RÓWNANIA DIOFANTYCZNE

Ryszard R. Andruszkiewicz

RÓWNANIA DIOFANTYCZNE

WYDAWNICTWO UNIWERSYTETU W BIAŁYMSTOKU

BIAŁYSTOK 2021

Recenzenci:
prof. dr hab. Piotr Grzeszczuk, PB
dr hab. Jerzy Stanisław Matczuk, prof. UW

Opracowanie graficzne:
Karol Pryszczepko

Redakcja i korekta:
Janina Demianowicz

Korekta merytoryczna:
Karol Pryszczepko

Redakcja techniczna i skład:
Ryszard R. Andruszkiewicz

ISBN 978-83-7431-707-8

Wydanie publikacji zostało sfinansowane ze środków
Wydziału Matematyki Uniwersytetu w Białymstoku

Wydawnictwo Uniwersytetu w Białymstoku
15-328 Białystok, ul. Świerkowa 20B, tel. (85) 745 71 20
http://wydawnictwo.uwb.edu.pl, wydawnictwo@uwb.edu.pl

Druk i oprawa: Hot Art Przemysław Zaczek

Spis treści

Wstęp

Równaniem diofantycznym (od greckiego matematyka Diofantosa) nazywamy równanie postaci:

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

gdzie f jest funkcją n-zmiennych całkowitych i $n \geqslant 2$. Jeśli f jest wielomianem o współczynnikach całkowitych, to (1) nazywamy **algebraicznym równaniem diofantycznym**. Ciąg $(a_1, a_2, \ldots, a_n)$ liczb całkowitych taki, że $f(a_1, a_2, \ldots, a_n) = 0$, nazywamy **rozwiązaniem** równania (1). Równanie diofantyczne posiadające co najmniej jedno rozwiązanie nazywamy **rozwiązalnym**.

Diofantos (III wiek n.e.) jest nazywany ojcem algebry. Zasłynął dzięki dziełu "Arithmetica" oraz dzięki rezultatom osiągniętym w teorii równań algebraicznych i 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.

Prace Diofantosa związane z równaniem (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.

Z równaniem diofantycznym są związane następujące fundamentalne problemy:

Problem 1. Czy jest ono rozwiązalne?

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.

Równaniom diofantycznym poświęcono wiele monografii i artykułów naukowych. Mają też one zaszczytne miejsce w olimpiadach matematycznych i różnorodnych konkursach matematycznych. Literatura jest tu tak bogata, że nie sposób wymienić wszystkich publikacji, nie mówiąc już nawet o ich omówieniu. W języku polskim istnieją bardzo ciekawe prace A. Nowickiego, w tym temacie prezentujące mnóstwo twierdzeń i problemów z podaniem obszernej literatury.

Powstaje zatem pytanie: jaki cel przeświecał autorowi tej książki? Otóż nie chodziło o zebranie jak największej liczby ciekawych zadań konkursowych, czy też podanie encyklopedycznych faktów o uzyskanych wynikach w teorii równań diofantycznych. Zamysłem było precyzyjne przedstawienie klasycznych (w miarę możliwości jak najbardziej elementarnych) metod i narzędzi, związanych z tym tematem. Moją pasją jest przedstawianie rozwiązań trudnych problemów w sposób zrozumiały dla czytelnika zainteresowanego matematyką, bez odsyłania go do trudno dostępnych artykułów naukowych, książek obcojęzycznych, czy polegania na zaawansowanych teoriach matematycznych. Chciałem tak zaprezentować materiał, aby był on zrozumiały dla Czytelnika zaznajomionego jedynie z podstawowym kursem elementarnej teorii liczb. Stąd w tej książce pojawiają się na przykład elementy teorii pierścieni oraz podstawy teorii ciał abstrakcyjnych umieszczone w ostatniej jej części. Mam nadzieję, że taka prezentacja materiału zachęci młodego matematyka do studiowania matematyki wyższej, ze szczególnym uwzględnieniem współczesnej algebry. Natomiast Czytelnik z wyższym wykształceniem algebraicznym może pominąć te fragmenty książki, które są mu dobrze znane i skupić się raczej na ich zastosowaniach podanych w innych częściach tej publikacji.

Podczas pracy na Wydziale Matematyki UwB wielokrotnie spotykałem różne nietrywialne równania diofantyczne i borykałem się ze znalezieniem ich w miarę możliwości jak najbardziej elementarnych

i prostych rozwiązań. Okazało się, że trzeba poszerzyć stosowane do tej pory metody, aby udowodnić kilka bardzo trudnych twierdzeń, które sprawiły podobny kłopot innym matematykom. Stąd moja wdzięczność za prace W. Narkiewicza, T. Nagella, J. Cohna, A. Nowickiego, W. Sierpińskiego, L. Mordella i innych. Uznałem, że zebrany materiał zasługuje na zaprezentowanie szerszemu gronu czytelników, tym bardziej, że znalazły się tu dowody twierdzeń, które opierały się przez kilkadziesiąt lat i dopiero niedawno zostały odkryte.

Część I

Elementarna teoria liczb

Rozdział 1

Podzielność liczb całkowitych

1.1 Zasady: indukcji, minimum i maksimum

Dodatnie liczby całkowite będziemy nazywali liczbami naturalnymi i przez $\mathbb{N}$ będziemy oznaczali zbiór wszystkich liczb naturalnych, natomiast $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Liczby naturalne można wprowadzić aksjomatycznie posługując się na przykład pięcioma postulatami Peano. Kluczową rolę odgrywa w tym systemie tak zwany Aksjomat indukcji zupełnej, który będziemy dalej nazywali **zasadą indukcji**. Oto jej sformułowanie:

Zasada indukcji. *Niech A będzie podzbiorem zbioru $\mathbb{N}$ takim, że $1 \in A$ oraz dla każdego $k \in \mathbb{N}$ spełniona jest implikacja:*

$$\text{jeżeli } k \in A, \text{ to } k+1 \in A.$$

Wówczas $A = \mathbb{N}$, tzn. każda liczba naturalna należy do A.

Wychodząc natomiast z aspektu porządkowego liczby naturalnej zauważamy, że zachodzi też bardzo ważna

Zasada minimum. *W każdym niepustym podzbiorze A zbioru $\mathbb{N}$ istnieje liczba najmniejsza, tzn. liczba mniejsza lub równa od każdej liczby ze zbioru A.*

Mówimy, że niepusty podzbiór X zbioru $\mathbb{N}$ jest ograniczony z góry, jeżeli istnieje $a \in \mathbb{N}$ takie, że $x \leqslant a$ dla każdego $x \in X$ i mówimy wówczas, że liczba a ogranicza z góry zbiór X. Stosując Zasadę minimum można udowodnić, że zachodzi następująca

Zasada maksimum. *Każdy niepusty i ograniczony z góry podzbiór A zbioru $\mathbb{N}$ posiada element największy, tzn. taki, który jest większy lub równy od każdej liczby należącej do A.*

W Arytmetyce dowodzi się, że te trzy zasady są równoważne (patrz na przykład [36]). Tutaj nie będziemy się zajmowali takimi formalizmami i przyjmiemy, że Czytelnik zna prawa działań i ich związek z nierównościami nie tylko w zbiorze $\mathbb{N}$, ale też w zbiorze $\mathbb{R}$ wszystkich liczb rzeczywistych. Warto też podkreślić, że zasada maksimum zachodzi nie tylko dla $A \subseteq \mathbb{N}$, ale też dla $A \subseteq \mathbb{Z}$, gdzie $\mathbb{Z}$ jest zbiorem wszystkich liczb całkowitych. Jako przykład zastosowania zasady maksimum podamy teraz następujące

Twierdzenie 1.1. *Niech $m \in \mathbb{N}$. Wówczas dla każdej liczby całkowitej a 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 k takich, że $k \cdot m \leqslant a$. Jeśli $a \geqslant 0$, to $0 \in X$ i dla $k \in X$ mamy, że $km \leqslant a \leqslant ma$, skąd $k \leqslant a$. Jeśli zaś $a < 0$, to $a \in X$, bo wtedy $m \geqslant 1$, skąd $am \leqslant a$ i dla $k \in X$ mamy, że $km \leqslant 0$, skąd $k \leqslant 0$. Zatem zbiór Xjest niepusty i 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 $(q_1 - q_2) \cdot m = r_2 - r_1$. Zauważmy, że $-m < r_2 - r_1 < m$, 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 1.2. Liczbę r w twierdzeniu 1.1 nazywamy **resztą z dzielenia** liczby całkowitej a przez liczbę naturalną m i oznaczamy sym-

bolem $[a]_m$, zaś 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 $r = 0 \cdot m + r$ oraz $0 \leqslant r < m$. 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 $[101]_7 = 3$, a $[-101]_7 = 4$.

Uwaga 1.3. Zauważmy, że twierdzenie 1.1 możemy wypowiedzieć równoważnie innymi słowami: Niech $m \in \mathbb{N}$, $m > 1$. Wówczas każda liczba całkowita jest dokładnie jednej z m postaci:

$$mk,\ mk+1,\ mk+2,\ \ldots,\ mk+(m-1) \quad \text{dla} \quad k \in \mathbb{Z},$$

czyli zbiór $\mathbb{Z}$ jest sumą m parami rozłącznych podzbiorów:

$$||0||_m,\ ||1||_m,\ ||2||_m,\ \ldots,\ ||m-1||_m,$$

gdzie $||j||_m = \{km + j \ : \ k \in \mathbb{Z}\}$ dla $j = 0, 1, \ldots, m-1$.

W szczególności dla $m = 2$ mamy, że każda liczba całkowita jest postaci $2k$ (tzn. jest parzysta) albo jest postaci $2k+1$ (tzn. 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 $\{3k+2 : k \in \mathbb{Z}\}$.

Twierdzenie 1.4. (O dzieleniu z resztą). *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 1.1. Niech $b < 0$. Wtedy $m = -b \in \mathbb{N}$. Weźmy dowolne $a \in \mathbb{Z}$. Wtedy z twierdzenia 1.1 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 1.1 mamy, że $-q = x$ i $s = r$, więc $q = -x$. Kończy to nasz dowód. □

1.2 Określenie i własności podzielności liczb całkowitych

Definicja 1.5. 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 1.6. Dla dowolnej liczby całkowitej a mamy, że

(1) $a \mid a$ (gdyż $a = a \cdot 1$), tzn. każda liczba całkowita dzieli siebie,

(2) $a \mid 0$ (gdyż $0 = a \cdot 0$), tzn. 0 jest podzielne przez każdą liczbę całkowitą,

(3) $1 \mid a$ (gdyż $a = 1 \cdot a$), tzn. 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 $a = 0$), tzn. 0 jest jedyną liczbą całkowitą podzielną przez 0.

Twierdzenie 1.7. *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 $n \in \mathbb{Z}$. Na mocy 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 $j - i = (l-k)m$. Ponadto mamy, że $0 < j-i \leqslant j < m$, 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.

□

Wniosek 1.8. *Liczba całkowita a jest podzielna przez liczbę naturalną m wtedy i tylko wtedy, gdy $[a]_m = 0$.*

Dowód. Niech $m \mid a$. Wtedy $a = qm$ dla pewnego $q \in \mathbb{Z}$, skąd $a = qm + 0$ i z twierdzenia o dzieleniu z resztą wynika, że $[a]_m = 0$. Na odwrót, niech $[a]_m = 0$. Wtedy z twierdzenia o dzieleniu z resztą otrzymujemy, że $a = qm + 0 = qm$, czyli $m \mid a$. □

Stwierdzenie 1.9. *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 $c = a \cdot (t \cdot s)$. Ponadto $t \cdot s$ 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 całkowitych x, y 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 $t \in \mathbb{Z}$ 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 1.6 i stwierdzenie 1.9 (4) redukują badanie podzielności liczb całkowitych do badania podzielności przez liczby naturalne.

Stwierdzenie 1.10. *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 $t \in \mathbb{Z}$. Ponadto $m, n > 0$, 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 $m = n$. □

1.3 Największy wspólny dzielnik i najmniejsza wspólna wielokrotność

Niech X będzie podzbiorem zbioru $\mathbb{Z}$ zawierającym co najmniej jedną niezerową liczbę a. Oznaczmy przez D_X zbiór wszystkich wspólnych dzielników naturalnych wszystkich liczb ze zbioru X, czyli

$$D_X = \{d \in \mathbb{N} \,:\, d \mid x \text{ dla każdego } x \in X\}.$$

Na mocy przykładu 1.6, $1 \in D_X$. Ponadto, jeśli $d \in D_X$, to $d \mid a$, skąd $d \mid |a|$, a ponieważ $|a| \in \mathbb{N}$, więc $d \leqslant |a|$ na mocy stwierdzenia 1.10. Wobec tego z zasady maksimum wynika, że w zbiorze D_X istnieje liczba największa, którą nazywamy **największym wspólnym dzielnikiem** liczb ze zbioru X i oznaczamy symbolem $\mathrm{NWD}(X)$. Oczywiście, $\mathrm{NWD}(X) = \mathrm{NWD}(\{|x| \,:\, x \in X\})$ oraz $\mathrm{NWD}(X) = \mathrm{NWD}(X \setminus \{0\})$. Jeżeli $X = \{a_1, a_2, \ldots, a_n\}$ dla pewnego $n \in \mathbb{N}$, to

zamiast $\mathrm{NWD}(\{a_1, a_2, \ldots, a_n\})$ będziemy pisali $\mathrm{NWD}(a_1, a_2, \ldots, a_n)$. Ze stwierdzenia 1.10 wynika, że $\mathrm{NWD}(a) = |a|$ dla każdego $0 \neq a \in \mathbb{Z}$.

Twierdzenie 1.11. *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*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = \mathrm{NWD}(a_1, a_2, \ldots, a_n).$$

Dowód. Oznaczmy przez A zbiór wszystkich liczb postaci $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ 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 $i = 1, 2, \ldots, n$. Jednak 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 $d = a_1u_1 + a_2u_2 + \ldots + a_nu_n$ dla pewnych $u_1, u_2, \ldots, u_n \in \mathbb{Z}$. Weźmy dowolne $a \in A$. Wtedy $a = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ dla pewnych $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ oraz na mocy 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 $D \leqslant d$. Mamy 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 1.12. Powiemy, że liczby całkowite $a_1, a_2, ..., a_k$, gdzie $k \geqslant 2$, są **względnie pierwsze**, jeżeli $\mathrm{NWD}(a_1, a_2, ..., a_k) = 1$.

