd $a^2 = 16k^2+8k+1 = 8(2k^2+k)+1$ lub $a^2 = 16k^2+16k+4 = 8(2k^2+2k)+4$ lub $a^2 = 16k^2+24k+9 = 8(2k^2+3k+1)+1$, czyli $a^2 = 8t+1$ lub $a^2 = 8t+4$ dla pewnego $t \in \mathbb{N}_0$. Stąd $x^2 = 8u+1$ lub $x^2 = 8u+4$ dla pewnego $u \in \mathbb{N}_0$ i $y^2 = 8v+1$ lub $y^2 = 8v+4$ i $z^2 = 8r+1$ lub $z^2 = 8r+4$ dla pewnego $r \in \mathbb{N}_0$. Wobec tego $x^2+y^2 = 8(u+v)+2$ lub $x^2+y^2 = 8(u+v)+5$ lub $x^2+y^2 = 8(u+v+1)$ oraz $x^2+y^2 = z^2$, więc mamy sprzeczność z twierdzeniem o dzieleniu z resztą. Wobec tego $4 \mid x$ lub $4 \mid y$ lub $4 \mid z$, skąd $4 \mid xyz$.

Załóżmy, że 5 nie dzieli żadnej z liczb x, y, z. Jeśli $a \in \mathbb{Z}$ i $5 \nmid a$, to z twierdzenia o dzieleniu z resztą wynika, że $a = 5k+1$ lub $a = 5k+2$ lub $a = 5k+3$ lub $a = 5k+4$ dla pewnego $k \in \mathbb{Z}$, skąd $a^2 = 25k^2+10k+1 = 5(5k^2+2k)+1$ lub $a^2 = 25k^2+20k+4 = 5(5k^2+4k)+4$ lub $a^2 = 25k^2+30k+9 = 5(5k^2+6k+1)+41$ lub $a^2 = 25k^2+40k+16 = 5(5k^2+8k+3)+1$, czyli $a^2 = 5t+1$ lub $a^2 = 5t+4$ dla pewnego $t \in \mathbb{N}_0$. Stąd $x^2 = 5u+1$ lub $x^2 = 5u+4$ dla pewnego $u \in \mathbb{N}_0$ i $y^2 = 5v+1$ lub $y^2 = 5v+4$ i $z^2 = 5r+1$ lub $z^2 = 5r+4$ dla pewnego $r \in \mathbb{N}_0$. Wobec tego $x^2+y^2 = 5(u+v)+2$ lub $x^2+y^2 = 5(u+v+1)+3$ lub $x^2+y^2 = 5(u+v+1)$ oraz $x^2+y^2 = z^2$, więc mamy sprzeczność z twierdzeniem o dzieleniu z resztą. Wobec tego $5 \mid x$ lub $5 \mid y$ lub $5 \mid z$, skąd $5 \mid xyz$, co kończy dowód.

Zadanie 22.190. Ponieważ $1^2 = 1$ i $\tau(1) = 1$, więc $1 \notin S$. Weźmy dowolne naturalne $n > 1$. Wtedy istnieją różne liczby pierwsze $p_1, \ldots, p_s$ i liczby naturalne $a_1, \ldots, a_s$ takie, że $n = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$, skąd $n^2 = p_1^{2a_1} \cdot \ldots \cdot p_s^{2a_s}$. Ponadto $\tau(n) = (a_1+1) \cdot \ldots \cdot (a_s+1)$ i $\tau(n^2) = (2a_1+1) \cdot \ldots \cdot (2a_s+1)$. Zatem $\tau(n^2) = 3\tau(n)$ wtedy i tylko wtedy, gdy $(2a_1+1) \cdot \ldots \cdot (2a_s+1) = 3 \cdot (a_1+1) \cdot \ldots \cdot (a_s+1)$.

Ponieważ $a_i \geqslant 1$, więc $2a_i+1 \geqslant \frac{3}{2}(a_i+1)$ dla $i = 1, \ldots, s$. Stąd $(2a_1+1) \cdot \ldots \cdot (2a_s+1) \geqslant (\frac{3}{2})^s \cdot (a_1+1) \cdot \ldots \cdot (a_s+1)$. Wobec tego, jeśli $n \in S$, to $3 \cdot (a_1+1) \cdot \ldots \cdot (a_s+1) \geqslant (\frac{3}{2})^s \cdot (a_1+1) \cdot \ldots \cdot (a_s+1)$, skąd $(\frac{3}{2})^s \leqslant 3$, ale dla $s \geqslant 3$ mamy, że $(\frac{3}{2})^s \geqslant (\frac{3}{2})^3 = 3\frac{3}{8} > 3$, więc $s \leqslant 2$.

Jeśli $s = 1$, to $2a_1 + 1 = 3(a_1 + 1)$, skąd $a_1 = -2$ i mamy sprzeczność. Wobec tego $s = 2$, co kończy dowód punktu a).

Niech teraz $n = p^a \cdot q^b$, gdzie p i q są różnymi liczbami pierwszymi i $a, b \in \mathbb{N}$, przy czym $a \leqslant b$. Wówczas $n \in S \iff (2a+1)(2b+1) = 3(a+1)(b+1) \iff 4ab + 2a + 2b + 1 = 3ab + 3a + 3b + 3$, czyli $n \in S \iff ab - a - b - 2 = 0 \iff (a-1)(b-1) = 3$, ale $a-1 \leqslant b-1$, więc $a - 1 = 1$ i $b - 1 = 3$, skąd $n \in S \iff [a = 2 \text{ i } b = 4]$. W takim razie $S = \{p^2q^4 : p, q \in \mathbb{P}, p \neq q\}$, gdzie $\mathbb{P}$ oznacza zbiór wszystkich liczb pierwszych. Stąd najmniejszą liczbą ze zbioru S jest $2^4 \cdot 3^2 = 144$.

Zadanie 22.191. Suma cyfr liczby $10n$ jest równa sumie cyfr liczby n, czyli wynosi s, ale reszta z dzielenia liczby naturalnej przez 9 jest równa reszcie z dzielenia przez 9 sumy cyfr tej liczby. Stąd liczby s i $10n$ dają tę samą resztę z dzielenia przez 9.

Zadanie 22.192. Niech $n \in \mathbb{N}$. Zauważmy, że $59 \mid 12n - 35$ wtedy i tylko wtedy, gdy $59 \mid (12n-35)+59 \iff 59 \mid 12(n+2)$, więc na mocy zasadniczego twierdzenia arytmetyki, $59 \mid 12n - 35 \iff 59 \mid n + 2$, ale $59 \mid n + 2 \iff 59 \mid (n + 2) - 59 \iff 59 \mid n - 57$, więc $59 \mid 12n - 35 \iff [n]_{59} = 57$. Ponadto, $3 \mid 5n - 1$ wtedy i tylko wtedy, gdy $3 \mid (5n - 1) - 6n \iff 3 \mid -(n + 1) \iff 3 \mid n + 1 \iff 3 \mid n - 2$. Stąd $[5n]_3 = 1 \iff [n]_3 = 2$.

W takim razie $59|12n - 35$ i jednocześnie $[5n]_3 = 1$ wtedy i tylko wtedy, gdy $n = 59k + 57$ dla pewnego $k \in \mathbb{N}_0$ takiego, że $3 \mid 59k + 55$. Dalej, $3 \mid 59k + 55 \iff 3 \mid (59k + 55) - (60k + 54)$, więc stąd $3 \mid 59k + 55 \iff 3 \mid -k + 1 \iff 3 \mid k - 1$, czyli $k = 3t + 1$ dla pewnego $t \in \mathbb{N}_0$ i ostatecznie $n = 59(3t+1)+57 = 177t+116$. Ponadto liczba n ma być trzycyfrowa, więc $177t + 116 \leqslant 999$, skąd $t \leqslant 4$. Zatem największe takie n jest równe $n = 177 \cdot 4 + 116 = 824$.

Zadanie 22.193. Załóżmy, że istnieje $k \in \mathbb{N}$ i istnieją liczby pierwsze p i q takie, że $p - q = 18k + 1$. Wtedy $p - q$ jest liczbą nieparzystą, a zatem liczby p i q są różnej parzystości, ale jedyną parzystą liczbą pierwszą jest liczba 2, więc $p = 2$ lub $q = 2$. W pierwszym przypadku $q \geqslant 3$, więc $p - q = 2 - 3 < 0$ i mamy sprzeczność. W drugim przy-

padku $p-2=18k+1$, więc $p=3(6k+1)$, a ponieważ $6k+1\in\mathbb{N}$ i $6k+1>1$, więc p jest liczbą złożoną i mamy sprzeczność.

Uzyskana sprzeczność pokazuje, że taka liczba naturalna k nie istnieje.

Zadanie 22.194. Dla $n>4$ mamy, że $2n>9$, skąd $(n+1)^2<$ $<n^2+4n-8<(n+2)^2$, więc jeżeli wtedy $n^2+4n-8=k^2$ dla pewnego $k\in\mathbb{N}$, to $(n+1)^2<k^2<(n+2)^2$, skąd $n+1<k<n+2$, co jest niemożliwe.

Pozostaje zatem sprawdzić dla liczb $n=1,2,3,4$: $1^2+4\cdot1-8=-3$ - nie jest kwadratem liczby naturalnej, $2^2+4\cdot2-8=2^2$ - jest kwadratem liczby naturalnej, $3^2+4\cdot3-8=13$ - nie jest kwadratem liczby naturalnej, $4^2+4\cdot4-8=24$ - nie jest kwadratem liczby naturalnej.

Wobec tego jedyną liczbą naturalną n, dla której n^2+4n-8 jest kwadratem liczby naturalnej jest $n=2$.

Zadanie 22.195. Niech X będzie niepustym podzbiorem zbioru $\mathbb{Z}$ ograniczonym z dołu. Wtedy istnieje $a\in\mathbb{Z}$ takie, że $a\leqslant x$ dla każdego $x\in X$. Wobec tego zbiór A liczb całkowitych k takich, że $k\leqslant x$ dla każdego $x\in X$ jest niepusty. Ponadto zbiór X jest niepusty i zbiór A jest ograniczony z góry przez każdą liczbę ze zbioru X. Z zasady maksimum (stwierdzenie 2.24) wynika zatem, że w zbiorze A istnieje liczba największa a_0. Zatem $b\leqslant a_0$ dla każdego $b\in A$ i $a_0\leqslant x$ dla każdego $x\in X$. Załóżmy, że $a_0\notin X$. Wtedy $a_0<x$, skąd $a_0+1\leqslant x$ dla każdego $x\in X$. Zatem $a_0+1\in A$ i $a_0<a_0+1$, co przeczy maksymalności a_0. Przypuszczenie, że $a_0\notin X$ doprowadziło nas zatem do sprzeczności. Wobec tego $a_0\in X$, skąd a_0 jest najmniejszym elementem zbioru X. Wystarczy więc przyjąć $x_0=a_0$.

Zadanie 22.196. Załóżmy, że przy tych założeniach istnieje liczba całkowita m taka, że $m\geqslant n_0$ i $m\notin A$. Ponieważ $n_0\in A$, więc $m>n_0$. Wobec tego zbiór B liczb całkowitych s takich, że $s>n_0$ i $s\notin A$ jest niepusty i ograniczony z dołu. Zatem z zadania 22.195 istnieje w tym zbiorze liczba najmniejsza m_0, ale $m_0>n_0$, więc $n_0-1\in\mathbb{Z}$ i $m_0-1\geqslant n_0$ oraz $m_0-1<m_0$. Wobec tego z minimalności m_0 mamy, że $m_0-1\notin B$. W takim razie $m_0-1\in A$, ale implikacja:

$m_0 - 1 \in A \Rightarrow (m_0 - 1) + 1 \in A$ jest prawdziwa i $(m_0 - 1) + 1 = m_0$, więc $m_0 \in A$ i mamy sprzeczność.

Przypuszczenie, że istnieje liczba całkowita $k \geqslant n_0$ taka, że $k \notin A$ doprowadziło nas zatem do sprzeczności. Wobec tego każda liczba całkowita $n \geqslant n_0$ należy do A.

Zadanie 22.197. Zastosujemy indukcję matematyczną dla $n_0 = 1$. Z naszych założeń wynika, że $m \mid a^2 + b$ i $m \mid a(a + b)$, więc m dzieli różnicę tych liczb, czyli $m \mid b - ab$. Załóżmy, że k jest taką liczbą naturalną, że $m \mid a^k + b$. Wtedy $a^{k+1} + b = a(a^k + b) + (b - ab)$, więc $m \mid a^{k+1} + b$. Wobec tego na mocy zasady indukcji matematycznej $m \mid a^n + b$ dla każdej liczby naturalnej n.

Zadanie 22.198. (P). Sprawdzamy prawdziwość naszego twierdzenia dla $n = 0$: $2^2 \cdot 3^0 + 5 \cdot 0 - 4 = 4 - 4 = 0 = 25 \cdot 0$, więc teza zachodzi dla $n = 0$.

(R). Założenie indukcyjne: Dla pewnego całkowitego $k \geqslant 0$ mamy, że $25 \mid 2^{k+2} \cdot 3^k + 5k - 4$.

Teza indukcyjna: $25 \mid 2^{n+2} \cdot 3^n + 5n - 4$ dla $n = k + 1$.

Dowód tezy indukcyjnej: Na mocy założenia indukcyjnego $2^{k+2} \cdot 3^k + 5k - 4 = 25t$ dla pewnego $t \in \mathbb{Z}$. Stąd $2^{k+2} \cdot 3^k = 25t + {} + 4 - 5k$. Po pomnożeniu obu stron tej równości przez 6 uzyskujemy, że $2^{k+3} \cdot 3^{k+1} = 25 \cdot 6t + 24 - 30k$. Dalej, dla $n = k + 1$ mamy, że $2^{n+2} \cdot 3^n + 5n - 4 = 2^{k+3} \cdot 3^{k+1} + 5(k + 1) - 4$, więc $2^{n+2} \cdot 3^n + 5n - 4 = {} = [25 \cdot 6t + 24 - 30k] + 5(k + 1) - 4 = 25 \cdot 6t + 24 - 30k + 5k + 5 - 4 = {} = 25 \cdot 6t - 25k + 25 = 25(6t - k + 1)$, a ponieważ $6t - k + 1 \in \mathbb{Z}$, więc $25 \mid 2^{n+2} \cdot 3^n + 5n - 4$ dla $n = k + 1$, co należało udowodnić w tezie indukcyjnej.

Z (P) i (R) na mocy zasady indukcji matematycznej wynika, że $25 \mid 2^{n+2} \cdot 3^n + 5n - 4$ dla każdego $n \in \mathbb{N}_0$.

Zadanie 22.199. (P). Sprawdzamy prawdziwość naszego twierdzenia dla $n = 0$: $3^1 + 40 \cdot 0 - 3 = 0 = 64 \cdot 0$, więc teza zachodzi dla $n = 0$.

(R). Założenie indukcyjne: Dla pewnego całkowitego $k \geqslant 0$ mamy, że $64 \mid 3^{2k+1} + 40k - 3$.

Teza indukcyjna: $64 \mid 3^{2n+1} + 40n - 3$ dla $n = k + 1$.

Dowód tezy indukcyjnej: Na mocy założenia indukcyjnego $3^{2k+1} + 40k - 3 = 64t$ dla pewnego $t \in \mathbb{Z}$, więc $3^{2k+1} = 64t - 40k + 3$. Po pomnożeniu obu stron tej równości przez 9 uzyskujemy, że $3^{2k+3} = 64 \cdot 9t - 360k + 27$. Ponadto dla $n = k+1$ mamy, że $3^{2n+1} + 40n - 3 = 3^{2k+3} + 40(k+1) - 3$, więc $3^{2n+1} + 40n - 3 = [64 \cdot 9t - 360k + 27] + 40(k+1) - 3 = 64 \cdot 9t - 360k + 27 + 40k + 40 - 3 = 64 \cdot 9t - 320k + 64 = 64(9t - 5k + 1)$, a ponieważ $9t - 5k + 1 \in \mathbb{Z}$, więc $64 \mid 3^{2n+1} + 40n - 3$ dla $n = k + 1$, co należało udowodnić w tezie indukcyjnej.

Z (P) i (R) na mocy zasady indukcji matematycznej wynika, że $25 \mid 2^{n+2} \cdot 3^n + 5n - 4$ dla każdego $n \in \mathbb{N}_0$.

Zadanie 22.200. Z twierdzenia o dzieleniu z resztą wynika, że możliwe są tylko następujące przypadki:

1. $n = 5k$ dla pewnego $k \in \mathbb{N}$. Wtedy dla $k > 1$ liczba n jest złożona, więc $k = 1$ i $n = 5$, skąd $n + 2 = 7$ jest liczbą pierwszą, $n + 6 = 11$ jest liczbą pierwszą, $n + 8 = 13$ jest liczbą pierwszą, $n + 12 = 17$ jest liczbą pierwszą i $n + 14 = 19$ jest liczbą pierwszą.

2. $n = 5k + 1$ dla pewnego $k \in \mathbb{N}$. Wtedy $n + 14 > 5$ i $n + 14 = 5(k + 3)$, więc $n + 14$ jest liczbą złożoną.

3. $n = 5k+2$, dla pewnego $k \in \mathbb{N}_0$. Wtedy $n+8 > 5$ i $n+8 = 5(k+2)$, więc $n + 8$ jest liczbą złożoną.

4. $n = 5k+3$ dla pewnego $k \in \mathbb{N}_0$. Wtedy $n+2 = 5(k+1)$, więc dla $k > 0$ liczba $n + 2$ jest złożona, skąd $k = 0$ i $n = 3$. Wtedy $n + 3 = 6$ jest liczbą złożoną.

5. $n = 5k+4$ dla pewnego $k \in \mathbb{N}_0$. Wtedy $n+6 > 5$ i $n+6 = 5(k+2)$, więc $n + 6$ jest liczbą złożoną.

Podsumowując mamy zatem, że $n = 5$.

Zadanie 22.201. Ponieważ $p \geqslant 2$, więc $n > 1$. Z twierdzenia 9.22 wynika, że wszystkimi naturalnymi dzielnikami liczby n mniejszymi od n są liczby: $1, 2, \ldots, 2^{p-1}, 2^p - 1, 2 \cdot (2^p - 1), \ldots, 2^{p-2} \cdot (2^p - 1)$. Ponieważ $1 + 2 + \ldots + 2^{p-1} = 2^p - 1$ i $1 + 2 + \ldots + 2^{p-2} = 2^{p-1} - 1$, więc suma tych wszystkich dzielników jest równa $(2^p - 1) + (2^p - 1) \cdot (2^{p-1} - 1) = (2^p - 1) \cdot [1 + (2^{p-1} - 1)] = 2^{p-1} \cdot (2^p - 1) = n$. Zatem liczba n jest doskonała.

Zadanie 22.202. Ponieważ $2^2 - 1 = 3$ jest liczbą pierwszą, więc

z zadania 22.201 liczba $2^1 \cdot 3 = 6$ jest doskonała. Ponieważ $2^3 - 1 = 7$ jest liczbą pierwszą, więc liczba $2^2 \cdot 7 = 28$ jest doskonała. Ponieważ $2^5 - 1 = 31$ jest liczbą pierwszą, więc liczba $2^4 \cdot 31 = 496$ jest doskonała.

Zadanie 22.203. Ponieważ $8128 = 2^6 \cdot 127$ i $127 = 2^7 - 1$ oraz z zadania 22.29, 127 jest liczbą pierwszą, więc na mocy zadania 22.201 liczba 8128 jest doskonała.

Zadanie 22.204. Z założenia wynika, że $2^p - 1 = ab$ dla pewnych liczb naturalnych $a, b > 1$. Liczba $n = 2^{p-1}(2^p - 1) = 2^{p-1}ab$ posiada następujące różne dzielniki mniejsze od n:

$$ab, 2ab, \ldots, 2^{p-2}ab, a, 2a, \ldots, 2^{p-1}a.$$

Stąd suma s wszystkich dzielników liczby n mniejszych od n jest co najmniej równa: $ab(1 + 2 + \ldots + 2^{p-2}) + a(1 + 2 + \ldots + 2^{p-1}) = ab(2^{p-1} - 1) + a(2^p - 1)$, ale $2^p - 1 = ab$, więc $s \geqslant ab(2^{p-1} - 1) + aab > ab(2^{p-1} - 1) + ab = ab \cdot 2^{p-1} = n$, czyli $s > n$, a to oznacza, że liczba n nie jest doskonała.

Zadanie 22.205. Ponieważ $2^{11} - 1 = 2047 = 23 \cdot 89$, więc na mocy zadania 22.204 liczba $2^{10} \cdot (2^{11} - 1)$ nie jest doskonała.

Zadanie 22.206. Zastosujemy indukcję względem n. Dla $n = 1$ mamy: $F_0 \cdot F_1 = (2^{2^0} + 1) \cdot (2^{2^1} + 1) = 3 \cdot 5 = 15$ oraz $F_2 = 2^{2^2} + 1 = 17$, więc wtedy wzór (22.3) zachodzi.

Załóżmy, że wzór (22.3) zachodzi dla pewnego naturalnego $n = k$. Wtedy $F_0 \cdot F_1 \cdot \ldots \cdot F_k = F_{k+1} - 2 = 2^{2^{k+1}} - 1$, więc $F_0 \cdot F_1 \cdot \ldots \cdot F_k \cdot F_{k+1} = (2^{2^{k+1}} - 1) \cdot (2^{2^{k+1}} + 1) = (2^{2^{k+1}})^2 - 1 = 2^{2^{k+2}} - 1 = F_{k+2} - 1$, czyli wówczas ten wzór zachodzi także dla liczby $n = k + 1$.

Stąd na mocy zasady indukcji matematycznej wzór (22.3) zachodzi dla każdej liczby naturalnej n.

Zadanie 22.207. (i). Z własności potęgowania liczb mamy, że $2^0 < 2^1 < 2^2 < \ldots$, skąd $2^{2^0} < 2^{2^1} < 2^{2^2} < \ldots$, a więc $2^{2^0} + 1 < 2^{2^1} + 1 < 2^{2^2} + 1 < \ldots$, czyli $F_0 < F_1 < F_2 < \ldots$.

(ii). Dla $n \in \mathbb{N}_0$ liczba $2^n \in \mathbb{N}$, skąd 2^{2^n} jest liczbą naturalną

parzystą, więc $F_n = 2^{2^n} + 1$ jest nieparzystą liczbą naturalną większą od 1.

(*iii*). Bez zmniejszania ogólności rozważań możemy zakładać, że $m < n$. Jeżeli $m = 0$ i $n = 1$, to $F_m = 3$ i $F_n = 5$, więc $\mathrm{NWD}(F_n, F_m) = 1$. W przeciwnym przypadku $n > 1$ i ze wzoru (6) wynika, że jeżeli liczba naturalna d jest wspólnym dzielnikiem liczb F_m i F_n, to $d \mid 2$, czyli $d = 1$ lub $d = 2$, ale na mocy (*ii*), $d \neq 2$, więc $d = 1$. Zatem liczby F_n i F_m są względnie pierwsze.

Zadanie 22.208. Z zadania 22.207 (*ii*) wynika, że dla każdego $n \in \mathbb{N}_0$ mamy, że $F_n > 1$ i $F_n \in \mathbb{N}$. Wobec tego istnieje liczba pierwsza p_n taka, że $p_n \mid F_n$ dla każdego $n \in \mathbb{N}_0$, ale na mocy zadania 22.207 (*iii*) ciąg (p_n) jest różnowartościowy, więc zbiór $\{p_n : n \in \mathbb{N}_0\}$ jest nieskończony. Zatem zbiór wszystkich liczb pierwszych też jest nieskończony.

Zadanie 22.209. Dla liczb naturalnych $n \geqslant 2$ mamy, że $2^{2^n} = (2^4)^{2^{n-2}} = 16^{2^{n-2}}$. Ponadto iloczyn liczb o cyfrze jedności 6 jest liczbą o cyfrze jedności równej 6, więc stąd cyfrą jedności liczby 2^{2^n} jest 6. Stąd cyfrą jedności liczby F_n jest $6 + 1 = 7$.

Zadanie 22.210. Jeżeli $a > 2$, to $a - 1 > 1$ i $a - 1 \mid a^n - 1$, przy czym $a < a^n$, bo $a, n > 1$, więc $a-1 < a^n-1$. Stąd a^n-1 nie jest liczbą pierwszą. Wobec tego $a - 1 = 1$ i $a = 2$. Jeżeli n jest nieparzyste, to z zadania 22.91, $3 \mid 2^n+1$, bo $3 = 2+1$. Ponadto $n > 1$, więc $2^n+1 > 3$, skąd $2^n + 1$ nie jest liczbą pierwszą. Wobec tego n jest parzyste, czyli $n = 2k$ dla pewnego $k \in \mathbb{N}$, ale wtedy $2^n - 1 = (2^k - 1)(2^k + 1)$, więc z pierwszości liczby $2^n - 1$ mamy, że $2^k - 1 = 1$, skąd $k = 1$ i $n = 2$. Ponadto $2^2 - 1 = 3$ i $2^2 + 1 = 5$ są liczbami pierwszymi.

Wobec tego jedynym rozwiązaniem naszego zadania jest $a = n = 2$.

Zadanie 22.211. Załóżmy, że istnieje permutacja a, b, c, d, e, f cyfr 1, 2, 3, 4, 5, 6 taka, że liczba $\overline{abcdef}$ jest podzielna przez 11. Wówczas na mocy zadania 22.20, $11 \mid f - e + d - c + b - a$. Zatem $b + d + f = a + c + e + 11k$ dla pewnego $k \in \mathbb{Z}$. Ponadto $a + b + c + d + e + f = 1 + 2 + 3 + 4 + 5 + 6 = 21$, więc $2(a + c + e) + 11k = 21$. Dalej,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$a+c+e \leqslant 4+5+6 = 15$, więc $21 \leqslant 2\cdot 15+11k$, skąd $k \geqslant 0$. Zauważmy, że $a+c+e \geqslant 1+2+3 = 6$, więc $21 \geqslant 2\cdot 6+11k$, skąd $k \leqslant 0$. Wobec tego $k = 0$ i $2(a+c+e) = 21$, co jest niemożliwe, bo $2 \nmid 21$.

Wobec tego nie jest możliwe utworzenie takiej liczby sześciocyfrowej.

Zadanie 22.212. Z twierdzenia o dzieleniu z resztą wynika, że możliwe są tylko następujące przypadki:

1. $p = 5k$ dla pewnego $k \in \mathbb{N}$. Wtedy z pierwszości p mamy, że $k = 1$ i $4p^2+1 = 101$ oraz $6p^2+1 = 151$ są liczbami pierwszymi na mocy zadania 22.29.

2. $n = 5k+1$ dla pewnego $k \in \mathbb{N}$. Wtedy $4p^2+1 = 4(25k^2+10k+1)+1 = 5(20k^2+8k+1)$ i $20k^2+8k+1 > 1$, więc $4p^2+1$ jest liczbą złożoną.

3. $p = 5k+2$ dla pewnego $k \in \mathbb{N}_0$. Wtedy $6p^2+1 > 5$ oraz $6p^2+1 = 6(25k^2+20k+4)+1 = 5(30k^2+24k+5)$, więc $6p^2+1$ jest liczbą złożoną.

4. $p = 5k+3$ dla pewnego $k \in \mathbb{N}_0$. Wtedy $6p^2+1 > 5$ oraz $6p^2+1 = 6(25k^2+30k+9)+1 = 5(30k^2+36k+11)$, więc $6p^2+1$ jest liczbą złożoną.

5. $p = 5k+4$ dla pewnego $k \in \mathbb{N}$. Wtedy $4p^2+1 > 5$ i $4p^2+1 = 4(25k^2+40k+16)+1 = 5(20k^2+32k+13)$, więc $4p^2+1$ jest liczbą złożoną.

Podsumowując widzimy zatem, że jedynym rozwiązaniem naszego zadania jest liczba $p = 5$.

Zadanie 22.213. Ponieważ $40 = 2^3\cdot 5$ i $51 = 3\cdot 17$, więc liczby 40 i 51 są względnie pierwsze. Z zasadniczego twierdzenia arytmetyki wynika zatem, że $51 \mid a$, czyli $a = 51u$ dla pewnego $u \in \mathbb{N}$. Stąd $b = 40u$, a zatem $a+b = 91u = 7\cdot 13u$, czyli $a+b$ jest liczbą złożoną.

Zadanie 22.214. Z założenia wynika, że $17 \mid 7(2x+4y+5z)$, czyli $17 \mid 14x+28y+35z$, ale $17 \mid 17x+34y+34z$, więc $17 \mid (17x+34y+34z)-(14x+28y+35z)$, czyli $17 \mid 3x+6y-z$.

Zadanie 22.215. Korzystając z algorytmu Euklidesa mamy, że $\mathrm{NWD}(5a+3b, 13a+8b) = \mathrm{NWD}(5a+3b, 13a+8b-2(5a+3b)) =$

$= \mathrm{NWD}(5a+3b, 3a+2b) = \mathrm{NWD}(3a+2b, 5a+3b-(3a+2b)) =$
$= \mathrm{NWD}(3a+2b, 2a+b) = \mathrm{NWD}(2a+b, 3a+b-(2a+b)) =$
$= \mathrm{NWD}(2a+b, a) = \mathrm{NWD}(a, 2a+b-2a) = \mathrm{NWD}(a,b)$, co kończy dowód.

Zadanie 22.216. Oznaczmy $d = \mathrm{NWD}(a,b)$. Wtedy istnieją względnie pierwsze liczby naturalne x i y takie, że $a = dx$ i $b = dy$. Stąd $a^n = d^n x^n$ i $b^n = d^n y^n$. Wobec tego z twierdzenia 8.46, $\mathrm{NWD}(a^n, b^n) = d^n \cdot \mathrm{NWD}(x^n, y^n)$. Jeśli liczby x^n i y^n nie są względnie pierwsze, to istnieje liczba pierwsza p taka, że $p \mid x^n$ i $p \mid y^n$, skąd $p \mid x$ i $p \mid y$, co przeczy temu, że $\mathrm{NWD}(x,y) = 1$. Wobec tego $\mathrm{NWD}(x^n, y^n) = 1$ i $\mathrm{NWD}(a^n, b^n) = d^n = [\mathrm{NWD}(a,b)]^n$.

Zadanie 22.217. Będziemy szukali liczb naturalnych a, b, c takich, że $a+b+c, a+b, a+c, b+c$ są kwadratami liczb naturalnych i $a+b+c$ jest najmniejsze. Jeżeli $\mathrm{NWD}(a,b,c) > 1$, to istnieje liczba pierwsza p taka, że $p \mid a$ i $p \mid b$ i $p \mid c$. Ponadto $a+b = x^2$, $a+c = y^2$, $b+c = z^2$ i $a+b+c = K^2$ dla pewnych $x, y, z, K \in \mathbb{N}$, więc $p \mid x^2$ i $p \mid y^2$ i $p \mid z^2$ i $p \mid K^2$, skąd $p \mid x$ i $p \mid y$ i $p \mid z$ i $p \mid K$. Wobec tego $p^2 \mid a+b+c$ i $p^2 \mid a+b$, skąd $p^2 \mid c$. Podobnie pokazujemy, że $p^2 \mid a$ i $p^2 \mid b$. Zatem $a = p^2 a_1$, $b = p^2 b_1$ i $c = p^2 c_1$ dla pewnych $a_1, b_1, c_1 \in \mathbb{N}$, przy czym $a_1 + b_1 + c_1 = (\frac{K}{p})^2$, $a_1^2 + b_1^2 = (\frac{x}{p})^2$, $a_1^2 + c_1^2 = (\frac{y}{p})^2$, $b_1^2 + c_1^2 = (\frac{z}{p})^2$ oraz $a_1 + b_1 + c_1 < a+b+c$ i mamy sprzeczność z minimalnością $a+b+c$. Wobec tego liczby a, b, c są względnie pierwsze.

Po dodaniu stronami równości $a+b = x^2$, $a+c = y^2$, $b+c = z^2$ uzyskamy, że $x^2 + y^2 + z^2 = 2(a+b+c)$, ale $a+b+c = K^2$, więc $x^2 + y^2 + z^2 = 2K^2$. Ponadto $x^2, y^2, z^2 < K^2$, skąd $x, y, z < K$.

Załóżmy, że K jest parzyste. Wtedy $8 \mid x^2 + y^2 + z^2$, a ponieważ kwadraty liczb całkowitych dają z dzielenia przez 8 reszty 0, 1 lub 4, więc liczby x, y, z muszą być parzyste. Zatem $2 \mid a+b$ i $2 \mid a+c$ i $2 \mid b+c$ i $2 \mid a+b+c$, skąd liczby a, b, c są parzyste i mamy sprzeczność, bo $\mathrm{NWD}(a,b,c) = 1$. Wobec tego K jest liczbą nieparzystą. Stąd $[K^2]_8 = 1$ i $[2K^2]_8 = 2$, czyli $[x^2 + y^2 + z^2]_8 = 2$. Zatem dokładnie jedna z liczb x, y, z jest podzielna przez 4, a pozostałe są nieparzyste. Bez zmniejszania ogólności możemy dalej zakładać, że $4 \mid x$ i liczby y i z są nieparzyste.