Twierdzenie 1.13. (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. Na mocy twierdzenia 1.11 istnieją liczby całkowite x i y takie, że $a \cdot x + b \cdot y = 1$. Zatem $c = acx + bcy$. Dodatkowo $a \mid b \cdot c$, więc z przykładu 1.6 i ze stwierdzenia 1.9 mamy, że $a \mid (acx + bcy)$, czyli $a \mid c$. □

Twierdzenie 1.14. *Jeżeli liczby całkowite $a_1, a_2, ..., a_k$, z których co najmniej jedna jest różna od zera, 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 $a_i = (dt)c_i$ 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 1.15. *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. Wtedy $q = \frac{x}{y}$ dla pewnych $x \in \mathbb{Z}$ i $y \in \mathbb{N}$. Niech $d = \mathrm{NWD}(x, y)$. Wówczas na mocy twierdzenia 1.14, $x = ad$ 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 $s \mid b$. Ponadto $b, s \in \mathbb{N}$, więc $b \leqslant s$ i $s \leqslant b$, skąd $b = s$. Wobec tego $as = sr$ i po skróceniu przez s, $a = r$. □

Lemat 1.16. *Niech $a, a_1, a_2, \ldots, a_n, q_1, q_2, \ldots, q_n \in \mathbb{Z}$ i $a \neq 0$. Wówczas zachodzi wzór:*

$$\mathrm{NWD}(a, a_1, a_2, \ldots, a_n) = \mathrm{NWD}(a, a_1 - q_1 a, a_2 - q_2 a, \ldots, a_n - q_n a).$$

Dowód. Wystarczy wykazać, że dla $X = \{a, a_1, a_2, \ldots, a_n\}$ i $Y = \{a, a_1 - q_1 a, a_2 - q_2 a, \ldots, a_n - q_n a\}$ jest $D_X = D_Y$. Dodatkowo, jeśli $d \in D_X$, to $d \in \mathbb{N}$ i $d \mid a$ oraz $d \mid a_i$ dla $i = 1, 2, \ldots, n$, skąd na mocy stwierdzenia 1.9, $d \mid a_i - q_i a$ dla $i = 1, 2, \ldots, n$, czyli $d \in D_Y$. Podobnie, jeśli $d \in D_Y$, to $d \in \mathbb{N}$ i $d \mid a$ oraz $d \mid a_i - q_i a$ dla $i = 1, 2, \ldots, n$, skąd na mocy stwierdzenia 1.9, $d \mid a_i$ dla $i = 1, 2, \ldots, n$, a to oznacza, że $d \in D_X$. □

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 1.17. Na mocy algorytmu Euklidesa otrzymujemy, że

$$\begin{gathered}\mathrm{NWD}(-42,-58,72)=\mathrm{NWD}(42,58,72)=\\ =\mathrm{NWD}(42,58-42,72-42)=\mathrm{NWD}(42,16,30)=\mathrm{NWD}(16,30,42)=\\ =\mathrm{NWD}(16,30-16,42-2\cdot 16)=\mathrm{NWD}(16,14,10)=\\ =\mathrm{NWD}(10,14,16)=\mathrm{NWD}(10,14-10,16-10)=\\ =\mathrm{NWD}(10,4,6)=\mathrm{NWD}(4,6,10)=\mathrm{NWD}(4,6-4,10-2\cdot 4)=\\ =\mathrm{NWD}(4,2,2)=2,\end{gathered}$$

bo $2 \mid 2$ i $2 \mid 4$.

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 $\mathrm{NWW}(a_1, \ldots, a_k)$.

Twierdzenie 1.18. *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 na mocy twierdzenia o dzieleniu z resztą istnieją liczby całkowite q, r takie, że $M = q \cdot m + r$ oraz $0 \leqslant r < m$. Wtedy ze stwierdzenia 1.9 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 1.9 uzyskujemy, że $a_i \mid a$ dla każdego $i = 1, \ldots, k$. □

Twierdzenie 1.19. *Niech $X \neq \{0\}$ będzie niepustym podzbiorem zbioru $\mathbb{Z}$. Wówczas każdy wspólny dzielnik liczb ze zbioru X jest dzielnikiem* $\mathrm{NWD}(X)$.

Dowód. Niech $D = \mathrm{NWD}(X)$ i niech d będzie wspólnym dzielnikiem liczb ze zbioru X. Z przykładu 1.6 i ze stwierdzenia 1.9 wynika, że bez zmniejszania ogólności możemy zakładać, że d jest liczbą naturalną. Dla każdego $x \in X$ mamy, że $D \mid x$ i $d \mid x$, więc na mocy twierdzenia 1.18, $\mathrm{NWW}(D, d) \mid x$. Stąd i z dowolności x, $\mathrm{NWW}(D, d) \in D_X$. Zatem $\mathrm{NWW}(D, d) \leqslant D$. Jednak $D \mid \mathrm{NWW}(D, d)$, więc ze stwierdzenia 1.10 mamy, że $D \leqslant \mathrm{NWW}(D, d)$. Stąd $D = \mathrm{NWW}(D, d)$. Ponadto d dzieli $\mathrm{NWW}(D, d)$, więc $d \mid D$. □

Twierdzenie 1.20. *Dla dowolnych liczb naturalnych a i b zachodzi wzór:*

$$a \cdot b = \mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b). \tag{1.1}$$

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 na mocy twierdzenia 1.18 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 $\mathrm{NWD}(a,b) \cdot$ $\cdot \mathrm{NWW}(a,b) = d \cdot kld = (kd) \cdot (ld) = ab$. □

Twierdzenie 1.21. *Jeżeli $X \neq \{0\}$ i $Y \neq \{0\}$ są niepustymi podzbiorami zbioru $\mathbb{Z}$, to zachodzi wzór:*

$$\mathrm{NWD}(X \cup Y) = \mathrm{NWD}(\mathrm{NWD}(X), \mathrm{NWD}(Y)).$$

Dowód. Oznaczmy $d = \mathrm{NWD}(X \cup Y)$, $d_1 = \mathrm{NWD}(X)$, $d_2 = \mathrm{NWD}(Y)$ i $D = \mathrm{NWD}(d_1, d_2)$. Wtedy $d, d_1, d_2, D \in \mathbb{N}$. Weźmy dowolne $x \in X$. Wtedy $d_1 \mid x$ i $D \mid d_1$, więc $D \mid x$. Podobnie $D \mid y$ dla $y \in Y$. Stąd $D \mid a$ dla każdego $a \in X \cup Y$ i wobec tego $D \leqslant d$. Dodatkowo $X \subseteq X \cup Y$, więc $d \mid x$ dla każdego $x \in X$ i na mocy twierdzenia 1.19, $d \mid d_1$. Analogicznie pokazujemy, że $d \mid d_2$. Wobec tego na mocy twierdzenia 1.19, $d \mid \mathrm{NWD}(d_1, d_2)$, czyli $d \mid D$, skąd $d \leqslant D$ i ostatecznie $d = D$. □

Twierdzenie 1.22. *Jeżeli $X \neq \emptyset$ i $Y \neq \emptyset$ są skończonymi podzbiorami zbioru $\mathbb{Z}$ takimi, że $0 \notin X$ i $0 \notin Y$, to zachodzi wzór:*

$$\mathrm{NWW}(X \cup Y) = \mathrm{NWW}(\mathrm{NWW}(X), \mathrm{NWW}(Y)).$$

Dowód. Oznaczmy $m = \mathrm{NWW}(X \cup Y)$, $m_1 = \mathrm{NWW}(X)$, $m_2 = $ $= \mathrm{NWW}(Y)$ i $M = \mathrm{NWW}(m_1, m_2)$. Wtedy $m, m_1, m_2, M \in \mathbb{N}$. Weźmy dowolne $x \in X$. Wtedy $x \mid m_1$ i $m_1 \mid M$, więc $x \mid M$. Podobnie $y \mid M$ dla $y \in Y$. Stąd $a \mid M$ dla każdego $a \in X \cup Y$ i na mocy twierdzenia 1.18, $m \mid M$, skąd $m \leqslant M$. Ponadto $X \subseteq X \cup Y$, więc znowu z twierdzenia 1.18 mamy, że $m_1 \mid m$. Analogicznie pokazujemy, że $m_2 \mid m$. Wobec tego na mocy twierdzenia 1.18, $\mathrm{NWW}(m_1, m_2) \mid m$, czyli $M \mid m$, skąd $M \leqslant m$ i ostatecznie $M = m$. □

Twierdzenie 1.23. *Niech $X \neq \{0\}$ będzie niepustym podzbiorem zbioru $\mathbb{Z}$ i niech $m \in \mathbb{N}$ oraz $mX = \{mx : x \in X\}$. Wówczas* $\mathrm{NWD}(mX) = m \cdot \mathrm{NWD}(X)$.

Dowód. Oznaczmy $d = \mathrm{NWD}(X)$ i $D = \mathrm{NWD}(mX)$. Dla $x \in X$ mamy, że $d \mid x$, więc ze stwierdzenia 1.9 dostajemy, że $md \mid mx$. Wobec

tego $md \leqslant D$ i na mocy twierdzenia 1.19, $md \mid D$, czyli $D = mdt$ dla pewnego $t \in \mathbb{N}$. Jednak to oznacza, że $mdt \mid mx$ dla każdego $x \in X$, czyli $dt \mid x$ na mocy stwierdzenia 1.9. Z dowolności $x \in X$ wnosimy, że $dt \leqslant d$, czyli $t = 1$ i $D = md$. □

Twierdzenie 1.24. *Niech $a_1, a_2, \ldots, a_n$ będą niezerowymi liczbami całkowitymi. Wówczas dla dowolnej liczby naturalnej d zachodzi wzór:*

$$\mathrm{NWW}(d \cdot a_1, d \cdot a_2, \ldots, d \cdot a_n) = d \cdot \mathrm{NWW}(a_1, a_2, \ldots, a_n). \qquad (1.2)$$

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 1.9 (5): $(d \cdot a_i) \mid (d \cdot m)$ dla $i = 1, \ldots, n$. Zatem z twierdzenia 1.18 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 1.18 uzyskujemy, że $m \mid s$. Tymczasem $s \mid m$, więc na mocy stwierdzenia 1.10, $m = s$, czyli $t = 1$. Stąd $d \cdot m = M$. □

Stwierdzenie 1.25. *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 niech $d = \mathrm{NWD}(a, a_1 a_2)$. 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 $\mathrm{NWD}(a, a_1 a_2) = 1$ 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 $\mathrm{NWD}(a, a_1 \cdot \ldots \cdot a_n) = 1$. Jednakże $\mathrm{NWD}(a, a_{n+1}) = 1$, 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 1.26. *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 1.20. 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 1.22, $\mathrm{NWW}(a_1, a_2, \ldots, a_n, a_{n+1}) = \mathrm{NWW}(a_1 \cdot a_2 \cdot \ldots \cdot a_n, a_{n+1})$. Ponadto ze stwierdzenia 1.25 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 1.18 i 1.26 wynika od razu następujący

Wniosek 1.27. *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 1.28. *Niech $a, b, c, n \in \mathbb{N}$. Jeżeli $ab = c^n$ i liczby a i b są względnie pierwsze, to $a = x^n$ i $b = y^n$ dla pewnych $x, y \in \mathbb{N}$.*

Dowód. Oznaczmy $x = \mathrm{NWD}(a, c)$. Wtedy $x \in \mathbb{N}$ i na mocy twierdzenia 1.14, $a = ux$ i $c = yx$ dla pewnych względnie pierwszych liczb naturalnych u i y. Zatem $uxb = y^n x^n$, czyli $ub = y^n x^{n-1}$. Dalej, ze stwierdzenia 1.25 wynika, że $\mathrm{NWD}(y^n, u) = 1$, a ponieważ $y^n \mid ub$, to na mocy zasadniczego twierdzenia arytmetyki uzyskujemy, że $y^n \mid b$. Dodatkowo $\mathrm{NWD}(a, b) = 1$ i $x \mid a$, więc ze stwierdzenia 1.25 mamy, że $\mathrm{NWD}(x^{n-1}, b) = 1$, a ponieważ $x^{n-1} \mid ub$, to znowu z zasadniczego twierdzenia arytmetyki, $x^{n-1} \mid u$. Ponadto $ub = y^n x^{n-1}$, więc u/x^{n-1} i b/y^n są liczbami naturalnymi o iloczynie równym 1, skąd $b = y^n$ i $u = x^{n-1}$, czyli $a = x^n$. □

Twierdzenie 1.29. *Niech $k, n, a_1, a_2, \ldots, a_k, c \in \mathbb{N}$, $k \geqslant 2$ i niech każde dwie spośród liczb $a_1, a_2, \ldots, a_k$ będą względnie pierwsze. Jeżeli $a_1 \cdot a_2 \cdot \ldots \cdot a_k = c^n$, to dla każdego $i = 1, 2, \ldots, k$ istnieje $x_i \in \mathbb{N}$ takie, że $a_i = x_i^n$.*

Dowód. Zastosujemy indukcję ze względu na k. Dla $k = 2$ teza wynika z twierdzenia 1.28. Przypuśćmy, że teza zachodzi dla pewnej liczby naturalnej $k \geqslant 2$ i niech każde dwie spośród liczb naturalnych $a_1, \ldots, a_k$, a_{k+1} będą względnie pierwsze oraz niech $a_1 \cdot \ldots \cdot a_k \cdot a_{k+1} = c^n$ dla pewnych $c, n \in \mathbb{N}$. Na mocy stwierdzenia 1.25 liczby $a_1 \cdot \ldots \cdot a_k$ i a_{k+1} są względnie pierwsze oraz ich iloczyn jest równy c^n, więc z twierdzenia 1.28 otrzymujemy, że $a_1 \cdot \ldots \cdot a_k = x^n$ i $a_{k+1} = x_{k+1}^n$ dla pewnych $x, x_{k+1} \in \mathbb{N}$. Ponadto na mocy założenia indukcyjnego dla każdego $i = 1, 2, \ldots, k$ istnieje $x_i \in \mathbb{N}$ takie, że $a_i = x_i^n$. □

Twierdzenie 1.30. *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 $b^n = a^n \cdot t^n$. Ponadto $t^n \in \mathbb{Z}$, więc $a^n \mid b^n$. Na odwrót, załóżmy, że $a^n \mid b^n$. Niech $d = \mathrm{NWD}(a, b)$. Wtedy z twierdzenia 1.14 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 1.9 uzyskujemy, że $x^n \mid y^n$, więc też $x \mid y^n$. Jednak ze stwierdzenia 1.25 mamy, że $\mathrm{NWD}(x, y^n) = 1$, więc $x = 1$. Zatem $a = d$, skąd $a \mid b$. □

Wniosek 1.31. *Niech $D, n \in \mathbb{N}$ będą takie, że $n \geqslant 2$ i $D \neq a^n$ dla każdego $a \in \mathbb{N}$. Wówczas $\sqrt[n]{D}$ jest liczbą niewymierną.*

Dowód. Załóżmy, że $\sqrt[n]{D}$ jest liczbą wymierną. Wtedy istnieją liczby naturalne a i b takie, że $\sqrt[n]{D} = \frac{b}{a}$. Stąd $D = \frac{b^n}{a^n}$, czyli $b^n = Da^n$. Zatem $a^n \mid b^n$ i na mocy twierdzenia 1.30, $a \mid b$, skąd $b = ac$ dla pewnego $c \in \mathbb{N}$ i $D = c^n$, co prowadzi do sprzeczności.