Na odwrót, załóżmy, że K jest liczbą naturalną nieparzystą, $x, y, z \in \mathbb{N}$, $x, y, z < K$, $x^2 + y^2 + z^2 = 2K^2$ i liczby y, z są nieparzyste, a $4 \mid x$. Wtedy $a = K^2 - z^2, b = K^2 - y^2, c = K^2 - x^2 \in \mathbb{N}$, przy czym $a + b + c = 3K^2 - 2K^2 = K^2$, $a + b = 2K^2 - (y^2 + z^2) = x^2$, $a + c = 2K^2 - (x^2 + z^2) = y^2$ i $b + c = 2K^2 - (x^2 + y^2) = z^2$.

Ponieważ $4 \mid x$ i $x \in \mathbb{N}$, więc $x \geqslant 4$, skąd $K \geqslant 5$. Jeśli $K = 5$, to $x = 4$ oraz $y, z \leqslant 3$, skąd $x^2 + y^2 + z^2 \leqslant 16 + 2 \cdot 9 = 34 < 2 \cdot 5^2$ i mamy sprzeczność.

Jeśli $K = 7$, to też $x = 4$ oraz $y, z \leqslant 5$, skąd $x^2 + y^2 + z^2 \leqslant$ $\leqslant 16 + 2 \cdot 25 = 66 < 2 \cdot 7^2$ i też mamy sprzeczność.

Jeśli $K = 9$, to $x = 4$ lub $x = 8$ oraz $y, z \leqslant 7$, ale $4^2 + y^2 + z^2 \leqslant$ $\leqslant 16 + 2 \cdot 49 = 114 < 2 \cdot 9^2$, więc $x = 8$, skąd $y^2 + z^2 = 98$. Jeśli $y < 7$ lub $z < 7$, to $y^2 + z^2 < 2 \cdot 49 = 98$ i mamy sprzeczność. Zatem $y = z = 7$ oraz $a = b = 81 - 49 = 32$, co prowadzi do sprzeczności.

Jeśli $K = 11$, to $x = 4$ lub $x = 8$ oraz $y, z \leqslant 9$, skąd $x^2 + y^2 + z^2 \leqslant$ $\leqslant 64 + 2 \cdot 81 = 226 < 2 \cdot 11^2$ i mamy sprzeczność.

Jeśli $K = 13$, to $x = 4$ lub $x = 8$ lub $x = 12$ oraz $y, z \leqslant 11$, ale $y \neq z$, bo inaczej $a = b$, więc dla $x \leqslant 8$: $x^2 + y^2 + z^2 \leqslant 8^2 + 11^2 + 9^2 =$ $= 266 < 2 \cdot 13^2$. Zatem $x = 12$ i $y^2 + z^2 = 2 \cdot 13^2 - 12^2 = 194$. Jeśli $y, z < 11$, to $y^2 + z^2 \leqslant 2 \cdot 9^2 = 162 < 194$. Bez zmniejszania ogólności możemy zatem zakładać, że $y = 11$ i wtedy $z^2 = 194 - 121 = 73$, co prowadzi do sprzeczności.

Jeśli $K = 15$, to $x = 4$ lub $x = 8$ lub $x = 12$ oraz $y, z \leqslant 13$, ale wtedy $x^2 + y^2 + z^2 \leqslant 12^2 + 11^2 + 13^2 = 434 < 2 \cdot 15^2$ i mamy sprzeczność.

Jeśli $K = 17$, to $x = 4$ lub $x = 8$ lub $x = 12$ lub $x = 16$ oraz $y, z \leqslant 15$. Zatem dla $x \leqslant 12$, $x^2 + y^2 + z^2 \leqslant 12^2 + 13^2 + 15^2 = 538 < 2 \cdot 17^2$. Wobec tego $x = 16$ i $y^2 + z^2 = 2 \cdot 17^2 - 16^2 = 322$. Jeśli $y, z \leqslant 11$, to $y^2 + z^2 \leqslant 11^2 + 9^2 = 202 < 322$ i mamy sprzeczność. Zatem jedna z liczb y, z jest równa 13 lub 15, a kwadrat drugiej jest równy $322 - 13^2 = 153$ lub $322 - 15^2 = 97$ i też mamy sprzeczność.

Jeśli $K = 19$, to $x = 4$ lub $x = 8$ lub $x = 12$ lub $x = 16$ oraz $y, z \leqslant 17$. Jeśli $x \leqslant 12$, to $x^2 + y^2 + z^2 \leqslant 12^2 + 15^2 + 17^2 = 658 < 2 \cdot 19^2$ i mamy sprzeczność. Zatem $x = 16$ i $y^2 + z^2 = 2 \cdot 19^2 - 16^2 = 466$. Jeśli $y, z \leqslant 15$, to $y^2 + z^2 \leqslant 13^2 + 15^2 = 394 < 466$. Zatem jedna z liczb y, z

jest równa 17, a kwadrat drugiej jest równy $466 - 17^2 = 177$ i mamy sprzeczność.

Jeśli $K = 21$, to $x = 4$ lub $x = 8$ lub $x = 12$ lub $x = 16$ lub $x = 20$ oraz $y, z \leqslant 19$. Jeśli $x \leqslant 12$, to $x^2 + y^2 + z^2 \leqslant 12^2 + 17^2 + 19^2 = 794 < 2 \cdot 21^2$ i mamy sprzeczność. Zatem $x = 16$ lub $x = 20$. Jeśli $x = 16$, to $y^2 + z^2 = 2 \cdot 21^2 - 16^2 = 626$, ale wtedy dla $y, z \leqslant 17$ będzie $y^2 + y^2 < 600 < 626$, więc jedna z liczb y, z jest równa 19, a kwadrat drugiej wynosi $626 - 19^2 = 265$ i mamy sprzeczność. Wobec tego $x = 20$ i $y^2 + z^2 = 2 \cdot 21^2 - 20^2 = 482$. Stąd $y > 15$ lub $z > 15$. Możemy zakładać, że $z > 15$. Wtedy $z = 17$ i $y^2 = 482 - 17^2 = 193$, co prowadzi do sprzeczności lub $z = 19$ i $y^2 = 482 - 19^2 = 121$, skąd $y = 11$. Zatem $a = 21^2 - 19^2 = 80$, $b = 21^2 - 11^2 = 320$ i $c = 21^2 - 20^2 = 41$. Ponadto, $a + b = 400 = 20^2$, $a + c = 121 = 11^2$, $b + c = 361 = 19^2$ i $a + b + c = 441 = 21^2$.

Wobec tego szukanymi liczbami są: 41, 80, 320.

Zadanie 22.218. Załóżmy, że tak nie jest. Wtedy istnieje liczba naturalna $n > 1$ taka, że $1 + \frac{1}{2} + \ldots + \frac{1}{n}$ jest liczbą całkowitą. Z zasady maksimum istnieje największa liczba naturalna s taka, że $2^s \leqslant n$, gdyż $2 \leqslant n$ i $2^n > n$ dla $n \in \mathbb{N}$. Wtedy $n < 2^{s+1} = 2 \cdot 2^s$. Udowodnimy, że w ciągu $1, 2, \ldots, n$ dokładnie jeden wyraz jest podzielny przez 2^s. Ponieważ $2^s \leqslant n$, więc 2^s występuje w tym ciągu. Załóżmy, że istnieje inny wyraz tego ciągu podzielny przez 2^s. Wtedy jest on postaci $t \cdot 2^s$ dla pewnego naturalnego $t > 1$, skąd $t \geqslant 2$ i $t \cdot 2^s \geqslant 2^{s+1} > n$, co prowadzi do sprzeczności. Wobec tego 2^s jest jedynym wyrazem ciągu $1, 2, \ldots, n$ podzielnym przez 2^s.

Każda liczba naturalna k taka, że $2 \leqslant k \leqslant n$ może być zapisana w postaci $k = 2^u \cdot r$, gdzie $u \in \mathbb{N}_0$ i r jest liczbą naturalną nieparzystą. Ponadto $u \leqslant s$ i jeśli $u = s$, to $r = 1$. Oznaczmy przez S iloczyn wszystkich takich r. Wtedy każda z liczb ciągu $1, 2, \ldots, n$ oprócz liczby 2^s jest dzielnikiem liczby $2^{s-1}S$. Stąd liczba naturalna $2^{s-1}S \cdot (1 + \frac{1}{2} + \ldots + \frac{1}{n})$ jest sumą $n - 1$ liczb naturalnych postaci $\frac{2^{s-1}S}{k}$ dla $k \in \{1, 2, \ldots, n\} \setminus \{2^s\}$ i liczby $\frac{2^{s-1}S}{2^s} = \frac{S}{2}$, która nie jest całkowita, bo S jest liczbą nieparzystą jako iloczyn liczb nieparzystych. Otrzymaliśmy zatem sprzeczność.

Wobec tego nie istnieje liczba naturalna $n > 1$ taka, że $1+\frac{1}{2}+\ldots+\frac{1}{n}$ jest liczbą całkowitą.

Zadanie 22.219. Niech $k \in \mathbb{Z}$. Wtedy z twierdzenia o dzieleniu z resztą istnieją $q, r \in \mathbb{Z}$ takie, że $k = qp + r$ oraz $0 \leqslant r < p$. Stąd $k^2 - r^2 = (q^2p + 2qr)p$, więc $p \mid k^2 - r^2$ i z wniosku 2.31, $[k^2]_p = [r^2]_p$. Ponadto $(p-r)^2-r^2 = (p-2r)p$, więc z wniosku 2.31, $[(p-r)^2]_p = [r^2]_p$, ale p jest liczbą nieparzystą, więc $\frac{p-1}{2} \in \mathbb{N}$. Zatem dla $r = 1, 2, \ldots, \frac{p-1}{2}$ mamy, że $[(p-r)^2]_p = [r^2]_p$. Ponadto $p - \frac{p-1}{2} = \frac{p-1}{2} + 1$, więc wszystkie reszty z dzielenia kwadratów liczb całkowitych przez p są zawarte w zbiorze $\{[k^2]_p : k = 0, 1, \ldots, \frac{p-1}{2}\}$.

Weźmy dowolne $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$ takie, że $x < y$. Wtedy $y - x > 0$, więc $y - x \in \mathbb{N}$, przy czym $y - x \leqslant y \leqslant \frac{p-1}{2} < p$, a zatem $p \nmid y-x$. Ponadto $x+y > 0$, więc $x+y \in \mathbb{N}$ i $x+y < \frac{p}{2}+\frac{p}{2} = p$, skąd $p \nmid y+x$. Z pierwszości liczby p wynika stąd, że $p \nmid (y-x)(y+x)$, czyli $p \nmid y^2-x^2$. Z wniosku 2.31 wynika zatem, że $[y^2]_p \neq [x^2]_p$. Kończy to rozwiązanie naszego zadania.

Zadanie 22.220. Niech $x \in \mathbb{Z}$. Wtedy $2 \mid 2x^2$ i $2 \nmid 29$, więc $2 \nmid 2x^2+29$. Pozostaje zatem rozważyć liczby $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$. Z zadania 22.219, $x^2 = mp + r$ dla pewnych $m \in \mathbb{N}_0$ i $r \in \{[k^2]_p : k = 0, 1, \ldots, \frac{p-1}{2}\}$. Zatem $2x^2+29 = 2mp+2r+29$, skąd na mocy wniosku 2.31, $[2x^2 + 29]_p = [2r + 29]_p$.

Dla $p = 3$ mamy $r = 0, 1$, więc $[2x^2+29]_3 \in \{2, 1\}$, skąd $3 \nmid 2x^2+29$.

Dla $p = 5$ mamy $r = 0, 1, 4$, więc $[2x^2 + 29]_5 \in \{4, 1, 2\}$, skąd $5 \nmid 2x^2 + 29$.

Dla $p = 7$ mamy $r = 0, 1, 4, 2$, więc $[2x^2 + 29]_7 \in \{1, 3, 2, 5\}$, skąd $7 \nmid 2x^2 + 29$.

Dla $p = 11$: $r = 0, 1, 4, 9, 5, 3$, więc $[2x^2 + 29]_{11} \in \{7, 9, 4, 3, 6, 2\}$, skąd $11 \nmid 2x^2 + 29$.

Dla $p = 13$ mamy $r = 0, 1, 4, 9, 3, 12, 10$, więc $[2x^2 + 29]_{13} \in \{3, 5, 11, 8, 9, 1, 10\}$, skąd $13 \nmid 2x^2 + 29$.

Dla $p = 17$ mamy $r = 0, 1, 4, 9, 16, 8, 2, 15, 13$, więc $[2x^2 + 29]_{17} \in \{12, 14, 3, 13, 10, 11, 16, 8, 4\}$, skąd $17 \nmid 2x^2 + 29$.

Dla $p = 19$ mamy $r = 0, 1, 4, 9, 16, 6, 17, 11, 7, 5$, więc $[2x^2 + 29]_{19} \in \{10, 12, 18, 9, 4, 3, 6, 13, 5, 1\}$, skąd $19 \nmid 2x^2 + 29$.

Dla $p = 23$ mamy $r = 0, 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6$, więc $[2x^2 + 29]_{23} \in \{6, 8, 14, 1, 15, 10, 9, 12, 19, 7, 22, 18\}$, skąd $23 \nmid 2x^2 + 29$.

Zadanie 22.221. Załóżmy, że dla pewnego $x = 0, 1, \ldots, 28$ liczba $2x^2 + 29$ nie jest liczbą pierwszą. Wtedy z twierdzenia 9.10 posiada ona dzielnik pierwszy p taki, że $p^2 \leqslant 2x^2 + 29$. Ponieważ $2x^2 + 29 \leqslant$ $\leqslant 2 \cdot 28^2 + 29 = 1597 < 1600 = 40^2$, więc $p < 40$, skąd $p \leqslant 37$. Ponadto z zadania 22.220 wynika, że $p \geqslant 29$. Wobec tego $p \in \{29, 31, 37\}$, ale jeśli $29 \mid 2x^2 + 29$, to $29 \mid 2x^2$, skąd $29 \mid x$. Ponadto $x \leqslant 28$, więc $x = 0$, skąd $2x^2 + 29 = 29 \in \mathbb{P}$ i mamy sprzeczność.

Załóżmy, że $31 \mid 2x^2 + 29$. Wtedy $31 \mid 2x^2 + 29 - 31$, skąd 31 dzieli liczbę $2(x^2 - 1)$, a więc $31 \mid x^2 - 1$. Ponadto $x^2 - 1 = (x - 1)(x + 1)$ i $31 \in \mathbb{P}$, więc $31 \mid x - 1$ lub $31 \mid x + 1$, ale $x \in \{0, 1, \ldots, 28\}$, więc stąd $x = 1$ i $2x^2 + 29 = 31 \in \mathbb{P}$, co prowadzi do sprzeczności.

Załóżmy, że $37 \mid 2x^2 + 29$. Wtedy $37 \mid 2x^2 + 29 - 37$, skąd 37 dzieli liczbę $2(x^2 - 4)$, a więc $37 \mid x^2 - 4$. Ponadto $x^2 - 4 = (x - 2)(x + 2)$ i $37 \in \mathbb{P}$, więc $37 \mid x - 2$ lub $37 \mid x + 2$, ale $x \in \{0, 1, \ldots, 28\}$, więc stąd $x = 2$ i $2x^2 + 29 = 37 \in \mathbb{P}$, co prowadzi do sprzeczności.

Przypuszczenie, że pewna z liczb $2x^2 + 29$ dla $x \in \{0, 1, \ldots, 28\}$ nie jest liczbą pierwszą doprowadziło nas zatem do sprzeczności. Wobec tego $2x^2 + 29$ jest liczbą pierwszą dla każdego $x = 0, 1, \ldots, 28$.

Zadanie 22.222. Niech $x \in \mathbb{Z}$. Należy rozważyć liczby pierwsze

$$p \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}.$$

Z zadania 22.219, $x^2 = mp + r$ dla pewnych $m \in \mathbb{N}_0$ i $r \in \{[k^2]_p : k = 0, 1, \ldots, \frac{p-1}{2}\}$. Zatem $x^2 + 163 = mp + r + 163$, skąd na mocy wniosku 2.31, $[x^2 + 163]_p = [r + 169]_p$.

Dla $p = 3$ mamy $r = 0, 1$, więc $[x^2 + 169]_3 \in \{1, 2\}$, skąd $3 \nmid x^2 + 163$.

Dla $p = 5$ mamy $r = 0, 1, 4$, więc $[x^2 + 163]_5 \in \{3, 4, 2\}$, skąd $5 \nmid x^2 + 163$.

Dla $p = 7$ mamy $r = 0, 1, 4, 2$, więc $[x^2 + 163]_7 \in \{2, 3, 4, 4\}$, skąd $7 \nmid x^2 + 163$.