Wobec tego liczba rzeczywista $\sqrt[n]{D}$ jest niewymierna. □

1.4 Liczby pierwsze

Przez dzielnik liczby naturalnej n będziemy rozumieli od tej pory liczbę naturalną dzielącą n. Przez D_n będziemy oznaczać zbiór wszystkich dzielników liczby n.

Definicja 1.32. 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 1.33. Liczba 1 nie jest ani pierwsza ani złożona, gdyż ze stwierdzenia 1.10 mamy, że $D_1 = \{1\}$, tzn. liczba 1 posiada dokładnie jeden dzielnik.

Uwaga 1.34. Na mocy przykładu 1.6 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 1.35. Wobec uwagi 1.34 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 1.36. 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 1.35 n jest liczbą złożoną. Natomiast dla $k = 1$ mamy, że $n = 2$, więc z przykładu 1.6 i ze stwierdzenia 1.10: $D_2 = \{1, 2\}$, czyli liczba 2 jest pierwsza. Zatem 2 jest też najmniejszą liczbą pierwszą.

Twierdzenie 1.37. *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 1.6, $n \in A$. 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 1.9 uzyskujemy, że $d \in A$ oraz ze stwierdzenia 1.10: $d \leqslant p$. Zatem z minimalności p jest $d = p$. Stąd p jest liczbą pierwszą. □

Twierdzenie 1.38. *Zbiór wszystkich liczb pierwszych jest nieskończony.*

Dowód. Załóżmy, że tak nie jest, i nich $p_1 = 2, p_2, \ldots, p_n$ będą wszystkimi liczbami pierwszymi. Niech $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Wtedy a jest liczbą naturalną większą od 1, więc z twierdzenia 1.37 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 1.9, $p_i \mid 1$, skąd ze stwierdzenia 1.10, $p_i \leqslant 1$ i mamy sprzeczność. Przypuszczenie, że zbiór wszystkich liczb pierwszych jest skończony doprowadziło nas do sprzeczności. Zatem ten zbiór jest nieskończony. □

Twierdzenie 1.39. *Każda liczba złożona n ma dzielnik pierwszy p taki, że $p^2 \leqslant n$.*

Dowód. Niech n będzie liczbą złożoną. Wtedy z uwagi 1.35 istnieją liczby naturalne a, b takie, że $1 < a \leqslant b$ oraz $n = a \cdot b$. Zatem z twierdzenia 1.37 istnieje liczba pierwsza p dzieląca liczbę a. Dodatkowo $a \mid n$, więc ze stwierdzenia 1.9, $p \mid n$. Ponadto $p \leqslant a$ na mocy stwierdzenia 1.10, więc $p^2 \leqslant a^2 \leqslant a \cdot b = n$, czyli $p^2 \leqslant n$. □

Stwierdzenie 1.40. *Niech p będzie liczbą pierwszą i niech $a \in \mathbb{Z}$. Wówczas:*

$$\mathrm{NWD}(p, a) = 1 \iff p \nmid a. \tag{1.3}$$

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 1.41. *Jeżeli $n \geqslant 2$ i liczba pierwsza p dzieli iloczyn $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ liczb całkowitych $a_1, a_2, \ldots, a_n$, to $p \mid a_i$ dla pewnego $i = 1, 2, \ldots, n$.*

Dowód. Załóżmy, że tak nie jest dla pewnej liczby pierwszej p. Wtedy istnieją: liczba naturalna $n \geqslant 2$ oraz 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 1.40, $\mathrm{NWD}(p, a_i) = 1$ dla $i = 1, \ldots, n$. Zatem ze stwierdzenia 1.25, $\mathrm{NWD}(p, a_1 \cdot a_2 \cdot \ldots \cdot a_n) = 1$, co przeczy temu, że $p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_n)$. □

Uwaga 1.42. Niech $p_1, p_2, \ldots, p_s$ będą różnymi liczbami pierwszymi i niech $\alpha_1, \alpha_2, \ldots, \alpha_s$ będą liczbami naturalnymi. Wtedy jedynymi dzielnikami pierwszymi liczby $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ są: $p_1, p_2, \ldots, p_s$. 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 1.41 wynika, że $p \mid p_i$ dla pewnego $i = 1, \ldots, s$, skąd z pierwszości p i p_i, $p = p_i$. □

Uwaga 1.43. 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 na mocy twierdzenia 1.41, $p \mid p_i^{\alpha_i}$ dla pewnego $i = 1, \ldots, s$. Stąd z uwagi 1.42 mamy, że $\alpha_i = 0$, więc $p \mid 1$, czyli $p = 1$ i mamy sprzeczność.

Twierdzenie 1.44. *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 1.43. □

Twierdzenie 1.45. (O jednoznaczności rozkładu). *Każda liczba naturalna $n > 1$ może być przedstawiona w postaci*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \tag{1.4}$$

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 (1.4) *jest jednoznaczne, tzn. 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 (1.4). Wtedy z zasady minimum istnieje wśród nich liczba najmniejsza $n_0 > 1$. Z twierdzenia 1.37 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 (1.4).

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 1.42 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 1.44 mamy, że $\alpha_i = \beta_i$ dla $i = 1, 2, \ldots, k$. □

Przedstawienie liczby naturalnej $n > 1$ w postaci (1.4) nazywamy jej **rozkładem kanonicznym**.

Liczba 1 nie posiada rozkładu kanonicznego, ale dla dowolnych różnych liczb pierwszych $p_1, \ldots, p_s$ mamy, że $1 = p_1^0 \cdot \ldots \cdot p_s^0$.

Stwierdzenie 1.46. *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 1.37 istnieje liczba pierwsza p będąca dzielnikiem d i wtedy ze stwierdzenia 1.9 liczba p jest wspólnym dzielnikiem liczb $a_1, \ldots, a_n$. □

Z uwagi 1.43 oraz z twierdzeń 1.44 i 1.45 wynika od razu następujące

Stwierdzenie 1.47. *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.*

Twierdzenie 1.48. (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 1.43, $p \in \{p_1, \ldots, p_k\}$. Zatem z twierdzenia 1.45 oraz z uwagi 1.43 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 1.44 uzyskujemy, że $\beta_i + \gamma_i = \alpha_i$, skąd $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, \ldots, k$. □

Liczbę wszystkich dzielników liczby naturalnej n będziemy oznaczali przez $\Theta(n)$.

Stwierdzenie 1.49. (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*

$$\Theta\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right) = (1 + \alpha_1) \cdot (1 + \alpha_2) \cdot \ldots \cdot (1 + \alpha_k). \qquad (1.5)$$

Dowód. Z twierdzeń 1.44 i 1.48 wynika od razu, że dla $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, $\Theta(n)$ jest równe liczbie wszystkich ciągów $(\beta_1, \ldots, \beta_k)$ takich, że $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, \ldots, k$, czyli $\Theta(n) = (1 + \alpha_1) \cdot (1 + \alpha_2) \cdot \ldots \cdot (1 + \alpha_k)$. □

Twierdzenie 1.50. *Jeżeli p jest liczbą pierwszą, to $p \mid \binom{p}{k}$ dla $k = 1, \ldots, p-1$.*

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 1.10 mamy, że p nie dzieli j dla $j = 1, \ldots, p-1$. Zatem z twierdzenia 1.41 mamy, że p nie dzieli $k!$ oraz p nie dzieli $(p-k)!$. Jednakże $p! = 1 \cdot 2 \cdot \ldots \cdot p$, więc $p \mid p!$. Zatem z twierdzenia 1.41 otrzymujemy, że $p \mid n_k$. □

Zadanie 1.51. Stosując twierdzenie 1.50 udowodnij, że dla dowolnej liczby pierwszej p i dowolnej liczby naturalnej n, $p \mid n^p - n$.

Zadanie 1.52. Niech $F_n = 2^{2^n} + 1$ dla $n \in \mathbb{N}_0$. Udowodnij, że $F_0 \cdot F_1 \cdot \ldots \cdot F_n + 2 = F_{n+1}$ dla każdego $n \in \mathbb{N}$ i wyprowadź stąd twierdzenie Goldbacha które mówi, że dla dowolnych różnych $n, m \in \mathbb{N}_0$ liczby F_n i F_m są względnie pierwsze.

Zadanie 1.53. Stosując zadanie 1.52 i twierdzenie 1.37 udowodnij, że zbiór wszystkich liczb pierwszych jest nieskończony.

Rozdział 2

Kongruencje i ich zastosowania

2.1 Kongruencje

Definicja 2.1. 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).

Stwierdzenie 2.2. *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) $[a]_m = [b]_m$.

Dowód. Równoważność warunków (i) oraz (ii) wynika wprost z Definicji 2.1. Niech $m \mid a - b$. Wtedy $a - b = qm$ dla pewnego $q \in \mathbb{Z}$. Ponadto z twierdzenia o dzieleniu z resztą uzyskujemy, że $a = xm + [a]_m$ i $b = ym + [b]_m$ dla pewnych $x, y \in \mathbb{Z}$. Stąd $xm + [a]_m = a = b + qm = (y + q)m + [b]_m$ i znowu z twierdzenia o dzieleniu z resztą wynika, że $[a]_m = [b]_m$. Na odwrót, niech $[a]_m = [b]_m$. Wtedy z twierdzenia o dzieleniu z resztą mamy, że $a = xm + [a]_m$ i $b = ym + [a]_m$ dla pewnych $x, y \in \mathbb{Z}$. Zatem $a - b = (x - y)m$, czyli $m \mid a - b$. □

Stwierdzenie 2.3. *Dla dowolnej liczby naturalnej m i dla dowolnych liczb całkowitych a, b, c:*
(i) $a \equiv a \pmod{m}$,
(ii) jeżeli $a \equiv b \pmod{m}$, *to* $b \equiv a \pmod{m}$,
(iii) jeżeli $a \equiv b \pmod{m}$ *i* $b \equiv c \pmod{m}$, *to* $a \equiv c \pmod{m}$.

Dowód. Ponieważ $[a]_m = [a]_m$, więc na mocy stwierdzenia 2.2, $a \equiv a \pmod{m}$. Załóżmy, że $a \equiv b \pmod{m}$. Wtedy $[a]_m = [b]_m$, więc $[b]_m = [a]_m$ i ze stwierdzenia 2.2, $b \equiv a \pmod{m}$.

Załóżmy, że $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$. Wtedy ze stwierdzenia 2.2, $[a]_m = [b]_m$ i $[b]_m = [c]_m$, więc $[a]_m = [c]_m$ i ze stwierdzenia 2.2, $a \equiv c \pmod{m}$. □

Klasą reszt modulo m o reprezentancie $a \in \mathbb{Z}$ nazywamy zbiór

$$||a||_m = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}. \tag{2.1}$$

Stwierdzenie 2.4. *Niech $m \in \mathbb{N}$ i niech $a, b \in \mathbb{Z}$. Wtedy:*
(i) $a \in ||a||_m$,
(ii) $||a||_m = ||b||_m \iff a \equiv b \pmod{m}$.
W szczególności dowolne dwie klasy reszt modulo m są albo równe, albo rozłączne.

Dowód. (i). Na mocy stwierdzenia 2.3 (i) mamy, że $a \equiv a \pmod{m}$, więc $a \in ||a||_m$.

(ii). Niech $||a||_m = ||b||_m$. Ponieważ $a \in ||a||_m$ na mocy (i), więc $a \in ||b||_m$, czyli $a \equiv b \pmod{m}$. Na odwrót, załóżmy, że $a \equiv b \pmod{m}$. Wtedy ze stwierdzenia 2.3 (ii) mamy, że $b \equiv a \pmod{m}$. Weźmy dowolne $t \in ||a||_m$. Wtedy $t \equiv a \pmod{m}$. Dodatkowo $a \equiv b \pmod{m}$, więc ze stwierdzenia 2.3 (iii), $t \equiv b \pmod{m}$, czyli $t \in ||b||_m$. Analogicznie, jeśli $t \in ||b||_m$, to $t \equiv b \pmod{m}$, a ponieważ $b \equiv a \pmod{m}$, więc $t \equiv a \pmod{m}$ na mocy stwierdzenia 2.3 (iii), skąd $t \in ||a||_m$. Wobec tego $||a||_m = ||b||_m$.

Weźmy dowolne $a, b \in \mathbb{Z}$ takie, że $||a||_m \cap ||b||_m \neq \emptyset$. Wtedy istnieje $x \in \mathbb{Z}$ takie, że $x \in ||a||_m$ i $x \in ||b||_m$. Zatem $x \equiv a \pmod{m}$ i $x \equiv b \pmod{m}$. Stąd $b \equiv x \pmod{m}$ na mocy stwierdzenia 2.3 (ii). Zatem $b \equiv x \pmod{m}$ i $x \equiv a \pmod{m}$, a to oznacza na mocy

stwierdzenia 2.3 (*iii*), że $b \equiv a \pmod{m}$. Wobec tego $||a||_m = ||b||_m$ z pierwszej części dowodu. □

Dla liczb naturalnych m oznaczmy przez $\mathbb{Z}_m$ zbiór wszystkich reszt z dzielenia przez m. Zatem:

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}. \tag{2.2}$$

Ze stwierdzenia 2.2 wynika, że dla dowolnych $m \in \mathbb{N}$ i $a \in \mathbb{Z}$:

$$||a||_m = \{x \in \mathbb{Z} : [x]_m = [a]_m\} = \{qm + a : q \in \mathbb{Z}\}. \tag{2.3}$$

Stwierdzenie 2.5. *Każda kongruencja według modułu m posiada dokładnie m klas reszt modulo m i są one postaci:*

$$||r||_m = \{qm + r : q \in \mathbb{Z}\} = \{a \in \mathbb{Z} : [a]_m = r\}, \quad \text{gdzie } r \in \mathbb{Z}_m. \tag{2.4}$$

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 $||a||_m = ||r||_m$ na mocy stwierdzenia 2.4. Niech $r, s \in \{0, 1, \ldots, m-1\}$ będą takie, że $||r||_m = ||s||_m$. Wtedy na mocy stwierdzenia 2.4 mamy, że $r \equiv s \pmod{m}$, więc $[r]_m = [s]_m$ na mocy stwierdzenia 2.2, czyli $r = s$, bo $r, s \in \mathbb{Z}_m$. Wobec tego zbiory (2.4) są parami różne i jest ich dokładnie $(m-1)+1 = m$. □

Dużą zaletą kongruencji jest to, że posiadają one podobne własności jak relacja równości. Wyraża to następujące

Twierdzenie 2.6. *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. Niech $a \equiv b \pmod m$. Wtedy $m \mid a - b$ i $(a + c) - (b + c) = a - b$, więc $a + c \equiv b + c \pmod m$. Ponadto $a \cdot c - b \cdot c = (a - b) \cdot c$, więc $m \mid a \cdot c - b \cdot c$, czyli $a \cdot c \equiv b \cdot c \pmod m$, co dowodzi punktów (i) oraz (ii).

(iii). Z założenia $a_i - b_i = q_i m$, gdzie $q_i \in \mathbb{Z}$ dla $i = 1, 2, \ldots, n$. Zatem $(a_1 + \ldots + a_n) - (b_1 + \ldots + b_n) = (q_1 + \ldots + q_n)m$. Stąd i na mocy stwierdzenia 2.2, $a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n \pmod m$.

(iv). Zastosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista. Dla $n = 2$ mamy, że $a_1 \equiv b_1 \pmod m$ i $a_2 \equiv b_2 \pmod m$. Zatem na mocy (i), $a_1 a_2 \equiv b_1 a_2 \pmod m$ i $b_1 a_2 \equiv b_1 b_2 \pmod m$, skąd $a_1 a_2 \equiv b_1 b_2 \pmod m$ na mocy stwierdzenia 2.3. Przypuśćmy teraz, że teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ i niech $a_i \equiv b_i \pmod m$ dla $i = 1, \ldots, n, n + 1$. Wtedy $a_{n+1} \equiv b_{n+1} \pmod m$ i z założenia indukcyjnego $a_1 \cdot \ldots \cdot a_n \equiv b_1 \cdot \ldots \cdot b_n \pmod m$, więc z kroku dowodu dla $n = 2$, $a_1 \cdot \ldots a_n \cdot a_{n+1} \equiv b_1 \cdot \ldots \cdot b_n \cdot b_{n+1} \pmod m$.

(v). Podstawiając $a_i = a$ oraz $b_i = b$ dla $i = 1, 2, \ldots, n$ w punkcie (iv) uzyskujemy, że $a^n \equiv b^n \pmod m$.

(vi). Na mocy (v), $a^k \equiv b^k \pmod m$, skąd na mocy (i), $c_k a^k \equiv c_k b^k \pmod m$ dla każdego $k = 0, 1, \ldots, s$. Stąd po dodaniu stronami tych kongruencji (punkt (iii)!) uzyskujemy tezę. □

Skracanie kongruencji jest bardziej subtelne niż skracanie równości. Mówi o tym następujące

Twierdzenie 2.7. *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* $a \equiv b \pmod m$.

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 1.9, $n \mid a-b$, czyli $a \equiv b \pmod{n}$.

(iii). Niech $\mathrm{NWD}(c,m)=1$ i $a \cdot c \equiv b \cdot c \pmod{m}$. Wtedy m dzieli $ac-bc$, 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 2.6 (ii). □

Twierdzenie 2.8. *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 1.27 otrzymujemy, że $m_1 \cdot m_2 \cdot \ldots \cdot m_s \mid a-b$, skąd uzyskujemy, że $a \equiv b \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_s}$. Implikacja odwrotna wynika od razu z twierdzenia 2.7 (ii). □

Lemat 2.9. *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 1.11 otrzymujemy, że $ax+my=1$ 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 2.3, $ay \equiv ax \pmod{m}$ i z twierdzenia 2.7 (iii) mamy, że $y \equiv x \pmod{m}$. Jeżeli zaś $y \equiv x \pmod{m}$, to ze stwierdzenia 2.2 (ii) uzyskujemy, że $ay \equiv ax \pmod{m}$, więc $ay \equiv 1 \pmod{m}$ na mocy stwierdzenia 2.3. □

2.2 Ważne twierdzenia o kongruencjach

Twierdzenie 2.10. (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 1.25, $\mathrm{NWD}(M_i, m_i) = 1$. Zatem z lematu 2.9 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 2.6 (ii), $M_i x_i r_i \equiv r_i \pmod{m_i}$, a zatem na mocy stwierdzenia 2.3, $r \equiv r_i \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, s$.

Ostatnia część naszego twierdzenia wynika od razu z twierdzenia 2.8. □

Definicja 2.11. 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 liczbą naturalną n, nazywamy **funkcją Eulera**.

Przykład 2.12. Wprost z definicji mamy, że $\varphi(1) = 1$. Jeśli zaś liczba naturalna $n > 1$, to $\varphi(n) \in \mathbb{N}$ i $\mathrm{NWD}(n, n) = n > 1$, skąd $\varphi(n) < n$. 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 1.40. Jednak $\mathrm{NWD}(p, p) > 1$, więc stąd $\varphi(p) = p - 1$. W szczególności: $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, i tak dalej. 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 2.13. (Euler). *Jeżeli liczba całkowita a jest względnie pierwsza z liczbą naturalną m, to*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2.5}$$

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 wiekszymi 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. Dodatkowo $\mathrm{NWD}(a, m) = 1$, więc na mocy stwierdzenia 1.25 mamy, że $\mathrm{NWD}(a \cdot r_i, m) = 1$ 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 lematu 1.16 uzyskujemy, że $\mathrm{NWD}([ar_i]_m, m) = \mathrm{NWD}(ar_i, m)$, 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 2.2, $ar_i \equiv ar_j \pmod{m}$. Stąd $r_i \equiv r_j \pmod{m}$ na mocy twierdzenia 2.7 (*iii*). Zatem ze stwierdzenia 2.2, $[r_i]_m = [r_j]_m$. Ponadto $r_i, r_j \in \mathbb{Z}_m$, 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 $[ar_1]_m \cdot [ar_2]_m \cdot \ldots \cdot [ar_s]_m = r_1 \cdot r_2 \cdot \ldots \cdot r_s$ i $ar_i \equiv [ar_i]_m \pmod{m}$ dla każdego $i = 1, 2, \ldots, s$, więc na mocy twierdzenia 2.6 (*iv*) mamy, że $(ar_1) \cdot (ar_2) \cdot \ldots \cdot (ar_s) \equiv [ar_1]_m \cdot [ar_2]_m \cdot \ldots \cdot [ar_s]_m \pmod{m}$, 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 1.25 liczby $r_1 \cdot r_2 \cdot \ldots \cdot r_s$ i m są względnie pierwsze, więc na mocy twierdzenia 2.7 (*iii*), $a^s \equiv 1 \pmod{m}$, czyli $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Z twierdzenia Eulera oraz ze stwierdzenia 1.40 i przykładu 2.12 uzyskujemy od razu następujący rezultat nazywany **Małym twierdzeniem Fermata**:

Twierdzenie 2.14. *Dla dowolnej liczby całkowitej a niepodzielnej przez liczbę pierwszą p zachodzi wzór:*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.6}$$

Twierdzenie 2.15. *Jeżeli liczba pierwsza p jest postaci $4k+3$ i dzieli sumę kwadratów dwóch liczb całkowitych a i b, to $p \mid a$ i $p \mid b$.*

Dowód. Ponieważ $p \mid a^2 + b^2$, więc jeśli $p \mid a$, to $p \mid b^2$, skąd $p \mid b$. Podobnie, jeśli $p \mid b$, to $p \mid a$. Przypuśćmy zatem, że $p \nmid a$. Wtedy $p \nmid b$ i z Małego twierdzenia Fermata, $a^{p-1} \equiv 1 \pmod{p}$ oraz $b^{p-1} \equiv \equiv 1 \pmod{p}$. Ponadto $p = 4k+3$ dla pewnego $k \in \mathbb{N}_0$ i $a^2 \equiv -b^2 \pmod{p}$, więc po podniesieniu tej kongruencji stronami do potęgi $2k+1$ uzyskamy, że $a^{p-1} \equiv -b^{p-1} \pmod{p}$, gdyż $(-1)^{2k+1} = -1$ oraz $2(2k+ +1) = 4k+2 = p-1$. Zatem $1 \equiv -1 \pmod{p}$, skąd $p \mid 2$, co prowadzi do sprzeczności. Wobec tego $p \mid a$ i $p \mid b$. □

Uwaga 2.16. 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 2.17. *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

$$F(a) = ([a]_m, [a]_n). \tag{2.7}$$

Z chińskiego twierdzenia 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 $a \leqslant \mathbb{Z}_{mn}$. Jeżeli $\mathrm{NWD}(a,m) = = \mathrm{NWD}(a,n) = 1$, to ze stwierdzenia 1.25, $\mathrm{NWD}(a,mn) = 1$. Na odwrót, jeśli $\mathrm{NWD}(a,mn) = 1$, to $\mathrm{NWD}(a,m) = \mathrm{NWD}(a,n) = 1$, bo $\mathrm{NWD}(a,m) | \mathrm{NWD}(a,mn)$ i $\mathrm{NWD}(a,m) | \mathrm{NWD}(a,mn)$. Wobec tego $a \in \mathbb{Z}_{mn}^*$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a,m) = \mathrm{NWD}(a,n) = 1$. Dodatkowo na mocy lematu 1.16 mamy, że $\mathrm{NWD}(a,m) = \mathrm{NWD}([a]_m, m)$

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 oraz z uwagi 2.16, $\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n)$. □

Wniosek 2.18. *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 2.17. 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 1.25 liczby m_{s+1} i $m_1 \cdot \ldots \cdot m_s$ są względnie pierwsze, więc na podstawie twierdzenia 2.17 otrzymujemy, że $\varphi(m_1 \cdot \ldots \cdot m_s \cdot m_{s+1}) = \varphi(m_1 \cdot \ldots \cdot m_s) \cdot \varphi(m_{s+1})$. Ponadto z założenia indukcyjnego mamy równość $\varphi(m_1 \cdot m_2 \cdot \ldots \cdot m_s) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_s)$. Dlatego $\varphi(m_1 \cdot \ldots \cdot m_s \cdot m_{s+1}) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_s) \cdot \varphi(m_{s+1})$. 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 2.19. *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 1.47 i uwagi 1.43 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 1.47 i uwagi 1.43 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 2.18 uzyskujemy tezę. □

Niech m i n będą liczbami naturalnymi i niech f będzie wielomianem o współczynnikach całkowitych stopnia n. Mówimy, że liczba

całkowita a spełnia kongruencję

$$f(x) \equiv 0 \pmod{m}, \tag{2.8}$$

jeżeli $f(a) \equiv 0 \pmod{m}$. Wówczas na mocy twierdzenia 2.6 (vi) każda liczba całkowita b taka, że $b \equiv a \pmod{m}$ też spełnia tę kongruencję. Z tego powodu **rozwiązaniem kongruencji** (2.8) nazywamy każdą klasę abstrakcji

$$||a||_m = \{a + km : k \in \mathbb{Z}\}$$

relacji przystawania według modułu m taką, że $f(a) \equiv 0 \pmod{m}$. W praktyce, rozwiązanie $||a||_m$ zapisujemy wzorem: $x \equiv a \pmod{m}$. Stopień wielomianu f nazywamy **stopniem kongruencji** (2.8). 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:

$$\mathbb{Z} = ||0||_m \cup ||1||_m \cup \ldots \cup ||m-1||_m. \tag{2.9}$$

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 $||a||_d$ przy pomocy klas $||a||_m$, gdzie $d \in \mathbb{N}$ i $d \mid m$. Mówi o tym następujące

Stwierdzenie 2.20. *Niech d będzie naturalnym dzielnikiem liczby naturalnej m. Wówczas dla każdego $a \in \mathbb{Z}$ klasa $||a||_d$ jest sumą $\frac{m}{d}$ parami rozłącznych klas modulo m:*

$$||a||_d = ||a||_m \cup ||a+d||_m \cup \ldots \cup ||a+(\frac{m}{d}-1)d||_m.$$

Dowód. Weźmy dowolną liczbę całkowitą b należącą do prawej strony dowodzonego wzoru. Wtedy $b \in ||a+id||_m$ dla pewnego $i = 0, 1, \ldots, \frac{m}{d}$.