Dla $p = 11$: $r = 0, 1, 4, 9, 5, 3$, więc $[x^2 + 163]_{11} \in \{9, 10, 2, 7, 3, 1\}$, skąd $11 \nmid x^2 + 163$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Dla $p = 13$ mamy $r = 0, 1, 4, 9, 3, 12, 10$, więc $[x^2 + 163]_{13} \in \in \{7, 8, 11, 3, 10, 6, 4\}$, skąd $13 \nmid x^2 + 163$.

Dla $p = 17$ mamy $r = 0, 1, 4, 9, 16, 8, 2, 15, 13$, więc $[x^2 + 163]_{17} \in \in \{10, 11, 14, 2, 9, 1, 12, 8, 6\}$, skąd $17 \nmid x^2 + 163$.

Dla $p = 19$ mamy $r = 0, 1, 4, 9, 16, 6, 17, 11, 7, 5$, więc $[x^2 + 163]_{19} \in \{11, 12, 15, 1, 8, 17, 9, 3, 18, 16\}$, skąd $19 \nmid x^2 + 163$.

Dla $p = 23$ mamy $r = 0, 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6$, więc $[x^2 + 163]_{23} \in \{2, 3, 6, 11, 18, 4, 15, 5, 20, 14, 10, 8\}$, skąd $23 \nmid x^2 + 163$.

Dla $p = 29$ mamy $r = 0, 1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22$, więc $[x^2 + 163]_{29} \in \{18, 19, 22, 27, 5, 14, 25, 9, 24, 12, 2, 23, 17, 13, 11\}$, skąd $29 \nmid x^2 + 163$.

Dla $p = 31$ mamy $r = 0, 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8$, więc $[x^2 + 163]_{31} \in \{8, 9, 12, 17, 24, 2, 13, 26, 10, 27, 15, 5, 28, 22, 18, 16\}$, skąd $31 \nmid x^2 + 163$.

Dla $p = 37$ mamy $r = 0, 1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28$, więc$[x^2 + 163]_{37} \in \{15, 16, 19, 24, 31, 3, 14, 27, 5, 22, 4, 25, 11, 36, 26, 18, 12, 8, 6\}$, skąd $37 \nmid x^2 + 163$.

Zadanie 22.223. Dla $x \in \mathbb{Z}$ liczba $x^2 - x$ jest podzielna przez 2, gdyż jest iloczynem dwóch kolejnych liczb całkowitych. Stąd $2 \nmid \nmid x^2 - x + 41$ dla $x \in \mathbb{Z}$. Załóżmy, że dla pewnego $x = 1, \ldots, 40$ liczba $x^2 - x + 41$ nie jest liczbą pierwszą. Wtedy z twierdzenia 9.10 posiada ona dzielnik pierwszy p taki, że $p^2 \leqslant x^2 - x + 41$, ale $x \in \{1, \ldots, 40\}$, więc $p^2 \leqslant 40^2 - 40 + 41 = 1601 < 41^2$. Zatem $p < 41$ i p jest nieparzystą liczbą pierwszą. Ponadto $p \mid x^2 - x + 41$, więc $p \mid 4(x^2 - x + 41)$. Dodatkowo, $4(x^2 - x + 41) = (2x - 1)^2 + 163$, więc dla $y = 2x - 1$ mamy, że $y \in \mathbb{Z}$ i $p \mid y^2 + 163$, co przeczy zadaniu 22.222.

Wobec tego $x^2 - x + 41$ jest liczbą pierwszą dla $x = 1, \ldots, 40$.

Zadanie 22.224. Ponieważ $a^2 + b^2 = (a + b - c)^2$, więc $a^2 + b^2 = = a^2 + b^2 + c^2 + 2ab - 2ac - 2bc$, skąd $c^2 - 2ac - 2bc + 2ab = 0$. Jeśli $a + b - c = 0$, to $a^2 + b^2 = 0$, skąd $a = b = 0$ i $a + b - c = 0$, czyli $c = 0$, skąd $b = c = 0$ i mamy sprzeczność. Zatem $a + b - c \neq 0$. Ponadto, $2(a+b-c)(b-c) - [b^2 + (b-c)^2] = 2a(b-c) + 2(b-c)^2 - b^2 - (b-c)^2 = = 2a(b - c) + (b - c)^2 - b^2 = 2ab - 2ac + b^2 - 2bc + c^2 - b^2 =$

$= c^2 + 2ab - 2ac - 2bc = 0$, więc

$$b^2 + (b-c)^2 = 2(a+b-c)(b-c).$$

Podobnie, $2(a+b-c)(a-c) - [a^2 + (a-c)^2] = 2b(a-c) + 2(a-c)^2 - +a^2 - (a-c)^2 = 2ab - 2bc + (a-c)^2 - a^2 = 2ab - 2bc + a^2 - 2ac + c^2 - a^2 = = c^2 + 2ab - 2ac - 2bc = 0$, czyli

$$a^2 + (a-c)^2 = 2(a+b-c)(a-c).$$

Stąd oraz z tego, że $a+b-c \neq 0$ wynika, że $\frac{a^2+(a-c)^2}{b^2+(b-c)^2} = \frac{2(a+b-c)(a-c)}{2(a+b-c)(b-c)} = = \frac{a-c}{b-c}$.

Zadanie 22.225. Załóżmy, że tak nie jest. Wtedy istnieje liczba naturalna n taka, że $\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$ jest liczbą całkowitą. Z zasady maksimum istnieje największa liczba naturalna s taka, że $3^s \leqslant 2n+1$, gdyż $3 \leqslant 2n+1$ i $3^{2n+1} > 2^{2n+1} \geqslant 2n+1$ dla $n \in \mathbb{N}$. Wtedy $2n + +1 < 3^{s+1} = 3 \cdot 3^s$. Udowodnimy, że w ciągu $3, 5, \ldots, 2n+1$ dokładnie jeden wyraz jest podzielny przez 3^s. Ponieważ $3^s \leqslant 2n+1$ i liczba 3^s jest nieparzysta, więc 3^s występuje w tym ciągu. Załóżmy, że istnieje inny wyraz tego ciągu podzielny przez 3^s. Wtedy jest on postaci $t \cdot 3^s$ dla pewnego nieparzystego naturalnego $t > 1$, skąd $t \geqslant 3$ i $t \cdot 3^s \geqslant \geqslant 3^{s+1} > 2n+1$, co prowadzi do sprzeczności. Wobec tego 3^s jest jedynym wyrazem ciągu $3, 5, \ldots, 2n+1$ podzielnym przez 3^s.

Każda nieparzysta liczba naturalna k taka, że $3 \leqslant k \leqslant 2n+1$ może być zapisana w postaci $k = 3^u \cdot r$, gdzie $u \in \mathbb{N}_0$ i r jest nieparzystą liczbą naturalną niepodzielną przez 3. Ponadto $u \leqslant s$ i jeśli $u = s$, to $r = 1$. Oznaczmy przez S iloczyn wszystkich takich r. Wtedy każda z liczb ciągu $3, 5, \ldots, 2n+1$ oprócz liczby 3^s jest dzielnikiem liczby $3^{s-1}S$. Stąd liczba naturalna $3^{s-1}S \cdot (\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1})$ jest sumą $n-1$ liczb naturalnych postaci $\frac{3^{s-1}S}{k}$ dla $k \in \{3, 5, \ldots, 2n+1\} \setminus \{3^s\}$ i liczby $\frac{3^{s-1}S}{3^s} = \frac{S}{3}$, która nie jest całkowita, bo S jest liczbą niepodzielną przez 3 jako iloczyn liczb niepodzielnych przez 3. Otrzymaliśmy zatem sprzeczność.

Wobec tego nie istnieje liczba naturalna n taka, że $\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$ jest liczbą całkowitą.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zadanie 22.226. Załóżmy, że $a = n^p$ i $b = n^q$ dla pewnych $n, p, q \in \mathbb{N}$, $n > 1$. Wtedy $a > 1$ i ze wzoru na zamianę podstaw $\log_a b = \frac{\log_n n^q}{\log_n n^p} = \frac{q}{p} \in \mathbb{Q}$.

Na odwrót, załóżmy, że dla pewnych liczb naturalnych $a, b > 1$ liczba $\log_a b \in \mathbb{Q}$. Wtedy z własności logarytmów, $\log_a b > 0$. Zatem istnieją względnie pierwsze liczby naturalne q, p takie, że $\log_a b = \frac{q}{p}$. Stąd z definicji logarytmu, $a^{\frac{q}{p}} = b$. Zatem po podniesieniu tej równości do potęgi p mamy, że $a^q = b^p$. Z tej równości wynika, że liczby a i b mają identyczne zbiory dzielników pierwszych. Istnieją zatem różne liczby pierwsze $p_1, \ldots, p_s$ oraz istnieją liczby naturalne a_i, b_i dla $i = 1, \ldots, s$ takie, że $a = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$ i $b = p_1^{b_1} \cdot \ldots \cdot p_s^{b_s}$. Stąd $p_1^{qa_1} \cdot \ldots \cdot p_s^{qa_s} = p_1^{pb_1} \cdot \ldots \cdot p_s^{pb_s}$ i z twierdzenia o jednoznaczności rozkładu, $qa_i = pb_i$ dla $i = 1, \ldots, s$, ale liczby p i q są względnie pierwsze, więc z zasadniczego twierdzenia arytmetyki, $p \mid a_i$, skąd $a_i = pt_i$ dla pewnego $t_i \in \mathbb{N}$ oraz $b_i = qt_i$ dla każdego $i = 1, \ldots, s$. Zatem $n = p_1^{t_1} \cdot \ldots \cdot p_s^{t_s}$ jest liczbą naturalną większą od 1 i $a = n^p$ oraz $b = n^q$. Zauważmy, że $n > 1$ jest wspólnym dzielnikiem liczb a i b. Wobec tego, jeśli dodatkowo a i b są względnie pierwsze, to $\log_a b$ nie jest liczbą wymierną.

Zadanie 22.227. Jak wiemy $\sqrt{2}$ jest liczbą niewymierną (i oczywiście dodatnią). Jeśli $\sqrt{2}^{\sqrt{2}}$ jest liczbą wymierną, to wystarczy przyjąć $a = b = \sqrt{2}$. W przeciwnym przypadku dla $a = \sqrt{2}^{\sqrt{2}}$ i $b = \sqrt{2}$ mamy, że $a^b = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

Zadanie 22.228. Jak wiemy $a = \sqrt{2}$ jest liczbą niewymierną większą od 1. Ponadto z zadania 22.226 liczba $\log_2 3$ jest niewymierna oraz ze wzoru na zamianę podstaw $\log_{\sqrt{2}} 3 = \frac{\log_2 3}{\log_2 \sqrt{2}} = \frac{\log_2 3}{\frac{1}{2}} = 2 \cdot \log_2 3$, skąd wynika, że liczba $b = \log_{\sqrt{2}} 3$ jest niewymierna. Ponadto $b > 0$, bo $\sqrt{2} > 1$ i $3 > 1$ oraz z definicji logarytmu $a^b = 3$, czyli a^b jest liczbą wymierną.

Zadanie 22.229. Załóżmy, że 5555555 jest sumą dwóch liczb pierwszych. Ponieważ suma dwóch liczb nieparzystych jest liczbą parzystą, a liczba 5555555 jest nieparzysta, więc jedna z tych liczb pierwszych jest parzysta, ale jedyną parzystą liczbą pierwszą jest 2, więc

jedną z naszych liczb pierwszych jest liczba 2, zaś drugą jest liczba 5555553, której suma cyfr wynosi $6 \cdot 5 + 3 = 33 = 3 \cdot 11$, a to oznacza, że $3 \mid 5555553$. Ponieważ $5555553 > 1$, więc 5555553 nie jest liczbą pierwszą. Przypuszczenie, że liczba 5555555 jest sumą dwóch liczb pierwszych doprowadziło nas do sprzeczności. Wobec tego liczba 5555555 nie jest sumą dwóch liczb pierwszych.

Zadanie 22.230. Teza jest oczywista dla $k = 1$. Dla $k = 2$ mamy, że $n^4 + n^2 + 1 = (n^3 - 1)n + (n^2 + n + 1) = (n - 1)n(n^2 + n + 1) + (n^2+n+1) = (n^2+n+1)(n^2-n+1)$, więc też teza wówczas zachodzi. Niech dalej $k > 2$. Ponieważ $3 \nmid k$, więc $k = 3q + 1$ lub $k = 3q + 2$ dla pewnego $q \in \mathbb{N}$.

W pierwszym przypadku, $n^{2k} + n^k + 1 = n^{6q+2} + n^{3q+1} + 1 = (n^{6q} - 1)n^2 + (n^{3q} - 1)n + (n^2 + n + 1)$, a ponieważ $n^3 - 1 = (n - 1)(n^2 + n + 1)$ oraz $n^3 - 1 \mid n^{3q} - 1$ i $n^{3q} - 1 \mid n^{6q} - 1$ na mocy zadania 22.88, więc $n^2 + n + 1$ dzieli liczby $n^{6q} - 1$ i $n^{3q} - 1$, skąd wynika, że $n^2 + n + 1 \mid n^{2k} + n^k + 1$.

W drugim przypadku, $n^{2k} + n^k + 1 = n^{6q+4} + n^{3q+2} + 1 = (n^{6q}-1)n^4+(n^{3q}-1)n^2+(n^4+n^2+1)$ i na mocy pierwszej części dowodu $n^2+n+1 \mid n^4+n^2+1$ oraz $n^2+n+1 \mid n^{3q}-1$ i $n^2+n+1 \mid n^{6q}-1$, więc także $n^2 + n + 1 \mid n^{2k} + n^k + 1$.

Zadanie 22.231. Załóżmy, że $n^{2k} + n^k + 1$ jest liczbą pierwszą. Ponieważ $n^2+n+1 > 1$ i na mocy zadania 22.230, $n^2+n+1 \mid n^{2k}+n^k+1$, więc $n^2 + n + 1 = n^{2k} + n^k + 1$, ale dla $n > 1$ jest $n < n^k$ i $n^2 < n^{2k}$, więc stąd $n = 1$. Ponadto dla $n = 1$: $n^{2k} + n^k + 1 = 3 \in \mathbb{P}$. Wobec tego $n^{2k} + n^k + 1$ jest liczbą pierwszą jedynie dla $n = 1$.

Zadanie 22.232. Z zadania 22.90 mamy, że

$$10^{11} + 1 =$$

$$= (10+1) \cdot (10^{10} - 10^9 + 10^8 - 10^7 + 10^6 - 10^5 + 10^4 - 10^3 + 10^2 - 10 + 1).$$

Zatem $10^{11} + 1 = 11 \cdot 90909090901$. Naprzemienna suma cyfr liczby 90909090901 jest równa $1 - 9 + 0 - 9 + 0 - 9 + 0 - 9 + 0 - 9 + 0 - 9 = -44$, a więc jest podzielna przez 11. Stąd z cechy podzielności przez 11 liczba

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

90909090901 jest podzielna przez 11. Wobec tego $121 = 11^2$ dzieli liczbę $10^{11} + 1$.

Prosty rachunek pokazuje też, że $90909090901 = 11 \cdot 826446281$, czyli

$$10^{11} + 1 = 11^2 \cdot 826446281.$$

Zadanie 22.233. Niech $A = 826446281$. Wtedy z zadania 22.232, $10^{11}+1 = 11^2 \cdot A$. Ponadto $4^2 \cdot A = 13223140496$. Wtedy liczba powstająca z $a = 13223140496$ przez dopisanie do niej z lewej strony liczby a jest równa $1322314049613223140496 = a \cdot 10^{11} + a = a \cdot (10^{11} + 1) = = 4^2 \cdot A \cdot 11^2 \cdot A = (44 \cdot A)^2$, czyli jest kwadratem liczby naturalnej.

Zadanie 22.234. Załóżmy, że $10^s + 1$ nie jest podzielne przez kwadrat żadnej liczby pierwszej. Wówczas istnieją różne liczby pierwsze $p_1, \ldots, p_k$ takie, że $10^s + 1 = p_1 \cdot \ldots \cdot p_k$. Ponadto $\overline{aa} = K^2$ dla pewnego $K \in \mathbb{N}$ oraz $\overline{aa} = a \cdot 10^s + a = a \cdot (10^s + 1) = a \cdot p_1 \cdot \ldots \cdot p_k$. Zatem $a \cdot p_1 \cdot \ldots \cdot p_k = K^2$. Stąd dla $i = 1, \ldots, k$ mamy, że $p_i \mid K^2$, skąd $p_i \mid K$, ale liczby pierwsze $p_1, \ldots, p_k$ są parami różne, więc $p_1 \cdot \ldots \cdot p_s \mid K$, czyli $K = t \cdot p_1 \cdot \ldots \cdot p_k$ dla pewnego $t \in \mathbb{N}$. Wobec tego $t^2 \cdot p_1^2 \cdot \ldots \cdot p_k^2 = a \cdot p_1 \cdot \ldots \cdot p_k$ i po skróceniu, $a = t \cdot p_1 \cdot \ldots \cdot p_k$, ale $p_1 \cdot \ldots \cdot p_k = 10^s + 1$, więc $a = t \cdot (10^s + 1) \geqslant 10^s + 1 > 10^s$, co przeczy temu, że a jest liczbą s-cyfrową.