Stąd $b \equiv a + id \pmod{m}$, a ponieważ $d \mid m$, więc z twierdzenia 2.7 (ii) mamy, że $b \equiv a + id \pmod{d}$. Jednak $a + id \equiv a \pmod{d}$, więc $b \equiv a \pmod{d}$, czyli $b \in ||a||_d$. Na odwrót, niech $b \in ||a||_d$. 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 wynika, że $k = q \cdot \frac{m}{d} + r$ 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 $b \in ||a + rd||_m$. To kończy dowód naszego wzoru.

Pozostaje do wykazania, że klasy $||a+id||_m$ i $||a+jd||_m$ 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 $||a + id||_m = ||a + jd||_m$. Wtedy $a + jd \equiv a + id \pmod{m}$, skąd $(j - i)d \equiv 0 \pmod{m}$, więc z twierdzenia 2.7 (i) wynika, że $j - i \equiv 0 \pmod{\frac{m}{d}}$, czyli $\frac{m}{d} \mid j - i$. Ponadto $0 < j - i < \frac{m}{d}$, więc mamy sprzeczność. □

Uwaga 2.21. W praktyce zamiast klasy $||a||_d$ piszemy $x \equiv a \pmod{d}$ i dla wielokrotności m liczby d zapisujemy to za pomocą wzoru: $x \equiv a, a + d, a + 2d, \ldots, a + (\frac{m}{d} - 1)d \pmod{m}$. Czasami mówi się, że stwierdzenie 2.20 podaje metodę podnoszenia rozwiązań kongruencji według modułu d do rozwiązań tej kongruencji według modułu m (oczywiście, gdy $d \mid m$).

Ogólna postać kongruencji liniowej:

$$ax \equiv b \pmod{m}, \tag{2.10}$$

gdzie $a, b \in \mathbb{Z}$, $a \neq 0$ i $m \in \mathbb{N}$.

Twierdzenie 2.22. *Kongruencja liniowa* (2.10) *posiada rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(a, m) \mid b$. *Jeżeli ten warunek jest spełniony, to kongruencja* (2.10) *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* (2.10) *są klasy:*

$$||x_0||_m, ||x_0 + m_1||_m, ||x_0 + 2m_1||_m, \ldots, ||x_0 + (d - 1)m_1||_m,$$

gdzie $d = \mathrm{NWD}(a, m)$ *i* $m_1 = \frac{m}{d}$.

Dowód. Przypuśćmy, że kongruencja (2.10) ma rozwiązanie $||r||_m$. Wtedy $ar \equiv b \pmod{m}$, więc $m \mid ar - b$, czyli $ar - b = km$ dla pewnego $k \in \mathbb{Z}$. Dodatkowo $d \mid a$ 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 1.14, $\mathrm{NWD}(a_1, m_1) = 1$. Kongruencja (2.10) ma zatem postać $da_1x \equiv db_1 \pmod{dm_1}$, więc na mocy twierdzenia 2.7, liczba całkowita spełnia ją wtedy i tylko wtedy, gdy ta liczba spełnia kongruencję $a_1x \equiv b_1 \pmod{m_1}$. Z lematu 2.9 ta ostatnia kongruencja posiada dokładnie jedno rozwiązanie $||x_0||_{m_1}$ i stąd na mocy stwierdzenia 2.20 kongruencja (2.10) posiada dokładnie d rozwiązań, przy czym są to klasy: $||x_0||_m, ||x_0 + m_1||_m, \ldots, ||x_0 + (d-1)m_1||_m$. □

Twierdzenie 2.23. (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 $p \nmid a_n$. 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 2.7 (*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 $f(a) \equiv 0 \pmod{p}$. Ponadto

$$x^k - a^k = (x - a)(x^{k-1} + x^{k-2}a + \ldots + xa^{k-2} + a^{k-1})$$

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 2.7 (*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 $n+1$. □

Twierdzenie 2.24. (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 2.14 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 $a = 1, 2, \ldots, p-1$, więc na mocy twierdzenia Lagrange'a, $p \mid c_i$ dla $i = 1, 2, \ldots, p-2$. Zatem $(p-1)! + 1 \equiv 0 \pmod{p}$, skąd $(p-1)! \equiv -1 \pmod{p}$. □

Wniosek 2.25. *Jeżeli p jest liczbą pierwszą i $p \equiv 1 \pmod{4}$, to $p \mid a^2 + 1$ dla $a = (\frac{p-1}{2})!$.*

Dowód. Dla każdego $i = 1, 2, \ldots, \frac{p-1}{2}$ 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 $(p-1)! = [1\cdot(p-1)]\cdot[2\cdot(p-2)]\cdot\ldots\cdot\left[\frac{p-1}{2}\cdot\left(p - \frac{p-1}{2}\right)\right] \equiv (-1)^{\frac{p-1}{2}}\cdot 1^2\cdot 2^2\cdot\ldots\cdot\left(\frac{p-1}{2}\right)^2 \pmod{p}$. Jednakże $p \equiv 1 \pmod{4}$, 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 2.26. (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 $k < \sqrt{p}$. Ponadto $p > 1$, 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 2.25 mamy, że $a^2 \equiv -1 \pmod{p}$. 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 2.7 (iii) uzyskujemy, że $y \equiv 0 \pmod{p}$. Zatem $y_1 \equiv y_2 \pmod{p}$, skąd $[y_1]_p = [y_2]_p$. Jednakże $y_1, y_2 \in A \subseteq \mathbb{Z}_p$, więc $y_1 = y_2$. Wobec tego $x_1 = x_2$ i $y_1 = y_2$, co przeczy temu, że $(x_1, y_1) \neq (x_2, y_2)$. Wobec tego $x \neq 0$. Dalej, $x \equiv ay \pmod{p}$, więc po podniesieniu do kwadratu, $x^2 \equiv a^2 y^2 \pmod{p}$. Jednak $a^2 \equiv -1 \pmod{p}$, 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 $p = x^2 + y^2$. □

Definicja 2.27. Liczbę pierwszą p nazywamy **liczbą pierwszą Sophie Germain**, jeżeli $p > 2$ i $2p+1$ jest liczbą pierwszą.

Zauważmy, że cztery najmniejsze liczby pierwsze Sophie Germain to 3, 5, 11 i 23.

Lemat 2.28. *Niech p będzie liczbą pierwszą Sophie Germain i niech k będzie liczbą całkowitą niepodzielną przez $2p+1$. Wówczas $k^p \equiv \pm 1 \pmod{2p+1}$.*

Dowód. Z założenia wynika, że p jest nieparzystą liczbą pierwszą i $q = 2p + 1$ też jest liczbą pierwszą. Z Małego twierdzenia Fermata, $q \mid k^{q-1}-1$. Ponadto $q = 2p+1$, więc $k^{q-1}-1 = k^{2p}-1 = (k^p-1)(k^p+1)$ i wobec tego $q \mid k^p - 1$ lub $q \mid k^p + 1$, skąd $k^p \equiv \pm 1 \pmod{q}$. □

Twierdzenie 2.29. (Sophie Germain). *Jeżeli p jest liczbą pierwszą Sophie Germain, to równanie*

$$x^p + y^p + z^p = 0 \tag{2.11}$$

nie posiada rozwiązania w liczbach całkowitych x, y, z niepodzielnych przez p.

Dowód. Załóżmy nie wprost, że istnieją $x, y, z \in \mathbb{Z}$ niepodzielne przez p spełniające równanie (2.11). Wtedy bez utraty ogólności możemy założyć, że liczby x, y, z są parami względnie pierwsze. Niech $q = 2p+1$.

Najpierw wykażemy, że $q \mid x$ lub $q \mid y$ lub $q \mid z$. W tym celu załóżmy, że tak nie jest. Ponieważ $x^p+y^p+z^p = 0$, więc $x^p+y^p+z^p \equiv 0 \pmod{q}$ i wobec tego na mocy lematu 2.28, $\pm 1 + \pm 1 + \pm 1 \equiv 0 \pmod{q}$. Dodatkowo każda z liczb postaci $\pm 1 + \pm 1 + \pm 1$ jest nieparzysta i ma moduł nie większy od 3, więc $\pm 1 + \pm 1 + \pm 1 \in \{1, -1, 3, -3\}$, skąd $q \mid 1$ lub $q \mid 3$, czyli $q = 3$. Zatem $3 = 2p + 1$, skąd $p = 1$ i mamy sprzeczność. Wobec tego $q \mid x$ lub $q \mid y$ lub $q \mid z$. Bez utraty ogólności możemy przyjąć, że $q \mid x$. Ponieważ liczby x, y, z są parami względnie pierwsze, więc $q \nmid y$ i $q \nmid z$.

Z nieparzystości liczby p otrzymujemy, że

$$y^p + z^p = (y + z)(y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1}),$$

co implikuje równość:

$$(-x)^p = (y + z)(y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1}). \tag{2.12}$$

Załóżmy, że liczby $y + z$ i $y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1}$ nie są względnie pierwsze. Wtedy istnieje ich wspólny dzielnik pierwszy r. Dodatkowo $r \neq p$, gdyż inaczej $p \mid (-x)^p$, skąd $p \mid x$, wbrew założeniu. Dalej, $z \equiv -y \pmod{r}$ oraz $y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1} \equiv 0$

(mod r), skąd po podstawieniu $z \equiv -y \pmod{r}$ uzyskamy, że $py^{p-1} \equiv \equiv 0 \pmod{r}$. Wobec tego $r \mid y$. Ponadto $z \equiv -y \pmod{r}$, więc $r \mid z$ i mamy sprzeczność, bo liczby y i z są względnie pierwsze. Zatem liczby $y+z$ i $y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1}$ są względnie pierwsze i na mocy (2.12) oraz twierdzenia 1.28, istnieją $a, A \in \mathbb{Z}$ takie, że

$$y + z = a^p \text{ oraz } y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1} = A^p. \tag{2.13}$$

Analogicznie pokazuje się, że istnieją $b, c \in \mathbb{Z}$ takie, że

$$x + y = b^p \text{ oraz } x + z = c^p. \tag{2.14}$$

Stąd $b^p + c^p - a^p = (x+y) + (x+z) - (y+z) = 2x$ i ponieważ $q \mid x$, więc $b^p + c^p + (-a)^p \equiv 0 \pmod{q}$. Z pierwszej części dowodu, $q \mid a$ lub $q \mid b$ lub $q \mid c$. Ponadto $q \mid x$ i jeśli $q \mid b$, to z (2.14) wynika, że $q \mid y$, co przeczy temu, że $\mathrm{NWD}(x, y) = 1$. Jeśli zaś $q \mid c$, to z (2.14) wynika, że $q \mid z$, co przeczy temu, że $\mathrm{NWD}(x, z) = 1$. Wobec tego $q \mid a$ i na mocy (2.13), $z \equiv -y \pmod{q}$ oraz $A^p \equiv py^{p-1} \pmod{q}$. Jednakże $q \mid x$, więc z (2.14), $y \equiv b^p \pmod{q}$. Zatem $A^p \equiv py^{p-1} \pmod{q}$ i $y \equiv b^p \pmod{q}$. Stąd $A^p \equiv p(b^p)^{p-1} \pmod{q}$. Ponadto $q \nmid b$, więc $q \nmid A$, skąd na mocy lematu 2.28, $A^p \equiv \pm 1 \pmod{q}$ i $b^p \equiv \pm 1 \pmod{q}$. Lecz, jak wykazaliśmy, $A^p \equiv p(b^p)^{p-1} \pmod{q}$, więc $p \equiv \pm 1 \pmod{q}$, skąd $q \mid p-1$ lub $q \mid p+1$. Dodatkowo $q = 2p+1 > p+1 > p-1 > 1$, więc mamy sprzeczność. □

Rozdział 3

Kongruencje kwadratowe

3.1 Zagadnienia wstępne

W tym rozdziale będą rozpatrywane kongruencje postaci:

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{3.1}$$

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 (3.1) 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: $||0||_2$ i $||1||_2$. 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 $||0||_2$, zaś dla nieparzystego c też posiada dokładnie jedno rozwiązanie: $||1||_2$. 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 2.7 (*iii*) zbiór rozwiązań kongruencji (3.1) jest równy zbiorowi rozwiązań kongruencji $4a^2x + 4abx + 4ac \equiv 0 \pmod{p}$. Ponadto mamy, że $4a^2x + 4abx + 4ac = (2ax + b)^2 - (b^2 - 4ac)$, więc zbiór rozwiazań

kongruencji (3.1) jest równy zbiorowi rozwiązań kongruencji

$$(2ax + b)^2 \equiv \Delta \pmod{p}, \tag{3.2}$$

gdzie $\Delta = b^2 - 4ac$ nazywamy **wyróżnikiem kongruencji** (3.1).

Jeśli teraz $p \mid \Delta$, to dla $x \in \mathbb{Z}$: $(2ax + b)^2 \equiv \Delta \pmod{p}$ wtedy i tylko wtedy, gdy $p \mid (2ax + b)^2$, czyli z pierwszości p, wtedy i tylko wtedy, gdy $2ax + b \equiv 0 \pmod{p}$. Ta ostatnia kongruencja na mocy twierdzenia 2.22 posiada dokładnie jedno rozwiązanie.

Dalej, jeśli nie istnieje $y \in \mathbb{Z}$ takie, że $y^2 \equiv \Delta \pmod{p}$, to kongruencja (3.2) nie posiada rozwiazania, a więc też kongruencja (3.1) 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 3.1. *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: $||y_0||_p$ i $|| - y_0||_p$.*

Dowód. Z naszych założeń wynika, że $p \nmid y_0$ oraz $(-y_0)^2 = y_0^2 \equiv \Delta \pmod{p}$. Zatem $||y_0||_p$ i $|| - y_0||_p$ są rozwiązaniami kongruencji $y^2 \equiv \Delta \pmod{p}$. Gdyby te rozwiązania były równe, to $y_0 \equiv -y_0 \pmod{p}$, skąd $p \mid 2y_0$. Jednakże p jest nieparzystą liczbą pierwszą i $p \nmid y_0$, więc prowadzi to do sprzeczności. Wobec tego $||y_0||_p \neq || - y_0||_p$.

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 $p \mid y_1^2 - y_0^2$ i $y_1^2 - y_0^2 = (y_1 - y_0)(y_1 + y_0)$, 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 $||y_1||_p = ||y_0||_p$ lub $||y_1|| = || - y_0||_p$, co kończy dowód. □

Z przeprowadzonego dowodu wynika, że w przypadku, gdy $p \nmid \Delta$ i istnieje $y_0 \in \mathbb{Z}$ takie, że $y_0^2 \equiv \Delta \pmod{p}$ rozwiązanie kongruencji (3.1) sprowadza się do rozwiązania dwóch kongruencji liniowych:

$$2ax + b \equiv y_0 \pmod{p} \quad \text{oraz} \quad 2ax + b \equiv -y_0 \pmod{p}. \tag{3.3}$$

Każda z tych kongruencji na mocy twierdzenia 2.22 posiada dokładnie jedno rozwiązanie, przy czym te rozwiazania są różne, bo jak pokazaliśmy, $y_0 \not\equiv -y_0 \pmod{p}$. Wobec tego w tym przypadku kongruencja (3.1) posiada dokładnie dwa rozwiązania.

W ten sposób udowodniliśmy następujące

Twierdzenie 3.2. *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 $p \mid \Delta$, to kongruencja (3.1) *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 (3.1) *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 (3.1) *posiada dokładnie dwa rozwiązania $||x_1||_p$ i $||x_2||_p$, gdzie $2ax_1 + b \equiv y_0 \pmod{p}$ i $2ax_2 + b \equiv -y_0 \pmod{p}$.*

3.2 Reszty i niereszty kwadratowe

Podsumowując rozważania poprzedniego paragrafu widzimy, że problem rozwiązywania kongruencji (3.1) sprowadziliśmy do problemu rozwiązywania kongruencji postaci:

$$x^2 \equiv a \pmod{p}, \tag{3.4}$$

gdzie p jest liczbą pierwszą nieparzystą, zaś a jest liczbą całkowitą niepodzielną przez p. Jeżeli kongruencja (10.4) ma rozwiązanie, to mówimy, że a **jest resztą kwadratową modulo** p i piszemy $(\frac{a}{p}) = 1$. W przeciwnym przypadku mówimy, że a **jest niereszta kwadratową modulo** p i piszemy $(\frac{a}{p}) = -1$. Tak zdefiniowany symbol $(\frac{a}{p})$ nazywamy **symbolem Legendre'a**.

Uwaga 3.3. 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 niereszta kwadratową modulo p, to każda liczba z klasy $||a||_p$ też jest resztą kwadratową modulo p. W szczególności, $(\frac{a}{p}) = (\frac{b}{p})$, jeśli $a \equiv b \pmod{p}$.

Lemat 3.4. *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 $p \mid x-y$, czyli $p \mid |x-y|$, więc ponieważ $|x-y| < p$, to $|x-y| = 0$, a zatem $x = y$. □

Twierdzenie 3.5. *Niech* p *będzie nieparzystą liczbą pierwszą. Wówczas zbiór* $\frac{p-1}{2}$ *elementowy:*

$$\{[1^2]_p, [2^2]_p, \ldots, [(p-1)/2)^2]_p\} \tag{3.5}$$

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:*

$$\{1, 2, \ldots, p-1\} \setminus \{[1^2]_p, [2^2]_p, \ldots, [(p-1)/2)^2]_p\} \tag{3.6}$$

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 nieresztami 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 3.4, $c \equiv \pm j \pmod{p}$ 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 $p \mid x^2 - y^2$ i $x^2 - y^2 = (x-y)(x+y)$, więc $p \mid x-y$, skąd $x = [x]_p = [y]_p = y$ lub $p \mid x+y$. Ponadto $0 < x+y \leqslant 2\cdot\frac{p-1}{2} = p-1 < p$, więc $p \nmid x+y$. Zatem zbiór (3.5) ma dokładnie $\frac{p-1}{2}$ elementów i pierwsza część naszego twierdzenia jest udowodniona.

Wobec tego zbiór (3.6) 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 (3.6) 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 (3.5). Stąd $[a]_p\neq 0$ i $[a]_p$ należy do zbioru (3.6) oraz $a\equiv[a]_p \pmod p$. Dowód twierdzenia został więc zakończony. □

Przykład 3.6. (a). Na mocy twierdzenia 3.5 wszystkimi elementami zbioru $\mathbb{Z}_3$, które są resztami kwadratowymi modulo 3 jest jedynie liczba $1^2=1$, zaś liczba 2 jest jedynym elementem zbioru $\mathbb{Z}_3$, który jest nieresztą kwadratową modulo 3. Stąd i z uwagi 3.3 uzyskujemy, że dla dowolnej liczby całkowitej a niepodzielnej przez 3:

$$\left(\frac{a}{3}\right)=1 \iff a\equiv 1 \pmod 3.$$

(b). Podobnie, na mocy twierdzenia 3.5 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. Stąd i z uwagi 3.3 uzyskujemy, że dla dowolnej liczby całkowitej a niepodzielnej przez 5:

$$\left(\frac{a}{5}\right)=1 \iff a\equiv 1,4 \pmod 5.$$

(c). Dla $p=7$, $\frac{p-1}{2}=3$, więc na mocy twierdzenia 3.5 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 nieresztami kwadratowymi modulo 7. Stąd i z uwagi 3.3 uzyskujemy, że dla dowolnej liczby całkowitej a niepodzielnej przez 7:

$$\left(\frac{a}{7}\right)=1 \iff a\equiv 1,2,4 \pmod 7.$$

Twierdzenie 3.7. (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 niereszt\u0105 kwadratow\u0105 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, $c^{p-1} \equiv 1 \pmod{p}$. Dodatkowo 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 $||a||_p$ jest rozwiązaniem kongruencji $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$. Ponadto z pierwszej części dowodu i z twierdzenia 3.5 klasy $||j^2||_p$ 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 niereszt\u0105 kwadratow\u0105 modulo p.

Na odwrót, załóżmy, że a jest niereszt\u0105 kwadratow\u0105 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 $p \mid (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$. Dodatkowo $p \nmid a^{\frac{p-1}{2}} - 1$, więc $p \mid a^{\frac{p-1}{2}} + 1$, skąd $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Wniosek 3.8. *Dla nieparzystej liczby pierwszej p liczba -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $p \equiv 1 \pmod{4}$, czyli:* $(\frac{-1}{p}) = 1 \iff p \equiv 1 \pmod{4}$.

Dowód. Ponieważ $p \nmid -1$, więc na mocy twierdzenia 3.7 liczba -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Ponadto $p > 2$ 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 3.9. *Jeżeli liczby całkowite $a_1, a_2, \ldots, a_n$ nie są podzielne przez nieparzystą liczbę pierwszą p, to zachodzi wzór:*

$$\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right).$$

Dowód. Z twierdzenia 1.41 mamy, że $p \nmid a_1 \cdot a_2 \cdot \ldots \cdot a_n$, więc na mocy kryterium Eulera, $\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) \equiv (a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{(p-1)/2} \pmod{p}$ oraz $\left(\frac{a_k}{p}\right) \equiv a_k^{(p-1)/2} \pmod{p}$ dla każdego $k = 1, \ldots, n$. Zatem po pomnożeniu stronami tych kongruencji uzyskamy, że

$$\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) \equiv \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right) \pmod{p}.$$

Dodatkowo obie strony tej kongruencji są równe 1 lub -1 oraz $-1 \not\equiv 1 \pmod{p}$, bo liczba pierwsza p jest nieparzysta, więc stąd mamy tezę. □

Przypomnijmy, że dla rzeczywistej liczby x symbol $\lfloor x \rfloor$ oznacza największą liczbę całkowitą nie większą od x.

Lemat 3.10. *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*

$$c \equiv (-1)^{\lfloor \frac{2c}{p} \rfloor} r \pmod{p}$$

oraz 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 mamy, że $c = kp + [c]_m$ dla pewnego $k \in \mathbb{Z}$ oraz $p \nmid c$, 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 $\lfloor \frac{2c}{p} \rfloor = 2k$. Lecz $c \equiv [c]_p \pmod{p}$, 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 3.11. (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 $\sum_{i=1}^{(p-1)/2} \lfloor (2ai)/p \rfloor$ 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 jest liczbą pierwszą, $p \nmid a$ oraz $p \nmid i$, więc $p \nmid ai$ dla każdego $i \in \{1,2,\ldots,\frac{p-1}{2}\}$. Stąd na mocy lematu 3.10 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

$$ai \equiv (-1)^{\lfloor (2ai)/p \rfloor} r_i \pmod p. \tag{3.7}$$

Ponadto z lematu 3.10 wynika, że funkcja $i \mapsto r_i$ jest różnowartościowa. Wobec tego

$$\{r_1, r_2, \ldots, r_{(p-1)/2}\} = \{1,2,\ldots,(p-1)/2\}. \tag{3.8}$$

Zatem wymnażając stronami kongruencje (3.7) dla $i = 1,2,\ldots,\frac{p-1}{2}$ i uwzględniając (3.8) uzyskujemy, że

$$a^{\frac{p-1}{2}} \cdot A \equiv (-1)^{\sum_{i=1}^{(p-1)/2} \lfloor (2ai)/p \rfloor} \cdot A \pmod p$$

dla $A = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$. Ponadto p jest liczbą pierwszą, więc $p \nmid A$, czyli $\mathrm{NWD}(A,p) = 1$ i w otrzymanej kongruencji możemy skrócić A uzyskując wzór:

$$a^{\frac{p-1}{2}} \equiv (-1)^{\sum_{i=1}^{(p-1)/2} \lfloor (2ai)/p \rfloor} \pmod p. \tag{3.9}$$

$(i) \Rightarrow (ii)$. Z Kryterium Eulera $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, więc na mocy (3.9) 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 3.10.

$(iii) \Rightarrow (i)$. Ponieważ suma parzystej liczby liczb nieparzystych jest liczbą parzystą, więc na mocy lematu 3.10 liczba $\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2ai)/p \rfloor$ jest parzysta. Zatem z (3.9), $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, więc na mocy Kryterium Eulera a jest resztą kwadratową modulo p. □

Uwaga 3.12. Zauważmy, że Kryterium Gaussa można sformułować inaczej. Mianowicie jeśli liczba całkowita a nie jest podzielna przez nieparzystą liczbę pierwszą p, to

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} \lfloor (2ai)/p \rfloor}.$$

Wniosek 3.13. *Dla dowolnej nieparzystej liczby pierwszej p zachodzi wzór:*

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/2 - \lfloor p/4 \rfloor} = (-1)^{(p^2-1)/8}.$$

W szczególności $\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 7 \pmod{8}$.

Dowód. Najpierw zauważamy, że dla każdego $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$ 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 $\lfloor (4i)/p \rfloor \in \in \{0, 1\}$. Pozostaje zatem obliczyć liczbę tych $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$, dla których $\lfloor (4i)/p \rfloor = 1$, czyli takich, że $1 \leqslant \frac{4i}{p}$, tzn. $\frac{p}{4} \leqslant i \leqslant \frac{p-1}{2}$. Dodatkowo $4 \nmid p$, 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 $\sum_{i=1}^{\frac{p-1}{2}} \lfloor (2 \cdot 2i)/p \rfloor = \dfrac{p-1}{2} - \lfloor p/4 \rfloor$ i na mocy uwagi 3.12 mamy, że $\left(\frac{2}{p}\right) = (-1)^{(p-1)/2 - \lfloor p/4 \rfloor}$.

Ponadto $p \equiv 1,3,5,7 \pmod 8$, więc w pierwszym przypadku $p = 8k+1$ dla pewnego $k \in \mathbb{N}$, skąd $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k - \lfloor 2k + \frac{1}{4} \rfloor = 4k-2k = 2k$ oraz $\frac{p^2-1}{8} = 2k(4k+1)$. W drugim przypadku, $p = 8k+3$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k+1-\lfloor 2k+\frac{3}{4} \rfloor = 4k+1-2k = 2k+1$ oraz $\frac{p^2-1}{8} = (4k+1)(2k+1)$. W trzecim przypadku, $p = 8k+5$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k+2-\lfloor 2k+1+\frac{1}{4} \rfloor = 4k+2-(2k+1) = 2k+1$ oraz $\frac{p^2-1}{8} = (2k+1)(4k+3)$. W ostatnim przypadku, $p = 8k+7$ dla pewnego $k \in \mathbb{N}_0$, więc $\frac{p-1}{2} - \lfloor p/4 \rfloor = 4k+3-\lfloor 2k+1+\frac{3}{4} \rfloor = 4k+3-(2k+1) = 2k+2$ oraz $\frac{p^2-1}{8} = 2(k+1)(4k+3)$.

Kończy to dowód naszego wniosku. □

Wniosek 3.14. *Dla dowolnej nieparzystej liczby pierwszej p zachodzi wzór:*

$$\left(\frac{-2}{p}\right) = (-1)^{\lfloor p/4 \rfloor}.$$

W szczególności $\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1,3 \pmod 8$.