Przypuszczenie, że $10^s + 1$ nie dzieli się przez kwadrat liczby pierwszej doprowadziło nas zatem do sprzeczności. Wobec tego $10^s + 1$ musi być podzielne przez kwadrat liczby pierwszej.

Uwaga. Okazuje się, że najmniejszą liczbą naturalną s, dla której $10^s + 1$ jest podzielne przez kwadrat liczby pierwszej jest liczba $s = 11$. Można to sprawdzić na przykład dzięki programowi z internetu na rozkładanie liczb naturalnych na czynniki pierwsze. Mamy kolejno: $11 = 11$, $101 = = 101$, $1001 = 7 \cdot 11 \cdot 13$, $10^4 + 1 = 73 \cdot 137$, $10^5 + 1 = 11 \cdot 9091$, $10^6 + 1 = 101 \cdot 9901$, $10^7 + 1 = 11 \cdot 909091$, $10^8 + 1 = 17 \cdot 5882353$, $10^9 + 1 = 7 \cdot 11 \cdot 13 \cdot 19 \cdot 52579$, $10^{10} + 1 = 101 \cdot 3541 \cdot 27961$, $10^{11} + 1 = = 11^2 \cdot 23 \cdot 4093 \cdot 8779$.

Niech teraz a będzie liczbą 11-to cyfrową o tej własności, że po dopisaniu do niej z lewej strony liczby a uzyskamy kwadrat liczby naturalnej, to znaczy $\overline{aa} = K^2$ dla pewnego $K \in \mathbb{N}$. Wtedy $K^2 = a \cdot 10^{11} + a = a \cdot (10^{11} + 1) = a \cdot 11^2 \cdot 23 \cdot 4093 \cdot 8779$. Ponieważ 11, 23, 4093 i 8779 są różnymi liczbami pierwszymi, więc rozumując podobnie jak w rozwiązaniu zadania 22.234 uzyskamy, że $K = t \cdot 11 \cdot 23 \cdot 4093 \cdot 8779$, skąd $a = t \cdot 23 \cdot 4093 \cdot 8779 = t^2 \cdot 826446281$, ale $9 \cdot 826446281 = 7438016529$ jest liczbą 10-cio cyfrową, więc najmniejsze $a = 4^2 \cdot 826446281 = 13223140496$. Wobec tego 13223140496 jest najmniejszą liczbą spełniającą warunki zadania 22.234!.

Zadanie 22.235. Niech $x, y \in \mathbb{Z}$ będą takie, że $x + y = (x - y)^2$. Oznaczmy $t = x - y$. Wtedy $t \in \mathbb{Z}$ i $x = t + y$ oraz $t + 2y = t^2$, skąd $y = \frac{t^2 - t}{2}$. Ponadto $x = t + \frac{t^2 - t}{2} = \frac{t^2 + t}{2}$.

Na odwrót, dla dowolnego $t \in \mathbb{Z}$ liczby $t^2 - t = (t - 1)t$ i $t^2 + t = t(t + 1)$ są podzielne przez 2 jako iloczyny dwóch kolejnych liczb całkowitych. Stąd $x = \frac{t^2 + t}{2} \in \mathbb{Z}$ i $y = \frac{t^2 - t}{2} \in \mathbb{Z}$ oraz $x + y = t^2$ i $x - y = t$, więc $x + y = (x - y)^2$.

Wobec tego: $x = \frac{t^2 + t}{2}$ i $y = \frac{t^2 - t}{2}$ dla dowolnego $t \in \mathbb{Z}$.

Zadanie 22.236. Załóżmy, że $2x^2 - 5y^2 = 6$ dla pewnych $x, y \in \mathbb{Z}$. Wtedy y jest parzyste, więc $y = 2t$ dla pewnego $t \in \mathbb{Z}$ oraz $2x^2 - 5 \cdot 4t^2 = 6$, skąd $x^2 = 10t^2 + 3$. Wobec tego $[x^2]_5 = 3$, ale $[0^2]_5 = 0$, $[1^2]_5 = 1$, $[2^2]_5 = 4$, $[3^2]_5 = [9]_5 = 4$ i $[4^2]_5 = [16]_5 = 1$, więc $[x^2]_5 \in \{0, 1, 4\}$, a zatem doszliśmy do sprzeczności.

Zadanie 22.237. Weźmy dowolne $x, y \in \mathbb{Z}$ takie, że $3^x - 2^y = 1$. Jeśli $x \leqslant 0$, to $3^x - 2^y < 3^x \leqslant 1$, więc $3^x - 2^y \neq 1$. Zatem $x > 0$, czyli $x \in \mathbb{N}$. Stąd $2^y = 3^x - 1 \geqslant 3 - 1 = 2$, a zatem $y \geqslant 1$, czyli $y \in \mathbb{N}$.

Jeśli $x = 1$, to $2^y = 2$, skąd $y = 1$. Jeśli $x = 2$, to $2^y = 8 = 2^3$, skąd $y = 3$. Niech dalej $x > 2$. Wtedy $y > 1$ i $2^y = 3^x - 1 = (3 + 1) \cdot (3^{x-1} + 3^{x-2} + \ldots + 3 + 1)$, czyli $2^{y-1} = 3^{x-1} + 3^{x-2} + \ldots + 3 + 1$, ale $y > 1$, więc lewa strona tego wzoru jest parzysta. Zatem także prawa jego strona musi być liczbą parzystą, a ponieważ jest ona sumą x liczb nieparzystych, to $x = 2t$ dla pewnego $t \in \mathbb{N}$, przy czym $t > 1$, bo $x > 2$. Wobec tego $2^y = 3^{2t} - 1 = (3^t - 1)(3^t + 1)$ i istnieją liczby naturalne a i b takie, że $y = a + b$ oraz $3^t - 1 = 2^a$ oraz $3^t + 1 = 2^b$, skąd $b > a$.

Po odjęciu stronami uzyskamy, że $2 = 2^b - 2^a$, skąd $2^a \mid 2$, więc $a = 1$ i $2 = 2^b - 2$, skąd $b = 2$. Zatem $y = 1 + 2 = 3$ i $3^x = 1 + 2^3 = 3^2$, czyli $x = 2$ i mamy sprzeczność.

Podsumowując: $x = y = 1$ lub $x = 2$ i $y = 3$.

Zadanie 22.238. Niech $x, y \in \mathbb{Z}$. Wtedy na mocy zadania 22.93 mamy, że $x^3 + y^3 + 1 - 3xy = (x + y + 1) \cdot (x^2 + y^2 + 1 - x - y - xy)$. Wobec tego $x^3 + y^3 + 1 = 3xy$ wtedy i tylko wtedy, gdy $x + y + 1 = 0$ lub $x^2 + y^2 + 1 - x - y - xy = 0$. Ponadto $2(x^2 + y^2 + 1 - x - y - xy) = (x - y)^2 + (x - 1)^2 + (y - 1)^2$, więc $x^2 + y^2 + 1 - x - y - xy = 0$ wtedy i tylko wtedy, gdy $x = y = 1$.

Podsumowując widzimy, że wszystkimi rozwiązaniami w liczbach całkowitych równania $x^3 + y^3 + 1 = 3xy$ są $x = y = 1$ oraz $x \in \mathbb{Z}$ i $y = -x - 1$.

Zadanie 22.239. Załóżmy, że $2x^2 - 4x - 5y^2 - 10y = 10$ dla pewnych $x, y \in \mathbb{Z}$. Wtedy $5y^2$ jest liczbą parzystą, więc y jest parzyste i $y = 2t$ dla pewnego $t \in \mathbb{Z}$. Stąd $2x^2 - 4x - 20t^2 - 20t = 10$, czyli $x^2 - 2x - 10t^2 - 10t = 5$. Zatem $(x-1)^2 - 1 = 10(t^2+t)+5$, skąd $(x-1)^2 = 10(t^2+t)+6$. Stąd $x - 1$ jest parzyste, czyli $x - 1 = 2u$ dla pewnego $u \in \mathbb{Z}$ i $4u^2 = 10(t^2 + t) + 6$. Zatem $2u^2 = 5(t^2 + t) + 3$, ale $t^2 + t = t(t + 1)$ jest iloczynem dwóch kolejnych liczb całkowitych, więc $t^2 + t$ jest liczbą parzystą i $3 = 2u^2 - 5(t^2 + t)$, skąd 3 jest liczbą parzystą. Otrzymana sprzeczność pokazuje, że nie istnieją $x, y \in \mathbb{Z}$, które spełniają podane równanie.

Zadanie 22.240. Niech $x, y \in \mathbb{Z}$ i $\frac{1}{x^2} + \frac{1}{xy} + \frac{1}{y^2} = 1$. Wtedy $x, y \neq 0$ i po pomnożeniu obu stron tego równania przez x^2y^2 otrzymamy równanie równoważne:

$$x^2 + xy + y^2 = x^2y^2.$$

Niech $d = \mathrm{NWD}(x, y)$. Wtedy istnieją względnie pierwsze liczby całkowite u i v takie, że $x = du$ i $y = dv$ oraz $d^2u^2 + d^2uv + d^2v^2 = d^4u^2v^2$, skąd $u^2 + uv + v^2 = d^2u^2v^2$. Wobec tego $v \mid u^2$ i z zasadniczego twierdzenia arytmetyki $v \mid 1$, czyli $v = \pm 1$, więc $v^2 = 1$. Podobnie, $u \mid v^2$, więc $u \mid 1$, skąd $u = \pm 1$ i $u^2 = 1$. Zatem $2 + uv = d^2$ i $u = \pm 1$ i $v = \pm 1$.

Stąd $d = 1$ oraz $u = 1$ i $v = -1$ lub $u = -1$ i $v = 1$. Wobec tego $x = 1$ i $y = -1$ lub $x = -1$ i $y = 1$. Ponadto $1^2+1\cdot(-1)+(-1)^2 = 1^2\cdot(-1)^2$, więc wszystkimi rozwiązaniami równania $\frac{1}{x^2} + \frac{1}{xy} + \frac{1}{y^2} = 1$ w liczbach całkowitych x i y są: $x = 1$ i $y = -1$ oraz $x = -1$ i $y = 1$.

Zadanie 22.241. Ponieważ $(x+4y)(2x-3y) = 2x^2-3xy+8xy-$ $+12y^2 = x^2+5xy-12y^2$, więc nasze równanie można zapisać w postaci:

$$(x + 4y)(2x - 3y) = 28.$$

Ponieważ $x, y \in \mathbb{N}$, więc stąd $2x - 3y > 0$. Ponadto $x + 4y \geqslant 5$, więc $x + 4y$ jest dzielnikiem 28 większym od 4, zaś $2x - 3y$ jest dzielnikiem dopełniającym, ale $D_{28} = \{1, 28; 2, 14; 4, 7\}$, więc $x+4y = 4$ i $2x-3y =$ $= 7$ lub $x + 4y = 14$ i $2x - 3y = 2$ lub $x + 4y = 28$ i $2x - 3y = 1$. Stąd po prostych rachunkach otrzymamy, że $x = 8$ i $y = 5$.

Zadanie 22.242. Dla $n = 1$: $n^8 + n^6 + n^4 + n^2 + 1 = 5 \in \mathbb{P}$. Niech dalej $n > 1$, $n \in \mathbb{N}$ będzie takie, że $n^8 + n^6 + n^4 + n^2 + 1$ jest liczbą pierwszą. Ponieważ $n^{10}-1 = (n^5-1)(n^5+1)$ oraz $n^{10}-1 = (n^2-1)(n^8+$ $+n^6+n^4+n^2+1)$, więc $(n^5-1)(n^5+1) = (n^2-1)(n^8+n^6+n^4+n^2+1)$, ale $n^5-1 = (n-1)(n^4+n^3+n^2+n+1)$, $n^5+1 = (n+1)(n^4-n^3+n^2-$ $+n+1)$ i $n^2-1 = (n-1)(n+1)$, więc po skróceniu: $n^8+n^6+n^4+n^2+1 =$ $= (n^4+n^3+n^2+n+1)(n^4-n^3+n^2-n+1)$. Zatem $n^4+n^3+n^2+n+1$ jest dzielnikiem liczby pierwszej $n^8 + n^6 + n^4 + n^2 + 1$ większym od 1, skąd $n^4+n^3+n^2+n+1 = n^8+n^6+n^4+n^2+1$, ale $n > 1$, więc $n^2 > n$, $n^4 > n^2$, $n^6 > n^3$ i $n^8 > n^4$, skąd $n^8+n^6+n^4+n^2+1 > n^4+n^3+n^2+n+1$ i mamy sprzeczność. Zatem ostatecznie: $n = 1$.

Zadanie 22.243. Niech $x, y \in \mathbb{Z}$ będą takie, że $x+y = 5$ i $2^x+3^y =$ $= 17$. Ponieważ $2^x, 3^y > 0$ i funkcje $x \mapsto 2^x$ oraz $y \mapsto 3^y$ są rosnące i $2^5 > 17$ oraz $3^3 > 17$, więc $x \leqslant 4$ i $y \leqslant 2$. Stąd $5 - x \leqslant 2$, czyli $x \geqslant 3$. Wobec tego $x = 3$ lub $x = 4$. Jeśli $x = 3$, to $3^y = 9 = 3^2$ i $y = 2$. Jeśli $x = 4$, to $3^y = 1$, skąd $y = 0$, lecz wtedy $x + y = 4 \neq 5$. Wobec tego ostatecznie $x = 3$ i $y = 2$.

Zadanie 22.244. Zastosujemy indukcję względem n. Dla $n = 2$: $2^n = 4 > 3 = n + 1$. Załóżmy, że dla pewnego naturalnego $k \geqslant 2$ jest $2^k > k+1$. Wtedy $2\cdot 2^k > 2\cdot(k+1)$, czyli $2^{k+1} > 2k+2 = k+2+k \geqslant k+2$,

czyli $2^{k+1} > (k+1)+1$ i dowodzona nierówność zachodzi dla $n = k+1$. Stąd na mocy zasady indukcji matematycznej $2^n > n+1$ dla każdego $n = 2, 3, \ldots$.

Zadanie 22.245. Niech $x, y \in \mathbb{N}$. Jeśli $y = 1$, to $x^y = xy$. Jeśli $y = 2$, to $x^y = xy \iff x^2 = 2x \iff x = 2$. Niech dalej $y \geqslant 3$. Wtedy $x^y = xy \iff x^{y-1} = y$, ale dla $x \geqslant 2$ mamy $x^{y-1} \geqslant 2^{y-1} > y$ na mocy zadania 22.244 i $1^{y-1} = 1 < y$, więc dla $y > 2$ nie istnieje $x \in \mathbb{N}$ takie, że $x^y = xy$.

Podsumowując: $x = y = 2$ lub $y = 1$ i x jest dowolną liczbą naturalną.

Zadanie 22.246. Niech $x, y \in \mathbb{N}$. Jeśli $x = y$, to $x^y = y^x$. Załóżmy dalej, że $x < y$. Wtedy $x^x \mid x^y$, skąd $x^x \mid y^x$. Zatem z twierdzenia 8.52, $x \mid y$, czyli $y = tx$ dla pewnego $t \in \mathbb{N}$ takiego, że $t > 1$, bo $y > x$. Stąd $x^{tx} = y^x$, a zatem $x^t = y$, czyli $x^t = tx$. Z zadania 22.245 i tego, że $t > 1$ wynika, że $x = t = 2$. Stąd $y = 4$. Ponadto $4^2 = 2^4$.

Podsumowując: $x = y$ lub $x = 2$ i $y = 4$ lub $x = 4$ i $y = 2$.

Zadanie 22.247. Niech $x_1 = y_1 = 1$ i dla $n \in \mathbb{N}$ niech $x_{n+1} = 2x_n + 3y_n$ oraz $y_{n+1} = 3x_n + 5y_n$. Wtedy $x_n, y_n \in \mathbb{N}$ i $x_n < x_{n+1}$ dla każdego $n \in \mathbb{N}$. Zatem mamy nieskończenie wiele par (x_n, y_n) liczb naturalnych. Ponadto $x_1^2 + x_1y_1 - y_1^2 = 2 - 1 = 1$ oraz jeżeli dla pewnego naturalnego k jest $x_k^2 + x_ky_k - y_k^2 = 1$. Wtedy dla $n = k+1$ mamy $x_n^2 + x_ny_n - y_n^2 = (2x_k + 3y_k)^2 + (2x_k + 3y_k)(3x_k + 5y_k) - (3x_k + 5y_k)^2 = 4x_k^2 + 12x_ky_k + 9y_k^2 + 6x_k^2 + 19x_ky_k + 15y_k^2 - (9x_k^2 + 30x_ky_k + 25y_k^2) = x_k^2 + x_ky_k - y_k^2 = 1$. Wobec tego na mocy zasady indukcji matematycznej $x_n^2 + x_ny_n - y_n^2 = 1$ dla każdego $n \in \mathbb{N}$.