Dowód. Z wniosku 3.9 mamy, że $(\frac{-2}{p}) = (\frac{-1}{p}) \cdot (\frac{2}{p})$. Dodatkowo na mocy wniosku 3.8, $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ i na mocy wniosku 3.13 uzyskujemy, że $(\frac{2}{p}) = (-1)^{(p-1)/2-\lfloor p/4 \rfloor}$, więc $(\frac{-2}{p}) = (-1)^{p-1-\lfloor p/4 \rfloor} = (-1)^{\lfloor p/4 \rfloor}$. Ponadto $p \equiv 1,3,5,7 \pmod 8$, więc $p = 8k+1$ lub $p = 8+3$ lub $p = 8k+5$ lub $p = 8k+7$ dla pewnego $k \in \mathbb{N}_0$ i $\lfloor \frac{8k+1}{4} \rfloor = 2k$, $\lfloor \frac{8k+3}{4} \rfloor = 2k$, $\lfloor \frac{8k+5}{4} \rfloor = 2k+1$ oraz $\lfloor \frac{8k+7}{4} \rfloor = 2k+1$. Stąd $\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1,3 \pmod 8$. □

3.3 Prawo wzajemności reszt kwadratowych

Lemat 3.15. *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 3.10 istnieje $r \in \{1, 2, \ldots, \frac{p-1}{2}\}$ takie, że $qx \equiv -r \pmod{p}$. Zatem $qx + r = py$ dla pewnego $y \in \mathbb{Z}$ oraz $qx + r > 0$, 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 $y' \in \{1, 2, \ldots, \frac{q-1}{2}\}$ i $1 \leqslant py' - qx \leqslant \frac{p-1}{2}$, to $|(py - qx) - (py' - qx)| \leqslant \frac{p-1}{2}$, 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. □

Fundamentalną rolę w teorii kongruencji kwadratowych pełni następujące twierdzenie nazywane **Prawem wzajemności reszt kwadratowych**:

Twierdzenie 3.16. *Dla dowolnych różnych nieparzystych liczb pierwszych p i q zachodzi wzór:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \tag{3.10}$$

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 $1 \leqslant py - qx \leqslant \frac{p-1}{2}$. Niech B będzie zbiorem 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 $1 \leqslant qx - py \leqslant \frac{q-1}{2}$, czyli $-\frac{q-1}{2} \leqslant py - qx \leqslant -1$. Wtedy na mocy lematu 3.15, $(\frac{q}{p}) = (-1)^{|A|}$ i $(\frac{p}{q}) = (-1)^{|B|}$. Zatem

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{|A|+|B|}. \tag{3.11}$$

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 $(\frac{p+1}{2} - x, \frac{q+1}{2} - y) \in U$ dla $(x, y) \in U$. 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 $(x, y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$ 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. Wobec tego $|C| = |D|$. 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 (3.11). □

Prawo wzajemności reszt kwadratowych znali już Euler i Legendre, ale po raz pierwszy udowodnił je Gauss, który nazywał je „fundamentalnym twierdzeniem" w swoich *Disquisitiones Arithmeticae*, pisząc: „fundamentalne twierdzenie należy z pewnością uznać za jedno z najbardziej eleganckich tego typu." Gauss opublikował sześć dowodów tego twierdzenia, a dwa kolejne znaleziono w notatkach znalezionych po jego śmierci. Obecnie istnieje ponad 240 opublikowanych dowodów tego prawa. Prawu wzajemności reszt kwadratowych poświęcona jest na przykład monografia [16].

Część II

Równania diofantyczne rozwiązywalne metodami elementarnymi

Rozdział 4

Metody podstawowe

4.1 Metody kongruencyjne

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 4.1. *Jeżeli a jest nieparzystą liczbą całkowitą, to $a^2 \equiv 1 \pmod 8$. W szczególności $a^2 \equiv 1 \pmod 4$ i równanie diofantyczne $x^2 = 4y + 3$ nie posiada rozwiązania.*

Dowód. Z założenia wynika, że $a = 2k + 1$ dla pewnego $k \in \mathbb{Z}$. Zatem $a^2 - 1 = 4k^2 + 4k = 4k(k + 1)$ oraz $k(k + 1)$ jest iloczynem dwóch kolejnych liczb całkowitych, więc na mocy twierdzenia 1.7, $k(k + 1) = 2n$ dla pewnego $n \in \mathbb{Z}$. Stąd $a^2 - 1 = 8n$, czyli $a^2 \equiv 1 \pmod 8$ oraz $a^2 \equiv 1 \pmod 4$.

Niech $x, y \in \mathbb{Z}$. Jeżeli x jest parzyste, to $x^2 \equiv 0 \pmod 4$ i $4y+3 \equiv 3 \pmod 4$, a ponieważ $3 \not\equiv 0 \pmod 4$, więc $x^2 \neq 4y+3$. Jeżeli zaś x jest nieparzyste, to z pierwszej części dowodu $x^2 \equiv 1 \pmod 4$ i $4y + 3 \equiv 3 \pmod 4$, a ponieważ $3 \not\equiv 1 \pmod 4$, więc $x^2 \neq 4y + 3$. Wobec tego równanie diofantyczne $x^2 = 4y + 3$ nie posiada rozwiązania. □

Przykład 4.2. Udowodnimy, że równanie diofantyczne

$$x^2 + y^2 = 4z + 3$$

nie posiada rozwiązania. W tym celu weźmy dowolne $x, y, z \in \mathbb{Z}$. Wtedy $4z + 3 \equiv 3 \pmod 4$. Ponadto dla liczby całkowitej a mamy, że $a^2 \equiv 0 \pmod 4$, gdy $2 \mid a$ oraz $a^2 \equiv 1 \pmod 4$, gdy $2 \nmid a$ na mocy stwierdzenia 4.1, więc $x^2 + y^2 \equiv 0+0, 0+1, 1+0, 1+1 \pmod 4$, czyli $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. Dodatkowo $3 \not\equiv 0, 1, 2 \pmod 4$, więc

$$x^2 + y^2 \not\equiv 3 \pmod 4. \tag{4.1}$$

W szczególności $x^2 + y^2 \neq 4z + 3$, co kończy nasz dowód.

Przykład 4.3. Udowodnimy, że równanie diofantyczne

$$x^2 + y^2 + z^2 = 8t + 7$$

nie posiada rozwiązania. W tym celu weźmy dowolne $x, y, z, t \in \mathbb{Z}$. Przypuśćmy, że pewna z liczb $a \in \{x, y, z\}$ jest parzysta. Wtedy $a^2 \equiv 0 \pmod 4$, więc z (4.1) $x^2 + y^2 + z^2 \not\equiv 3 \pmod 4$. Ponadto $8t + 7 \equiv 3 \pmod 4$, więc $x^2 + y^2 + z^2 \neq 8t + 7$.

Jeżeli zaś liczby x, y, z są nieparzyste, to na mocy stwierdzenia 4.1, $x^2 \equiv 1 \pmod 8$, $y^2 \equiv 1 \pmod 8$ i $z^2 \equiv 1 \pmod 8$, więc $x^2+y^2+z^2 \equiv$ $\equiv 1 + 1 + 1 = 3 \pmod 8$. Tymczasem $8t + 7 \equiv 7 \pmod 8$ i $7 \not\equiv 3 \pmod 8$, więc $x^2 + y^2 + z^2 \neq 8t + 7$, co kończy nasz dowód.

Stwierdzenie 4.4. *Jeżeli a jest liczbą całkowitą niepodzielną przez 3, to $a^2 \equiv 1 \pmod 3$. W szczególności równanie diofantyczne $x^2 = 3y + 2$ nie posiada rozwiązania.*

Dowód. Z twierdzenia o dzieleniu z resztą wynika, że $a = 3k + 1$ lub $a = 3k + 2$ dla pewnego $k \in \mathbb{Z}$. W pierwszym przypadku $a^2 - 1 = 3k(3k+2)$, a w drugim, $a^2 - 1 = (3k+1)(3k+3) = 3(k+1)(3k+1)$. Zatem w każdym przypadku $3 \mid a^2 - 1$, więc $a^2 \equiv 1 \pmod 3$.

Niech $x, y \in \mathbb{Z}$. Jeśli $3 \mid x$, to $3 \mid x^2$ i $3 \nmid 3y + 2$, skąd $x^2 \neq 3y + 2$. Jeżeli zaś $3 \nmid x$, to z pierwszej części dowodu $x^2 \equiv 1 \pmod 3$. Ponadto $3y + 2 \equiv 2 \pmod 3$ i $2 \not\equiv 1 \pmod 3$, więc $x^2 \neq 3y + 2$. Wobec tego równanie diofantyczne $x^2 = 3y + 2$ nie posiada rozwiązania. □

Stwierdzenie 4.5. *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 $1^3 \equiv 1 \pmod 9$, $2^3 \equiv 8 \equiv -1 \pmod 9$, $4^3 \equiv (2^3)^2 \equiv (-1)^2 \equiv 1 \pmod 9$, $(-4)^3 \equiv -4^3 \equiv -1 \pmod 9$, $(-2)^3 \equiv -8 \equiv 1 \pmod 9$ i $(-1)^3 \equiv -1 \pmod 9$, więc $a^3 \equiv \pm 1 \pmod 9$. □

Przykład 4.6. 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 $3 \mid x$ 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 4.5, $x^3 \equiv \pm 1 \pmod 9$ i $y^3 \equiv \pm 1 \pmod 9$. Zatem $x^3 + {} + ay^3 \equiv 1 + a, 1 - a, -1 + a, -1 - a \pmod 9$. Ponadto $a \equiv 2, 3, 4, 5, 6, 7 \pmod 9$, więc $x^3 + ay^3 \equiv 1, 2, 3, 4, 5, 6, 7, 8 \pmod 9$. Tymczasem $x^3 + {} + ay^3 = 9z^3 \equiv 0 \pmod 9$, więc uzyskaliśmy sprzeczność.

Stąd $3 \mid x$ i $3 \mid y$ i $3 \mid z$.

Przykład 4.7. 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 $a^3 \equiv \pm 1, \pm 5 \pmod{13}$. Rzeczywiście, $a \equiv \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6 \pmod{13}$ oraz $1^3 \equiv 1 \pmod{13}$, $2^3 = 8 \equiv -5 \pmod{13}$, $3^3 = 17 \equiv 1 \pmod{13}$, $4^3 = 64 \equiv -1 \pmod{13}$, $5^3 = 5^2 \cdot 5 \equiv (-1) \cdot 5 \equiv -5 \pmod{13}$, $6^3 = 2^3 \cdot 3^3 \equiv (-5) \cdot 1 \equiv -5 \pmod{13}$, skąd wynika, że $a^3 \equiv \pm 1, \pm 5 \pmod{13}$.

Przypuśćmy teraz, że $13 \nmid x$ i $13 \nmid y$. Wtedy $x^3, y^3 \equiv \pm 1, \pm 1 \pmod{13}$ i $5x^3 + 11y^3 \equiv 5x^3 - 2y^3 \pmod{13}$, skąd $5x^3 + 11y^3 \equiv 5a - 2b \pmod{13}$, gdzie $a, b \in \{1, -1, 5, -5\}$. Ponadto $5x^3 + 11y^3 = -13z^3 \equiv 0 \pmod{13}$, więc $5a \equiv 2b \pmod{13}$. Stąd po pomnożeniu przez 5 obu stron tej kongruencji, $-a \equiv -3b \pmod{13}$, czyli $a \equiv 3b \pmod{13}$. Lecz $3b \equiv 3, -3, 2, -2 \pmod{13}$, zaś $a \equiv 1, -1, 5, -5 \pmod{13}$, 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 $13 \mid z$.

Zadanie 4.8. 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 $13 \mid z$.

Przykład 4.9. Udowodnimy, że nie istnieją liczby nataralne x, y, z takie, że $4xy - y - 1 = z^2$. Przypuśćmy, że tak nie jest. Wtedy $(4x - 1)y = z^2 + 1$. Liczba $4x - 1 \in \mathbb{N}$ jest nieparzysta i większa od 1. Istnieją zatem liczby pierwsze nieparzyste $p_1, p_2, \ldots, p_s$ takie, że $4x-1 = p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Jeżeli $p_i \equiv 1 \pmod{4}$ dla każdego $i = 1, 2, \ldots, s$, to po pomnożeniu tych kongruencji stronami uzyskamy, że $4x - 1 \equiv 1 \pmod{4}$, co prowadzi do sprzeczności. Wobec tego $p_i \equiv 3 \pmod{4}$ dla pewnego $i = 1, 2, \ldots, s$. Stąd $p_i \mid z^2 + 1^2$, więc z Twierdzenia 2.15 uzyskujemy, że $p_i \mid 1$, co jest niemożliwe.

Zatem nie istnieją $x, y \in \mathbb{N}$ takie, że $4xy - y - 1 = z^2$.

Zadanie 4.10. Udowodnij twierdzenie Eulera, które mówi, że nie istnieją liczby naturalne x, y, z takie, że $4xy - x - y = z^2$.

Zadanie 4.11. Udowodnij, że jeżeli $x, y, z \in \mathbb{N}$ i $3^x + 4^y = 5^z$, to liczby x i z są parzyste.

Zadanie 4.12. Rozwiąż równanie diofantyczne $15x^2 - 7y^2 = 9$.

Zadanie 4.13. Udowodnij twierdzenie Levi ben Gersona (1288-1344), że równanie $2^x - 3^y = 1$ nie posiada rozwiązania w liczbach naturalnych $x, y > 1$, zaś jedynym rozwiązaniem równania $3^x - 2^y = 1$ w liczbach naturalnych $x, y > 1$ jest $x = 2$ i $y = 3$.

4.2 Wykorzystanie zasady minimum

Rozumowania, które zaprezentujemy w tym rozdziale 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 nazywamy **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 samo zdanie byłoby prawdziwe dla liczby naturalnej mniejszej od k, co prowadziłoby do nieskończonego, malejącego ciągu liczb naturalnych, prowadząc ostatecznie do sprzeczności. Czyli, 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 w. 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 4.14. Udowodnimy, że dla dowolnej liczby $n \in \mathbb{N}_0$ równanie diofantyczne $x^2 + y^2 = 4^n(4z + 3)$ nie posiada rozwiązania. W tym celu załóżmy, że tak nie jest. Wtedy z zasady minimum wynika, że istnieje najmniejsza liczba $n \in \mathbb{N}_0$ taka, że $x^2+y^2 = 4^n(4z+3)$ dla pewnych $x, y, z \in \mathbb{Z}$. Z przykładu 4.2 wynika, że $n \geqslant 1$. Zatem $n-1 \in \mathbb{N}_0$ oraz $4 \mid x^2+y^2$. Stąd liczby x i y są tej samej parzystości. Jeśli obie te liczby są nieparzyste, to ze stwierdzenia 4.1, $x^2 \equiv 1 \pmod 4$ i $y^2 \equiv 1 \pmod 4$, więc $x^2 + y^2 \equiv 2 \pmod 4$, co prowadzi do sprzeczności. Wobec tego $2 \mid x$ i $2 \mid y$, skąd $x = 2X$ i $y = 2Y$ dla pewnych $X, Y \in \mathbb{Z}$. Zatem $4X^2+4Y^2 = 4^n(4z+3)$, skąd $X^2+Y^2 = 4^{n-1}(4z+3)$ oraz $n - 1 < n$, więc mamy sprzeczność z minimalnością liczby n.