Zadanie 22.248. Mamy: $9 = (x + \frac{1}{x})^2 = x^2 + 2x \cdot \frac{1}{x} + \frac{1}{x^2}$, skąd $x^2 + \frac{1}{x^2} = 7$. Dalej, $x^3 + \frac{1}{x^3} = (x + \frac{1}{x})(x^2 + \frac{1}{x^2}) - (x + \frac{1}{x}) = 3 \cdot 7 - 3 = 18$. W końcu, $x^5 + \frac{1}{x^5} = (x^2 + \frac{1}{x^2})(x^3 + \frac{1}{x^3}) - (x^2 + \frac{1}{x^2}) = 7 \cdot 18 - 7 = 119$. Wobec tego $x^5 + \frac{1}{x^5} = 119$.

Zadanie 22.249. Ponieważ $a + b = 1$, więc $1 = (a+b)^3 = a^3 + b^3 + 3ab(a+b) = a^3 + b^3 + 3ab$, skąd $3ab = 1 - (a^3 + b^3)$. Zatem $3ab \in \mathbb{Q}$, skąd $ab = \frac{1}{3} \cdot (3ab) \in \mathbb{Q}$. Wobec tego $1 - ab \in \mathbb{Q}$. Dalej, $1 - ab = 1 - a(1-a) = 1 - a + a^2 = (a - \frac{1}{2})^2 + \frac{3}{4} > 0$ oraz $1 + a^3 = (1+a)(1 - a + a^2)$,

więc $1+a=\frac{1+a^3}{1-a+a^2}$, skąd $1+a\in\mathbb{Q}$. Zatem $a=(1+a)-1\in\mathbb{Q}$ oraz $b=1-a\in\mathbb{Q}$.

Zadanie 22.250. Ponieważ $x^2-1\in\mathbb{Z}$, więc też $x^2=(x^2-1)+1\in\in\mathbb{Z}$. Jeśli $x^2=0$ lub $x^2=1$, to $x=0$ lub $x=\pm1$, więc $x\in\mathbb{Z}$. Niech dalej $x^2\neq0$ i $x^2\neq1$. Zatem $x^2>0$ i $x^2\in\mathbb{Z}$, czyli $x^2\in\mathbb{N}$ oraz $x^2>1$, więc $x^4>1$ oraz $x^4-1\in\mathbb{Z}$, a zatem $x^4-1\in\mathbb{N}$. Dalej, $x^5-x=x(x^4-1)$ oraz $x^5-x\in\mathbb{Z}$, więc $x=\frac{x^5-x}{x^4-1}\in\mathbb{Q}$. Wobec tego istnieją względnie pierwsze liczby całkowite p i q takie, że $q>0$ i $x=\frac{p}{q}$, ale $x^2\in\mathbb{Z}$, więc $\frac{p^2}{q^2}\in\mathbb{Z}$, skąd $q^2\mid p^2$. Ponadto liczby p^2 i q^2 też są względnie pierwsze, więc $q^2=1$, skąd $q=1$, bo $q>0$. Wobec tego $x=p$, czyli $x\in\mathbb{Z}$.

Zadanie 22.251. Z twierdzenia 8.45 i z zadania 22.160 mamy, że $9\cdot\mathrm{NWD}(\underbrace{11\ldots1}_{n},\ \underbrace{11\ldots1}_{m})=\mathrm{NWD}(\underbrace{99\ldots9}_{n},\ \underbrace{99\ldots9}_{m})=$ $=\mathrm{NWD}(10^n-1,10^m-1)=10^{\mathrm{NWD}(n,m)}-1$, skąd po podzieleniu przez 9 uzyskamy tezę.

Zadanie 22.252. Niech (p_n) będzie rosnącym ciągiem wszystkich liczb pierwszych. Wtedy dla dowolnych różnych liczb naturalnych n i m mamy, że $\mathrm{NWD}(p_n,p_m)=1$. Wobec tego na mocy zadania 22.251 liczby $\underbrace{11\ldots1}_{p_n}$ i $\underbrace{11\ldots1}_{p_m}$ są względnie pierwsze. Kończy to rozwiązanie naszego zadania.

Zadanie 22.253. Teza jest oczywista dla $n=1$. Niech dalej $n>1$. Z dwumianu Newtona wynika, że $(1+n)^n=1+\binom{n}{1}n+k\cdot n^2$ dla pewnego $k\in\mathbb{N}$. Zatem $(n+1)^n-1=(k+1)\cdot n^2$, skąd $n^2\mid(n+1)^n-1$.

Zadanie 22.254. Zastosujemy indukcję ze względu na n. Dla $n=1$: $(n+1)\cdot\ldots\cdot(n+n)=2$ i $2^n=2$, więc teza zachodzi. Załóżmy, że $2^k\mid(k+1)\cdot(k+2)\cdot\ldots\cdot(k+k)$ dla pewnego $k\in\mathbb{N}$. Wtedy dla $n=k+1$: $(n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)=(k+2)\cdot(k+3)\cdot\ldots\cdot(2k+2)=$ $=(k+2)\cdot(k+3)\cdot\ldots\cdot2k\cdot(2k+1)\cdot(2k+2)$, ale $2k+2=2(k+1)$ oraz $(k+1)\cdot(k+2)\cdot\ldots\cdot(k+k)=2^k\cdot t$ dla pewnego $t\in\mathbb{Z}$, więc $(n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)=2^k\cdot t\cdot(2k+1)\cdot2=2^{k+1}t(2k+1)$, skąd wynika, że $2^n\mid(n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)$ dla $n=k+1$.

Stąd na mocy zasady indukcji matematycznej mamy, że $2^n \mid (n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)$ dla każdego $n \in \mathbb{N}$.

Zadanie 22.255. Niech $n, x \in \mathbb{N}$. Wtedy $4^n + 65 = x^2 \iff 65 = x^2 - (2^n)^2 \iff 65 = (x-2^n)\cdot(x+2^n)$, ale $x + 2^n > x - 2^n$ oraz $D_{65} = \{1, 5, 13, 65\}$, więc $x + 2^n = 13$ i $x - 2^n = 5$ lub $x + 2^n = 65$ i $x - 2^n = 1$.

W pierwszym przypadku po odjęciu stronami $2 \cdot 2^n = 8 = 2^3$, skąd $n = 2$ oraz $x = 2^2 + 5 = 9$. Natomiast w drugim przypadku, $2 \cdot 2^n = 64$, czyli $2^{n+1} = 2^6$, skąd $n + 1 = 6$ i $n = 5$ oraz $x = 2^5 + 1 = 33$.

Ponadto: $4^2 + 65 = 81 = 9^2$ i $4^5 + 65 = 1089 = 33^2$. Wobec tego ostatecznie: $n = 2$ lub $n = 5$.

Zadanie 22.256. Załóżmy, że dla pewnych $n, k \in \mathbb{N}$ jest $n^4 + 2n^3 + 2n^2 + 2n + 1 = k^2$. Ponieważ $(n^2+n+1)^2 = n^4 + n^2 + 1 + 2n^3 + 2n^2 + 2n$, więc $k^2 < (n^2 + n + 1)^2$, skąd $k < n^2 + n + 1$. Ponadto, $(n^2 + n)^2 = n^4 + 2n^3 + n^2 < n^4 + 2n^3 + 2n^2 + 2n + 1 = k^2$, więc $n^2 + n < k$. Zatem $n^2 + n < k < n^2 + n + 1$, a ponieważ $n^2 + n, n^2 + n + 1 \in \mathbb{N}$, więc mamy sprzeczność.

Wobec tego dla każdej liczby naturalnej n liczba $n^4 + 2n^3 + 2n^2 + 2n + 1$ nie jest kwadratem liczby naturalnej.

Zadanie 22.257. Mamy: $n^2 + 8n - 65 = (n+4)^2 - 16 - 85 = (n+4)^2 - 101$, więc $101 \mid n^2 + 8n - 65 \iff 101 \mid (n+4)^2$, ale, jak wiemy, 101 jest liczbą pierwszą, więc $101 \mid n + 4$, czyli $[n]_{101} = 97$. Wobec tego $101 \mid n^2 + 8n - 65$ wtedy i tylko wtedy, gdy $n = 101k + 97$ dla pewnego $k \in \mathbb{N}_0$.

Zadanie 22.258. Mamy: $b^2 = a^2 + c \iff c = b^2 - a^2 \iff c = (b-a)(b+a)$, ale $c \in \mathbb{P}$ i $b + a > 1$, więc stąd $b + a = c$ i $b - a = 1$. Suma liczb nieparzystych większych od 1 jest liczbą parzystą większą od 2, czyli nie może być liczbą pierwszą. Stąd a lub b jest parzyste, ale jedyną parzystą liczbą pierwszą jest 2, więc $a = 2$ lub $b = 2$. Gdy $b = 2$, to $a = 1 \notin \mathbb{P}$. Jeśli zaś $a = 2$, to $b = 3 \in \mathbb{P}$ i $c = 2 + 3 = 5 \in \mathbb{P}$. Ponadto $2^2 + 5 = 9 = 3^2$. Wobec tego ostatecznie: $a = 2$, $b = 3$ i $c = 5$.

Zadanie 22.259. Dla $n \in \mathbb{N}$ mamy, $n^4 + 4 = n^4 + 4n^2 + 4 -$

$+4n^2 = (n^2+2)^2 - (2n)^2 = (n^2+2-2n)(n^2+2n+2)$. Załóżmy, że $p = \frac{n^4+4}{17} \in \mathbb{P}$. Wtedy $17 \mid n^4+4$, czyli $17 \mid (n^2+2n+2)(n^2-2n+2)$, ale 17 jest liczbą pierwszą, więc $17 \mid n^2+2n+2$ lub $17 \mid n^2-2n+2$. W pierwszym przypadku $n > 1$ i $p = \frac{n^2+2n+2}{17} \cdot (n^2-2n+2)$ oraz $n^2-2n+2 = (n-1)^2+1 > 1$, więc z pierwszości p, $n^2-2n+2 = p$ oraz $\frac{n^2+2n+2}{17} = 1$. Stąd $n^2+2n+2 = 17$, czyli $(n+1)^2+1 = 17$, a zatem $(n+1)^2 = 16$, skąd $n+1 = 4$ i $n = 3$. Ponadto dla $n = 3$: $p = 1 \cdot (3^2 - 2 \cdot 3 + 2) = 5 \in \mathbb{P}$.

W drugim przypadku, $n > 1$ i $p = \frac{n^2-2n+2}{17} \cdot (n^2+2n+2)$ oraz $n^2+2n+2 > 1$, więc z pierwszości p, $n^2+2n+2 = p$ oraz $\frac{n^2-2n+2}{17} = 1$. Stąd $n^2-2n+2 = 17$, czyli $(n-1)^2+1 = 17$, a zatem $(n-1)^2 = 16$, skąd $n-1 = 4$ i $n = 5$. Ponadto dla $n = 5$: $p = 1 \cdot (5^2 + 2 \cdot 5 + 2) = 37 \in \mathbb{P}$.

Ostatecznie więc: $n = 3$ lub $n = 5$.

Zadanie 22.260. Dla $n \in \mathbb{N}$ mamy, że $n^4+4 = (n^2-2n+2) \cdot (n^2+2n+2)$, więc $17 \mid n^4+4$ wtedy i tylko wtedy, gdy $17 \mid n^2-2n+2$ lub $17 \mid n^2+2n+2$.

Zauważmy, że $n^2-2n+2 = (n-1)^2+1$, więc warunek $17 \mid n^2-2n+2$ jest równoważny temu, że $17 \mid (n-1)^2+1$, a ten z kolei jest równoważny warunkowi $17 \mid (n-1)^2+1-17$, który można zapisać w postaci $17 \mid (n-1)^2-16$. Ponadto, $(n-1)^2-16 = (n-1)^2-4^2 = (n-1-4)(n-1+4) = (n-5)(n+3)$, więc $17 \mid n^2-2n+2$ wtedy i tylko wtedy, gdy $17 \mid n-5$ lub $17 \mid n+3$. Wobec tego $17 \mid n^2-2n+2$ wtedy i tylko wtedy, gdy $n = 17k+5$ lub $n = 17k+14$ dla pewnego $k \in \mathbb{N}_0$.

Podobnie, $n^2+2n+2 = (n+1)^2+1$, więc $17 \mid n^2+2n+2$ wtedy i tylko wtedy, gdy $17 \mid (n+1)^2+1$ a to z kolei jest równoważne temu, że $17 \mid (n+1)^2+1-17$, czyli temu, że $17 \mid (n+1)^2-16$. Ponadto, $(n+1)^2-16 = (n+1)^2-4^2 = (n+1-4)(n+1+4) = (n-3)(n+5)$, więc $17 \mid n^2+2n+2 \iff [17 \mid n-3 \text{ lub } 17 \mid n+5]$. Wobec tego $17 \mid n^2+2n+2$ wtedy i tylko wtedy, gdy $n = 17k+3$ lub $n = 17k+12$ dla pewnego $k \in \mathbb{N}_0$.

Ostatecznie zatem: $n = 17k+3$ lub $n = 17k+5$ lub $n = 17k+12$ lub $n = 17k+14$ dla pewnego $k \in \mathbb{N}_0$.

Zadanie 22.261. Teza jest oczywista dla $k = 0$. Niech dalej $k > 0$.

Wtedy z zadania 22.88, $n^3-1 \mid n^{3k}-1$ i $n^3-1=(n-1)(n^2+n+1)$, więc $n^2+n+1 \mid n^{3k}-1$. Ponadto, $n^{3k+2}+n+1=(n^{3k}-1)\cdot n^2+(n^2+n+1)$, więc $n^2+n+1 \mid n^{3k+2}+n+1$.

Zadanie 22.262. Załóżmy, że $x,y,z \in \mathbb{Z}$ i $\frac{yz}{x}+\frac{xz}{y}+\frac{xy}{z}=3$. Wtedy $x,y,z \neq 0$ i po pomnożeniu obu stron tej równości przez xyz uzyskujemy zależność: $(yz)^2+(xz)^2+(xy)^2=3xyz$, skąd wynika, że $xyz>0$. Zatem $a=\frac{yz}{x}$, $b=\frac{xz}{y}$ i $c=\frac{xy}{z}$ są dodatnimi liczbami wymiernymi o sumie równej 3. Dalej, $bc=\frac{xz}{y}\cdot\frac{xy}{z}=x^2$, $ab=\frac{yz}{x}\cdot\frac{xz}{y}=z^2$ i $ac=\frac{yz}{x}\cdot\frac{xy}{z}=y^2$, ale $a+b+c=3$, więc $a(a+b+c)=3a$, skąd $a^2+z^2+y^2=3a$. Zatem $3a-a^2=y^2+z^2 \in \mathbb{N}$, ale liczbę wymierną a można zapisać w postaci $a=\frac{p}{q}$ dla pewnych względnie pierwszych liczb naturalnych p i q, więc $3a-a^2=\frac{3pq-p^2}{q^2}$, skąd $q \mid 3pq-p^2$. Zatem $q \mid p^2$ i wobec tego $q=1$, bo $\mathrm{NWD}(p,q)=1$. Zatem $a=p \in \mathbb{N}$. Analogicznie pokazujemy, że $b,c \in \mathbb{N}$, ale $a+b+c=3$, więc stąd $a=b=c=1$. Ponadto $x^2=bc$, $y^2=ac$ i $z^2=ab$, więc $x^2=y^2=z^2=1$, przy czym $xyz>0$. Stąd albo wszystkie liczby x,y,z są dodatnie albo dokładnie dwie z nich są ujemne. Wobec tego $x=y=z=1$ lub $x=1$ i $y=z=-1$ lub $x=y=-1$ i $z=1$ lub $x=z=-1$ i $y=1$. W każdym z tych przypadków $\frac{yz}{x}+\frac{xz}{y}+\frac{xy}{z}=3$. Wobec tego nasze zadanie ma dokładnie cztery rozwiązania (x,y,z): $(1,1,1),(1,-1,-1),(-1,1,-1),(-1,-1,1)$.

Zadanie 22.263. Niech k będzie dowolnym naturalnym wspólnym dzielnikiem liczb $an+b$ i $cn+d$. Wtedy k jest wspólnym dzielnikiem liczb $c(an+b)$ i $a(cn+d)$, więc k jest dzielnikiem różnicy tych liczb, czyli $k \mid ad-bc$, ale $ad-bc=\pm 1$, więc $k=1$, Wobec tego $\mathrm{NWD}(an+n,cn+d)=1$ dla każdego $n \in \mathbb{Z}$.

Zadanie 22.264. Zauważmy, że jeżeli $b,k \in \mathbb{N}$ oraz $b>1$, to $b<b^{2k+1}$, skąd $1<b+1<b^{2k+1}+1$ i z zadania 22.91 mamy, że $b+1 \mid b^{2k+1}+1$. Wobec tego liczba $b^{2k+1}+1$ nie jest pierwsza.

Przypuśćmy, że liczba n posiada dzielnik nieparzysty większy od 1. Wtedy $n=(2k+1)m$ dla pewnych $m,k \in \mathbb{N}$, więc $a^n+1=b^{2k+1}+1$, gdzie $b=a^m>1$. Zatem wtedy liczba a^n+1 nie jest pierwsza. Wobec

tego liczba $n > 1$ nie posiada nieparzystego dzielnika naturalnego, więc $n = 2^k$ dla pewnego $k \in \mathbb{N}$.

Zadanie 22.265. Dla $n = 1$ mamy, że $1^2+1 = 2 \in \mathbb{P}$ i $2^2+1 = 5 \in \in \mathbb{P}$. Ponadto $4^4+1 = 257$ i $16^2 < 257 < 17^2$ oraz liczbami pierwszymi $\leqslant 16$ są jedynie 2, 3, 5, 7, 11 i 13, przy czym oczywiście $2 \nmid 257$ i $5 \nmid 257$ oraz $3 \nmid 2+5+7$, więc $3 \nmid 257$. Dodatkowo $257 = 36 \cdot 7 + 5$, $257 = 23 \cdot 11 + 4$ i $257 = 19 \cdot 13 + 10$. Wobec tego na mocy twierdzenia 9.10 mamy, że $257 \in \mathbb{P}$ i liczby $n = 1$ oraz $n = 2$ spełniają warunki zadania.

Przypuśćmy, że istnieje liczba naturalna $n > 2$ taka, że $n^n + 1 \in \mathbb{P}$ i $(2n)^{2n} + 1 \in \mathbb{P}$. Wtedy z zadania 22.264 uzyskujemy, że $n = 2^k$ dla pewnego $k \in \mathbb{N}$, a ponieważ $n > 2$, więc $k > 1$. Dalej, $n^n + 1 = = (2^k)^{2^k} + 1 = 2^{k2^k} + 1$, skąd znowu na mocy zadania 22.264 mamy, że $k2^k = 2^s$ dla pewnego $s \in \mathbb{N}$. Po uwzględnieniu tego, że $k > 1$ i $k \mid 2^s$ otrzymujemy zatem, że $k = 2^t$ dla pewnego $t \in \mathbb{N}$. Zauważmy, że $(2n)^{2n} + 1 = 2^{(k+1)2^{k+1}} + 1 = 2^{(2^t+1)2^{k+1}} + 1 = [2^{2^{k+1}}]^{2^t+1} + 1 \in \mathbb{P}$, co przeczy zadaniu 22.267.

Ostatecznie mamy zatem, że $n = 1$ lub $n = 2$.

Zadanie 22.266. Niech $p \in \mathbb{P}$ i $p \equiv 31 \pmod{40}$. Wtedy $p \equiv 7 \pmod 8$, więc z przykładu 12.20 uzyskujemy, że $(\frac{2}{p}) = 1$. Dalej, na mocy prawa wzajemności reszt kwadratowych uzyskujemy, że $(\frac{5}{p}) = = (\frac{p}{5}) = (\frac{31}{5}) = (\frac{1}{5}) = 1$. Stąd i z własności symbolu Legendre'a wynika, że $(\frac{10}{p}) = (\frac{2}{p}) \cdot (\frac{5}{p}) = 1 \cdot 1 = 1$ i $(\frac{10^n}{p}) = (\frac{10}{p})^n = 1^n = 1$ dla każdego $n \in \mathbb{N}$. Ponadto $p \equiv 3 \pmod 4$, więc $(\frac{-1}{p}) = -1$ na mocy wniosku 12.16. Stąd $10^n \not\equiv -1 \pmod p$, czyli $p \nmid 10^n + 1$ dla każdego $n \in \mathbb{N}$.

Zadanie 22.267. Niech $n, x, y, z \in \mathbb{N}$ i $2n = x^2$, $3n = y^3$ i $4n = z^5$. Wtedy z drugiej równości $3^3 \mid 3n$, więc $3^2 \mid n$, zaś z trzeciej równości $2^5 \mid 4n$, więc $2^2 \mid n$. Wobec tego $n = 2^a \cdot 3^b \cdot m$ dla pewnych $a, b, m \in \mathbb{N}$ takich, że $2 \nmid m$ i $3 \nmid m$. Zatem istnieją różne liczby pierwsze $p_1, \ldots, p_s$ większe od 3 oraz istnieją $a_1, \ldots, a_s \in \mathbb{N}_0$ takie, że $m = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$. Weźmy dowolne $i = 1, \ldots, s$. Z równości $2n = x^2$, $3n = y^3$ i $4n = z^5$ na mocy twierdzenia o jednoznaczności rozkładu wynika, że $2 \mid a_i$ oraz

$3 \mid a_i$ oraz $5 \mid a_i$, skąd $30 \mid a_i$. Wobec tego $m = v^{30}$ dla pewnego $v \in \mathbb{N}$ takiego, że $2 \nmid v$ i $3 \nmid v$.

Analogicznie, z równości $2n = x^2$ wynika, że $2 \mid a+1$ i $2 \mid b$, z równości $3n = y^3$ wynika, że $3 \mid a$ i $3 \mid b+1$ oraz z równości $4n = z^5$ wynika, że $5 \mid a+2$ i $5 \mid b$. Stosując twierdzenie chińskie o resztach uzyskujemy stąd, że $a = 30l + 3$ dla pewnego $l \in \mathbb{N}_0$ oraz $b = 30u + 20$ dla pewnego $u \in \mathbb{N}_0$. Stąd $n = 2^{30l+3} \cdot 3^{30u+20} \cdot v^{30}$. Proste sprawdzenie pokazuje, że takie n spełnia warunki zadania. Stąd najmniejszą liczbą spełniającą warunki zadania jest $n = 2^3 \cdot 3^{20}$.

Zadanie 22.268. Ponieważ $\mathrm{NWD}(3k+4, 3) = 1$, więc na mocy zasadniczego twierdzenia arytmetyki mamy, że

$$3k+4 \mid 7k+1 \iff 3k+4 \mid 3 \cdot (7k+1).$$

Ponadto $3 \cdot (7k+1) = 21k+3 = 7 \cdot (3k+4) - 25$, więc $3k+4 \mid 7k+1 \iff 3k+4 \mid 25$. Zatem $3k+4$ jest całkowitym dzielnikiem liczby 25 dającym resztę 1 z dzielenia przez 3. Wobec tego $3k+4 = 1$ lub $3k+4 = 25$ lub $3k+4 = -5$, czyli $k \in \{-1, 7, -3\}$.

Zadanie 22.269. Niech a będzie nieparzystą liczbą naturalną niepodzielną przez 5. Wtedy $\mathrm{NWD}(10, 9a) = 1$, więc z twierdzenia Eulera $10^n \equiv 1 \pmod{9a}$ dla $n = \varphi(9a)$. Stąd $9a \mid 10^n - 1$, a więc $a \mid \frac{10^n-1}{9}$, przy czym $\frac{10^n-1}{9} = \underbrace{11\ldots1}_{n}$.

Zadanie 22.270. Ponieważ $a, b, c \in \mathbb{N}$ i $2c^2 = 3ab$, więc $a+b-c > 0$, skąd $a+b-c \in \mathbb{N}$. Ponadto $ab \geqslant 6$, więc $a+b-c > 1$. Dalej, $2c^3 = 3abc$, więc $a^3+b^3+c^3 = a^3+b^3+(-c)^3 - 3ab(-c)$. Dalej, korzystając z zadania 22.93 mamy, że $a^3+b^3+(-c)^3 - 3ab(-c) = (a+b-c)(a^2+b^2+c^2-ab+ac+bc)$, więc $a+b-c \mid a^3+b^3+c^3$. Ponadto $1 < a+b-c < a+b+c \leqslant a^3+b^3+c^3$, więc $a^3+b^3+c^3$ jest liczbą złożoną.

Zadanie 22.271. Przypuśćmy, że tak nie jest. Wtedy istnieje liczba naturalna $n > 1$ taka, że $n \mid 2^n - 1$. Oczywiście liczba n jest nieparzysta. Oznaczmy przez p najmniejszy dzielnik liczby n większy od 1. Wtedy $p \in \mathbb{P}$ i $p \mid 2^n - 1$ z przechodniości relacji podzielności. Ponadto

$p \mid 2^{p-1} - 1$ na mocy małego twierdzenia Fermata. Wobec tego $p \mid \mathrm{NWD}(2^n - 1, 2^{p-1} - 1)$ i stosując zadanie 22.160 uzyskujemy, że $p \mid 2^d - 1$, gdzie $d = \mathrm{NWD}(n, p-1)$. Zatem $d \mid n$ i $d < p$, czyli z minimalności p jest $d = 1$ i $p \mid 2^1 - 1$, co prowadzi do sprzeczności.

Zadanie 22.272. Załóżmy, że istnieją $x, y \in \mathbb{N}$ i $k \in \mathbb{Z}$ takie, że $4xy - x - y = k^2$. Wtedy $16xy - 4x - 4y = 4k^2$, skąd $(4x-1)\cdot(4y-1) = (2k)^2 + 1^2$. Dalej, na mocy przykładu 10.39 nie istnieje liczba pierwsza $p \equiv 3 \pmod 4$ taka, że $p \mid (2k)^2 + 1^2$. Ponadto $4x - 1 > 1$ jest liczbą naturalną nieparzystą. Zatem każdy dzielnik pierwszy liczby $4x - 1$ przystaje do 1 modulo 4. Stąd $4x - 1 = p_1 \cdot \ldots \cdot p_s$ dla pewnych liczb pierwszych $p_i \equiv 1 \pmod 4$ dla $i = 1, \ldots, s$, więc po pomnożeniu stronami tych kongruencji $4x - 1 \equiv 1 \pmod 4$, co prowadzi do sprzeczności i kończy dowód twierdzenia Eulera.

Zadanie 22.273. Niech $n > 1$ i $n \in \mathbb{N}$. Jeśli liczba n jest nieparzysta, to $n = 2k + 1$ dla pewnego $k \in \mathbb{N}$ i wtedy $3^n + 1 = 3^{2k+1} + 1 = 3 \cdot 9^k + 1$, a ponieważ $9 \equiv 1 \pmod 8$, więc $3^n + 1 \equiv 3 \cdot 1 + 1 \equiv 4 \pmod 8$, skąd $8 \nmid 3^n + 1$ i tym bardziej $2^n \nmid 3^{n+1}$, bo $n \geqslant 3$. Jeśli liczba n jest parzysta, to $n = 2k$ dla pewnego $k \in \mathbb{N}$, więc $3^n + 1 = 3^{2k} + 1$. Ponadto $3 \equiv -1 \pmod 4$, więc $3^{2k} \equiv (-1)^{2k} \equiv 1 \pmod 4$, skąd $3^n + 1 \equiv 2 \pmod 4$, czyli $4 \nmid 3^n + 1$, a tym bardziej $2^n \nmid 3^n + 1$, bo $n \geqslant 2$.

Zadanie 22.274. Zadanie sprowadza się do wyznaczenia reszty z dzielenia przez 1000 liczby n^{100}. Rozważmy najpierw przypadek, gdy $2 \nmid n$ i $5 \nmid n$. Wtedy $\mathrm{NWD}(n, 1000) = 1$, więc na mocy twierdzenia 10.21 jest $n^{\xi(1000)} \equiv 1 \pmod{1000}$, gdzie $\xi(1000) = \mathrm{NWW}(2^2 \cdot (2-1), 5^2 \cdot (5-1)) = 100$. Wobec tego w tym przypadku ostatnimi trzema cyframi liczby n są 001.

Jeśli $2 \mid n$ i $5 \mid n$, to $10 \mid n$ i wtedy $n^{100} \equiv 0 \pmod{1000}$, więc w tym przypadku trzema ostatnimi cyframi liczby n^{100} są 000.

Niech teraz $2 \mid n$ i $5 \nmid n$. Wtedy $n^{100} \equiv 0 \pmod 8$ i z twierdzenia Eulera $n^{\varphi(5^3)} \equiv 1 \pmod{5^3}$, czyli $n^{100} \equiv 1 \pmod{125}$. Stosując twierdzenie chińskie o resztach znajdujemy stąd, że $n^{100} \equiv 376 \pmod{1000}$, co oznacza, że w ty przypadku ostatnimi cyframi liczby n^{100} są 376.

W końcu, niech $2 \nmid n$ i $5 \mid n$. Wtedy $n^{100} \equiv 0 \pmod{125}$ oraz

z twierdzenia Eulera jest $n^4 \equiv 1 \pmod 8$, więc $n^{100} \equiv 1 \pmod 8$. Stosując twierdzenie chińskie o resztach znajdujemy stąd, że $n^{100} \equiv 625 \pmod{1000}$, co oznacza, że w ty przypadku ostatnimi cyframi liczby n^{100} są 625.

Zadanie 22.275. Dowodzoną równość można zapisać w postaci $a \cdot \mathrm{NWD}(a,b,c,d) = \mathrm{NWD}(a,c) \cdot \mathrm{NWD}(a,d)$. Dalej, na mocy twierdzenia 8.46 i ćwiczenia 8.40 oraz tego, że $ab = cd$ otrzymujemy, że $a \cdot \mathrm{NWD}(a,b,c,d) = \mathrm{NWD}(a^2,ab,ac,ad) = \mathrm{NWD}(a^2,cd,ac,ad) = \mathrm{NWD}(\mathrm{NWD}(a^2,ac),\mathrm{NWD}(cd,ad))$, skąd dostajemy, że $a \cdot \mathrm{NWD}(a,b,c,d) = \mathrm{NWD}(a\mathrm{NWD}(a,c), d\mathrm{NWD}(a,c)) = \mathrm{NWD}(a,c) \cdot \mathrm{NWD}(a,d)$.

Zadanie 22.276. Z twierdzenia o dzieleniu z resztą wynika, że $a = 3s$ lub $a = 3s+1$ lub $a = 3s-1$ dla pewnego $s \in \mathbb{Z}$. W pierwszym przypadku $a^3 \equiv 0 \pmod 9$. W drugim przypadku $a^3 = (3s+1)^3 = 27s^3 + 27s^2 + 9s + 1 \equiv 1 \pmod 9$, a w trzecim przypadku $a^3 = (3s-1)^3 = 27s^3 - 27s^2 + 9s - 1 \equiv -1 \pmod 9$, co kończy rozwiązanie pierwszej części zadania.

Stąd wynika, że suma sześcianów trzech liczb całkowitych przystaje modulo 9 jedynie do liczb $\pm 1 \pm 1 \pm 1$, $0 \pm 1 \pm 1$, $0 + 0 \pm 1$, $0 + 0 + 0$, czyli przystaje jedynie do liczb $-3, -2, -1, 0, 1, 2, 3$, czyli nie przystaje ani do 4, ani do 5 modulo 9, co należało wykazać.

Zadanie 22.277. Teza wynika z twierdzenia o dzieleniu z resztą oraz z następujących tożsamości: $6k = (-k)^3 + (-k)^3 + (k+1)^3 + (k-1)^3$, $6k+1 = (-k)^3 + (-k)^3 + (k+1)^3 + (k-1)^3 + 1^3$, $6k+5 = (-k-1)^3 + (-k-1)^3 + k^3 + (k+2)^3 + (-1)^3$, $6k+2 = (1-k)^3 + (1-k)^3 + k^3 + (k-2)^3 + 2^3$, $6k+4 = (-k-2)^3 + (-k-2)^3 + (k+1)^3 + (k+3)^3 + (-2)^3$ i $6k+3 = (4-k)^3 + (4-k)^3 + (k-3)^3 + (k-5)^3 + 3^3$.

Zadanie 22.278. Dla $p = 2$ mamy, że $a = 0$ lub $a = 1$ oraz $0! = 1! = 1$ i $(-1)^{a+1} = \pm 1$, więc teza zachodzi.

Niech dalej $p > 2$. Dla $a = 0$ teza zachodzi na mocy twierdzenia Wilsona. Przypuśćmy, że teza zachodzi dla pewnego $a = 0, \ldots, p-2$, czyli $a! \cdot (p-1-a)! \equiv (-1)^{a+1} \pmod p$. Ponieważ $(p-1-a)! = (p-1-(a+1))! \cdot (p-1-a) \equiv (p-1-(a+1))! \cdot (-1) \cdot (a+1)$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

(mod p) oraz $(a+1)! = a! \cdot (a+1)$, więc stąd otrzymujemy, że $(a+1)! \cdot$ $\cdot (p-1-(a+1))! \cdot (-1) \equiv (-1)^{a+1} \pmod{p}$. Teraz mnożąc obie strony tej kongruencji przez -1 uzyskamy, że $(a+1)! \cdot (p-1-(a+1))! \equiv$ $\equiv (-1)^{(a+1)+1} \pmod{p}$. Zatem wtedy teza zachodzi dla liczby $a+1$.

Wobec tego na mocy zasady indukcji matematycznej teza zachodzi dla każdego $a = 0, \ldots, p-1$.

Zadanie 22.279. Ze wzoru dwumianowego Newtona wynika, że x^p występuje w rozwinięciu $(1+x)^{np}$ ze współczynnikiem $\binom{np}{p}$. ponadto na mocy twierdzenia 9.28 i wzoru Newtona mamy, że $(1+x)^p =$ $= 1 + x^p + p \cdot w$, gdzie w jest wielomianem stopnia $p-1$ o współczynnikach całkowitych. Stąd $(1+x)^{np} = [(1+x^p) + pw]^n = (1+x^p)^n +$ $+\binom{n}{1}(1+x^p)^{n-1} \cdot pw + \binom{n}{2}(1+x^p)^{n-2}(pw)^2 + \ldots + (pw)^n$, więc $(1+x)^{np} =$ $= (1+x^p)^n + n(1+x^p)^{n-1} \cdot pw + p^2 u$ dla pewnego wielomianu u o współczynnikach całkowitych. Ponieważ $w(x) = a_1 x + \ldots + a_{p-1} x^{p-1}$ dla pewnych $a_1, \ldots, a_{p-1} \in \mathbb{Z}$, więc x^p występuje w wielomianie $(1+x^p)^{n-1} \cdot pw$ ze współczynnikiem 0. Dodatkowo $(1+x^p)^n = 1 + nx^p + \binom{n}{2} x^{2p} + \ldots +$ $+\binom{n}{n} x^{np}$, więc x^p występuje w wielomianie $(1+x^p)^n + n(1+x^p)^{n-1} \cdot pw$ ze współczynnikiem n. Stąd porównując współczynniki przy x^p w obu sposobach rozwinięcia $(1+x)^{np}$ dostajemy, że $\binom{np}{p} \equiv n \pmod{p^2}$.

Zadanie 22.280. Z twierdzenia o dzieleniu z resztą $n = mp + r$ dla pewnego $m \in \mathbb{N}$ oraz dla pewnego $r = 0, 1, \ldots, p-1$. Wtedy $\lfloor \frac{n}{p} \rfloor = m$. Z zadania 22.279 wynika, że $(1+x)^{mp} = 1 + mx^p + p^2 w$ dla pewnego wielomianu w o współczynnikach całkowitych oraz $\binom{mp}{p} \equiv$ $\equiv m \pmod{p^2}$. Pozostaje zatem rozważyć $r = 1, \ldots, p-1$. Wtedy $(1+x)^{mp+r} = (1+x)^r \cdot (1 + mx^p + p^2 w) = 1 + mx^p + p^2 w + x^r +$ $+ mx^{p+r} + p^2 x^r w$, skąd porównując współczynnik przy x^p w obu stronach tej równości uzyskamy, że $\binom{mp+r}{p} \equiv m \pmod{p^2}$, co kończy nasz dowód.

Lista początkowych liczb pierwszych

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281,
2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371,
2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447,
2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557,
2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671,
2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731,
2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833,
2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927,
2939, 2953, 2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037,
3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, 3119, 3121, 3137, 3163,
3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, 3251, 3253,
3257, 3259, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343,
3347, 3359, 3361, 3371, 3373, 3389, 3391, 3407, 3413, 3433, 3449, 3457,
3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529, 3533, 3539,
3541, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623,
3631, 3637, 3643, 3659, 3671, 3673, 3677, 3691, 3697, 3701, 3709, 3719,
3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803, 3821, 3823,
3833, 3847, 3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919,
3923, 3929, 3931, 3943, 3947, 3967, 3989, 4001, 4003, 4007, 4013, 4019,
4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099, 4111, 4127,
4129, 4133, 4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229,
4231, 4241, 4243, 4253, 4259, 4261, 4271, 4273, 4283, 4289, 4297, 4327,
4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421, 4423, 4441,
4447, 4451, 4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523,
4547, 4549, 4561, 4567, 4583, 4591, 4597, 4603, 4621, 4637, 4639, 4643,
4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723, 4729, 4733,
4751, 4759, 4783, 4787, 4789, 4793, 4799, 4801, 4813, 4817, 4831, 4861,
4871, 4877, 4889, 4903, 4909, 4919, 4931, 4933, 4937, 4943, 4951, 4957,
4967, 4969, 4973, 4987, 4993, 4999, 5003, 5009, 5011, 5021, 5023, 5039,
5051, 5059, 5077, 5081, 5087, 5099, 5101, 5107, 5113, 5119, 5147, 5153,
5167, 5171, 5179, 5189, 5197, 5209, 5227, 5231, 5233, 5237, 5261, 5273,
5279, 5281, 5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381, 5387, 5393,
5399, 5407, 5413, 5417, 5419, 5431, 5437, 5441, 5443, 5449, 5471, 5477,
5479, 5483, 5501, 5503, 5507, 5519, 5521, 5527, 5531, 5557, 5563, 5569,
5573, 5581, 5591, 5623, 5639, 5641, 5647, 5651, 5653, 5657, 5659, 5669,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

5683, 5689, 5693, 5701, 5711, 5717, 5737, 5741, 5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813, 5821, 5827, 5839, 5843, 5849, 5851, 5857, 5861, 5867, 5869, 5879, 5881, 5897, 5903, 5923, 5927, 5939, 5953, 5981, 5987, 6007, 6011, 6029, 6037, 6043, 6047, 6053, 6067, 6073, 6079, 6089, 6091, 6101, 6113, 6121, 6131, 6133, 6143, 6151, 6163, 6173, 6197, 6199, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, 6269, 6271, 6277, 6287, 6299, 6301, 6311, 6317, 6323, 6329, 6337, 6343, 6353, 6359, 6361, 6367, 6373, 6379, 6389, 6397, 6421, 6427, 6449, 6451, 6469, 6473, 6481, 6491, 6521, 6529, 6547, 6551, 6553, 6563, 6569, 6571, 6577, 6581, 6599, 6607, 6619, 6637, 6653, 6659, 6661, 6673, 6679, 6689, 6691, 6701, 6703, 6709, 6719, 6733, 6737, 6761, 6763, 6779, 6781, 6791, 6793, 6803, 6823, 6827, 6829, 6833, 6841, 6857, 6863, 6869, 6871, 6883, 6899, 6907, 6911, 6917, 6947, 6949, 6959, 6961, 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057, 7069, 7079, 7103, 7109, 7121, 7127, 7129, 7151, 7159, 7177, 7187, 7193, 7207, 7211, 7213, 7219, 7229, 7237, 7243, 7247, 7253, 7283, 7297, 7307, 7309, 7321, 7331, 7333, 7349, 7351, 7369, 7393, 7411, 7417, 7433, 7451, 7457, 7459, 7477, 7481, 7487, 7489, 7499, 7507, 7517, 7523, 7529, 7537, 7541, 7547, 7549, 7559, 7561, 7573, 7577, 7583, 7589, 7591, 7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717, 7723, 7727, 7741, 7753, 7757, 7759, 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, 7877, 7879, 7883, 7901, 7907, 7919, 7927, 7933, 7937, 7949, 7951, 7963, 7993, 8009, 8011, 8017, 8039, 8053, 8059, 8069, 8081, 8087, 8089, 8093, 8101, 8111, 8117, 8123, 8147, 8161, 8167, 8171, 8179, 8191, 8209, 8219, 8221, 8231, 8233, 8237, 8243, 8263, 8269, 8273, 8287, 8291, 8293, 8297, 8311, 8317, 8329, 8353, 8363, 8369, 8377, 8387, 8389, 8419, 8423, 8429, 8431, 8443, 8447, 8461, 8467, 8501, 8513, 8521, 8527, 8537, 8539, 8543, 8563, 8573, 8581, 8597, 8599, 8609, 8623, 8627, 8629, 8641, 8647, 8663, 8669, 8677, 8681, 8689, 8693, 8699, 8707, 8713, 8719, 8731, 8737, 8741, 8747, 8753, 8761, 8779, 8783, 8803, 8807, 8819, 8821, 8831, 8837, 8839, 8849, 8861, 8863, 8867, 8887, 8893, 8923, 8929, 8933, 8941, 8951, 8963, 8969, 8971, 8999, 9001, 9007, 9011, 9013, 9029, 9041, 9043, 9049, 9059, 9067, 9091, 9103, 9109, 9127, 9133, 9137, 9151, 9157, 9161, 9173, 9181, 9187, 9199, 9203, 9209, 9221, 9227, 9239, 9241, 9257, 9277, 9281, 9283, 9293, 9311, 9319, 9323, 9337, 9341, 9343, 9349, 9371, 9377, 9391, 9397, 9403, 9413, 9419, 9421, 9431,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

9433, 9437, 9439, 9461, 9463, 9467, 9473, 9479, 9491, 9497, 9511, 9521, 9533, 9539, 9547, 9551, 9587, 9601, 9613, 9619, 9623, 9629, 9631, 9643, 9649, 9661, 9677, 9679, 9689, 9697, 9719, 9721, 9733, 9739, 9743, 9749, 9767, 9769, 9781, 9787, 9791, 9803, 9811, 9817, 9829, 9833, 9839, 9851, 9857, 9859, 9871, 9883, 9887, 9901, 9907, 9923, 9929, 9931, 9941, 9949, 9967, 9973, 10007, 10009, 10037, 10039, 10061, 10067, 10069, 10079, 10091, 10093, 10099, 10103, 10111, 10133, 10139, 10141, 10151, 10159, 10163, 10169, 10177, 10181, 10193, 10211, 10223, 10243, 10247, 10253, 10259, 10267, 10271, 10273, 10289, 10301, 10303, 10313, 10321, 10331, 10333, 10337, 10343, 10357, 10369, 10391, 10399, 10427, 10429, 10433, 10453, 10457, 10459, 10463, 10477, 10487, 10499, 10501, 10513, 10529, 10531, 10559, 10567, 10589, 10597, 10601, 10607, 10613, 10627, 10631, 10639, 10651, 10657, 10663, 10667, 10687, 10691, 10709, 10711, 10723, 10729, 10733, 10739, 10753, 10771, 10781, 10789, 10799, 10831, 10837, 10847, 10853, 10859, 10861, 10867, 10883, 10889, 10891, 10903, 10909, 10937, 10939, 10949, 10957, 10973, 10979, 10987, 10993, 11003, 11027, 11047, 11057, 11059, 11069, 11071, 11083, 11087, 11093, 11113, 11117, 11119, 11131, 11149, 11159, 11161, 11171, 11173, 11177, 11197, 11213, 11239, 11243, 11251, 11257, 11261, 11273, 11279, 11287, 11299, 11311, 11317, 11321, 11329, 11351, 11353, 11369, 11383, 11393, 11399, 11411, 11423, 11437, 11443, 11447, 11467, 11471, 11483, 11489, 11491, 11497, 11503, 11519, 11527, 11549, 11551, 11579, 11587, 11593, 11597, 11617, 11621, 11633, 11657, 11677, 11681, 11689, 11699, 11701, 11717, 11719, 11731, 11743, 11777, 11779, 11783, 11789, 11801, 11807, 11813, 11821, 11827, 11831, 11833, 11839, 11863, 11867, 11887, 11897, 11903, 11909, 11923, 11927, 11933, 11939, 11941, 11953, 11959, 11969, 11971, 11981, 11987, 12007, 12011, 12037, 12041, 12043, 12049, 12071, 12073, 12097, 12101, 12107, 12109, 12113, 12119, 12143, 12149, 12157, 12161, 12163, 12197, 12203, 12211, 12227, 12239, 12241, 12251, 12253, 12263, 12269, 12277, 12281, 12289, 12301, 12323, 12329, 12343, 12347, 12373, 12377, 12379, 12391, 12401, 12409, 12413, 12421, 12433, 12437, 12451, 12457, 12473, 12479, 12487, 12491, 12497, 12503, 12511, 12517, 12527, 12539, 12541, 12547, 12553

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Spis symboli

Skorowidz

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Bibliografia

[1] Aczel A. D., *Wielkie twierdzenie Fermata. Rozwiązanie zagadki starego matematycznego problemu*, Wydawnictwo Prószyński i S-ka, Warszawa 1998.

[2] Aigner M., Gunter Z. M., *Dowody z księgi*, Wydawnictwo PWN, Warszawa 2023.

[3] Andreescu T., Andrica D., Cucurezeanu I., *An Introduction to Diophantine Equantions*, Springer-Birkhauser, New York 2010.

[4] Andruszkiewicz R. R., *Równania diofantyczne*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2021.

[5] Białynicki-Birula A., *Algebra*, Wydawnictwo PWN, Warszawa 2016.

[6] Brezinski C., *History of continued fractions and Pade approximants*, Springer-Verlag, New York 1991.

[7] Buchsztab A. A., *Teoria liczb*, Proswieszczenije, Moskwa 1960.

[8] Corless R. M., *Continued Fractions and Chaos*, Amer. Math. Monthly 99(3), 1992, s. 203-215.

[9] Dedekind R., *Stetigkeit und irrationale Zahlen*, Brunszwik 1872.

[10] Dickson L. E., *Notes on the theory of numbers*, Amer. Math. Monthly (18), 1911, s. 109.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

[11] Euler L., *De numeris anicabilibus*, Reprinted in: Opera posthuma, Euler archive [E798].

[12] Flachsmeyer J., *Kombinatoryka. Podstawowy wykład w ujęciu mnogościowym*, Wydawnictwo PWN, Warszawa 1977.

[13] Gimbel S., JaromaJ. H., *Sylvester: ushering in the modern era of research on odd perfect numbers*, Integers Electronic Journal of Combinatorial Number Theory (3), 2003.

[14] Goldfeld D., *Beyond the Last Theorem*, Math Horizons, 4:1, 1996, s. 26-34.

[15] Gupta R., Ram Murty M., *A remark on Artin's conjecture*, Inventiones Math. 78, 1984, s. 127-130.

[16] Guy R. K., *Unsolved Problems in Number Theory*, Springer New York, NY 2004.

[17] Heath-Brown D. R., *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford (2)37, 1985, s. 27-38.

[18] Holdener J. A., *A theorem of Touchard on the form of odd perfect numbers*, Amer. Math. Monthly, 109(7), 2002, 661-663.

[19] Jaroma J. H., *Note on the Lucas Lehmer Test*, Irish Math. Soc. Bulletin 54, 2004, 63-72.

[20] Oliver Knill, *The oldest open problem in mathematics*, NEU Math Circle, December 2, 2007.

[21] Khinchin, A. I., *Continued fractions*, University of Chicago Press, Chicago 1964.

[22] Marzantowicz W., Zarzycki P., *Elementarna teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2015.

[23] Matijasevic V. J., Jones P. J., *Proof of recursive unsolvability of Hilbert's tenth problem*, The American Math. Monthly, (98), 1991, s. 689-709.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

[24] Metsänkylä T., *Catalan's conjecture: another old Diophantine problem solved*, Bull. Amer. Math. Soc 41(1), 2004, s. 43–57.

[25] Mihăilescu P., *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Amgew. Math. 572, 2004, s. 167-195.

[26] Nahin, P. J., *An Imaginary Tale: The Story of* $\sqrt{-1}$, Princeton University Press, New Jersey 2016.

[27] Narkiewicz W., *Teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2003.

[28] Narkiewicz W., *Clasical problems in number theory*, Wydawnictwo Naukowe PWN, Warszawa 1986.

[29] Nowicki A., *Równanie Pella, Podróże po Imperium Liczb 14*, Olsztyńska Wyższa Szkoła Informatyki i Zarządzania, Toruń 2014.

[30] Nowicki A., Cykl - *Podróże po Imperium Liczb* , Olsztyńska Wyższa Szkoła Informatyki i Zarządzania, Toruń 2014.

[31] Peirce B., *On perfect numbers*, New York Math. Diary 2, XIII 1832, s. 267-277.

[32] Ribenboim P., *Catalan's Conjecture*, Academic Press, Boston 1994.

[33] Sierpiński W., *Arytmetyka teoretyczna*, Wydawnictwo Naukowe PWN, Warszawa 1959.

[34] Sierpiński W., *Wstęp do teorii liczb*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1987.

[35] Weil A., *Number Theory: An Approach through History from Hammurapi to Legendre*, Birkhäuser, Boston 1984.

[36] Wells D., *Prime Numbers: The Most Mysterious Figures in Math*, John Wiley & Sons, Inc., New Jersey 2005.