Nasze przypuszczenie doprowadziło zatem do sprzeczności. Wobec tego nie istnieją $n \in \mathbb{N}_0$ oraz $x, y, z \in \mathbb{Z}$ takie, że $x^2 + y^2 = 4^n(4z + 3)$.

Przykład 4.15. Udowodnimy, że dla dowolnej liczby $n \in \mathbb{N}_0$ równanie diofantyczne $x^2 + y^2 + z^2 = 4^n(8t + 7)$ nie posiada rozwiązania. W tym celu załóżmy, że tak nie jest. Wtedy z zasady minimum wynika, że istnieje najmniejsza liczba $n \in \mathbb{N}_0$ taka, że $x^2 + y^2 + z^2 = 4^n(8t + 7)$

dla pewnych $x, y, z, t \in \mathbb{Z}$. Z przykładu 4.3 wynika, że $n \geqslant 1$. Zatem $n-1 \in \mathbb{N}_0$ oraz $4 \mid x^2+y^2+z^2$. Stąd albo dokładnie jedna z liczb x, y, z jest parzysta albo wszystkie te liczby są parzyste. W pierwszym przypadku bez zmniejszania ogólności możemy zakładać, że $2 \mid x$ oraz $2 \nmid y$ i $2 \nmid z$. Wtedy ze stwierdzenia 4.1, $y^2 \equiv 1 \pmod 4$ i $z^2 \equiv 1 \pmod 4$, skąd $x^2+y^2+z^2 \equiv 0+1+1 \equiv 2 \pmod 4$, co prowadzi do sprzeczności. Wobec tego $2 \mid x$, $2 \mid y$ i $2 \mid z$, czyli $x = 2X$, $y = 2Y$ i $z = 2Z$ dla pewnych $X, Y, Z \in \mathbb{Z}$. Zatem $4X^2+4Y^2+4Z^2 = 4^n(8t+7)$, skąd $X^2+Y^2+Z^2 = 4^{n-1}(8t+7)$, co przeczy minimalności liczby n.

Nasze przypuszczenie doprowadziło zatem do sprzeczności. Wobec tego nie istnieją $n \in \mathbb{N}_0$ oraz $x, y, z, t \in \mathbb{Z}$ takie, że $x^2+y^2+z^2 = 4^n(8t+7)$.

Przykład 4.16. 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 4.6 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 4.17. 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 4.7, $x = 13X$, $y = 13Y$ 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 $x = y = z = 0$.

Zadanie 4.18. 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 $x = y = z = 0$.

4.3 Metoda faktoryzacji

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 $k = 1, \ldots, s$.

Zilustrujemy tę metodę różnymi przykładami i zadaniami.

Przykład 4.19. 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 4.20. 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 odpowienio $xy - x - y - 46 = -93, -31, -3, -1$ 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 $y = 5$.

Zadanie 4.21. Wyznacz wszystkie liczby naturalne x i y takie, że $(xy-103)^2 = x^2+y^2$.

Zadanie 4.22. Wyznacz wszystkie liczby naturalne x i y oraz wszystkie liczby pierwsze p takie, że $x^4+4 = py^4$.

Przykład 4.23. Wyznaczymy wszystkie liczby naturalne x i y takie, że $2^x - 1 = 3^y$. Jeżeli liczba x jest nieparzysta, to $x > 1$, więc $x = 2k+1$ dla pewnego $k \in \mathbb{N}$. Stąd $2^x = 2^{2k+1} = 2 \cdot 4^k \equiv 2 \cdot 1 \equiv 2 \pmod 3$, bo $4^k \equiv 1 \pmod 3$, gdyż $4 \equiv 1 \pmod 3$. Wobec tego $2^x - 1 \equiv \equiv 1 \pmod 3$, co prowadzi do sprzeczności.

Zatem $x = 2k$ dla pewnego $k \in \mathbb{N}$ oraz $3^y = 2^{2k} - 1 = (2^k-1)(2^k + +1)$. Stąd $2^k - 1 = 3^a$ i $2^k + 1 = 3^b$ dla pewnych $a \in \mathbb{N}_0$ i $b \in \mathbb{N}$, przy czym $a < b$, bo $2^k - 1 < 2^k + 1$. Jeżeli $a \neq 0$, to $3 \mid 2^k - 1$ i $3 \mid 2^k + 1$, skąd $3 \mid (2^k+1) - (2^k-1)$, czyli $3 \mid 2$, co jest niemożliwe. Zatem $a = 0$, skąd $2^k = 2$, więc $k = 1$ i $x = 2$ oraz $3^y = 4 - 1 = 3$, więc $y = 1$.

Wobec tego jedynym rozwiązaniem równania $2^x - 1 = 3^y$ w liczbach naturalnych jest $x = 2$ i $y = 1$.

Zadanie 4.24. Wyznacz wszystkie liczby naturalne x, y i z takie, że $3^x + 4^y = 5^z$.

Twierdzenie 4.25. *Wszystkie rozwiązania w liczbach naturalnych równania $xy = zw$ dane są wzorami: $x = mn$, $y = kp$, $z = mp$, $w = kn$, gdzie $m, n, k, p \in \mathbb{N}$ oraz $\mathrm{NWD}(n, p) = 1$.*

Dowód. Niech $m, n, k, p \in \mathbb{N}$ i $x = mn$, $y = kp$, $z = mp$, $w = kn$. Wtedy $xy = mnkp$ i $zw = mpkn$, więc $xy = zw$.

Na odwrót, niech $x, y, z, w \in \mathbb{N}$ i $xy = zw$. Oznaczmy $\mathrm{NWD}(x, z) = = m$. Wtedy $m \in \mathbb{N}$ oraz na mocy twierdzenia 1.14 istnieją $n, p \in \mathbb{N}$ takie, że $\mathrm{NWD}(n, p) = 1$, $x = mn$ i $z = mp$. Zatem $mny = mpw$, skąd $ny = pw$. Z zasadniczego twierdzenia arytmetyki, $n \mid w$, więc $w = kn$ dla pewnego $k \in \mathbb{N}$ oraz $ny = pkn$, skąd $y = kp$. □

Zadanie 4.26. Udowodnij, że jeżeli liczby naturalne x, y, z, w spełniają równanie $xy = zw$, to liczba $x + y + z + w$ jest złożona.

Zadanie 4.27. Stosując twierdzenie 4.25 udowodnij, że wszystkie rozwiązania równania $xy = z^2$ w liczbach naturalnych dane są wzorami $x = kn^2$, $y = km^2$, $z = kmn$, gdzie $k, m, n \in \mathbb{N}$ oraz $\mathrm{NWD}(m, n) = 1$.

Zadanie 4.28. Wyznacz wszystkie liczby całkowite x i y takie, że $x^3 + y^3 + 1 = 3xy$.

4.4 Metody stosujące nierówności

Przykład 4.29. 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 4.30. 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:
$(1, 1, 2, 4)$, $(1, 1, 4, 2)$, $(1, 2, 1, 4)$, $(1, 4, 1, 2)$, $(1, 2, 4, 1)$, $(1, 4, 2, 1)$, $(2, 1, 1, 4)$, $(4, 1, 1, 2)$, $(2, 1, 4, 1)$, $(4, 1, 2, 1)$, $(2, 4, 1, 1)$, $(4, 2, 1, 1)$.

Zadanie 4.31. Wyznacz wszystkie liczby naturalne x, y, z, t, u takie, że $x + y + z + t + u = xyztu$.

Przykład 4.32. Wyznaczymy wszystkie pary (x, y) liczb całkowitych spełniające równanie

$$x^2 + y^2 = 1.$$

Niech $x, y \in \mathbb{Z}$ i $x^2 + y^2 = 1$. Wtedy $|x| \leqslant |x|^2 = x^2 \leqslant x^2 + y^2 = 1$, więc $x = 1, -1, 0$. Jeżeli $x = \pm 1$, to $1 + y^2 = 1$, skąd $y = 0$. Jeżeli zaś $x = 0$, to $y^2 = 1$, więc $y = \pm 1$. Wobec tego wszystkimi rozwiązaniami równania diofantycznego $x^2 + y^2 = 1$ są pary: $(1, 0)$, $(-1, 0)$, $(0, 1)$ i $(0, -1)$.

Przykład 4.33. Wyznaczymy wszystkie pary (x, y) liczb całkowitych spełniające równanie

$$x^2 + xy + y^2 = 1.$$

Po pomnożeniu przez 4 obu stron otrzymamy równanie równoważne: $4x^2 + 4xy + 4y^2 = 4$, które można zapisać w postaci $(2x + y)^2 + 3y^2 = 4$. Stąd $3y^2 \leqslant 4$, więc $|y| \leqslant 1$, a zatem $y = 1, -1, 0$.

Jeśli $y = 1$, to $(2x + 1)^2 = 1$, skąd $2x + 1 = 1$ lub $2x + 1 = -1$, czyli $x = 0$ lub $x = -1$.

Jeśli $y = -1$, to $(2x - 1)^2 = 1$, skąd $2x - 1 = 1$ lub $2x - 1 = -1$, czyli $x = 1$ lub $x = 0$.

Jeśli $y = 0$, to $(2x)^2 = 4$, skąd $2x = 2$ lub $2x = -2$, czyli $x = 1$ lub $x = -1$.

Zatem nasze równanie diofantyczne posiada dokładnie 6 rozwiązań: $(0, 1)$, $(-1, 1)$, $(1, -1)$, $(0, -1)$, $(1, 0)$ i $(-1, 0)$.

Przykład 4.34. Wyznaczymy wszystkie liczby naturalne x, y, z takie, że

$$x^2y + y^2z + z^2x = 3xyz.$$

W rozwiązaniu tego problemu posłużymy się następującym twierdzeniem Cauchy'ego: Niech $n = 2, 3, \ldots$ i niech $x_1, x_2, \ldots, x_n$ będą dodatnimi liczbami rzeczywistymi. Wówczas zachodzi nierówność:

$$\frac{x_1 + x_2 + \ldots + x_n}{n} \geqslant \sqrt[n]{x_1 \cdot x_2 \cdot \ldots \cdot x_n}$$

przy czym $\frac{x_1+x_2+\ldots+x_n}{n} = \sqrt[n]{x_1 \cdot x_2 \cdot \ldots \cdot x_n}$ wtedy i tylko wtedy, gdy $x_1 = x_2 = \ldots = x_n$.

Niech x, y, z będą dodatnimi liczbami rzeczywistymi takimi, że

$$x^2y + y^2z + z^2x = 3xyz.$$

Wtedy $\frac{x^2y+y^2z+z^2x}{3} = xyz$ oraz $\sqrt[3]{x^2y \cdot y^2z \cdot z^2x} = xyz$. Zatem

$$\frac{x^2y + y^2z + z^2x}{3} = \sqrt[3]{x^2y \cdot y^2z \cdot z^2x},$$

więc z twierdzenia Cauchy'ego mamy, że $x^2y = y^2z = z^2x$, skąd

$$x^2y = \sqrt[3]{x^2y \cdot y^2z \cdot z^2x} = xyz,$$

więc $x = z$ i $y = x$, czyli $x = y = z$. Na odwrót, jeżeli $x = y = z$, to $x^2y + y^2z + z^2x = 3x^3 = 3xyz$.

W szczególności wszystkimi rozwiązaniami naszego równania diofantycznego są trójki (k, k, k) dla $k \in \mathbb{N}$.

Przykład 4.35. Wyznaczymy wszystkie trójki (x, y, z) liczb naturalnych takie, że

$$(x + y)^2 + 3x + y + 1 = z^2.$$

Przypuśćmy, że $y < x$. Wtedy $2x+2y < 3x+y$ i $(x+y)^2+3x+y+1 > (x+y)^2+2(x+y)+1 = (x+y+1)^2$ oraz $(x+y+2)^2 = (x+y)^2 + 4(x+y)+4 > (x+y)^2+3x+y+1$, więc wtedy $(x+y+2)^2 > z^2 > (x+y+1)^2$, skąd $x+y+2 > z > x+y+1$, co prowadzi do sprzeczności.

Teraz przypuśćmy, że $y > x$. Wtedy $2x + 2y > 3x + y$, więc $(x+y+1)^2 = (x+y)^2+2(x+y)+1 > (x+y)^2+3x+y+1 > (x+y)^2$, więc $(x + y + 1)^2 > z^2 > (x + y)^2$, skąd $x + y + 1 > z > x + y$, co prowadzi do sprzeczności.

Wobec tego $y = x$ i nasze równanie przybiera postać $4x^2+4x+1 = z^2$, czyli $(2x + 1)^2 = z^2$, skąd $z = 2x + 1$.

Zatem wszystkimi szukanymi trójkami są $(n, n, 2n + 1)$ dla $n \in \mathbb{N}$.

Rozdział 5

Liniowe równania diofantyczne

5.1 Liniowe równania diofantyczne

Definicja 5.1. Liniowym równaniem diofantycznym nazywamy równanie postaci:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{5.1}$$

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 i niewiadome $x_1, x_2, \ldots, x_n$ są liczbami całkowitymi. Jeżeli $b = 0$, to dane równanie nazywamy **jednorodnym**.

Twierdzenie 5.2. *Liniowe równanie diofantyczne* (5.1) *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* (5.1) *posiada nieskończenie wiele rozwiazań.*

Dowód. Niech $a_1x_1+a_2x_2+\ldots+a_nx_n = b$ dla pewnych $x_1, x_2, \ldots, x_n \in \in \mathbb{Z}$. Ponieważ pewna z liczb $a_1, a_2, \ldots, a_n$ jest różna od zera, więc istnieje $\mathrm{NWD}(a_1, a_2, \ldots, a_n) = d$. 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 istnieje $b \in \in \mathbb{Z}$ takie, że $b = a \cdot \mathrm{NWD}(a_1, a_2, \ldots, a_n)$. Z twierdzenia 1.11 uzyskujemy, że $\mathrm{NWD}(a_1, a_2, \ldots, a_n) = a_1u_1 + a_2u_2 + \ldots + a_nu_n$ dla pewnych $u_1, u_2, \ldots, u_n \in \mathbb{Z}$. 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 (5.1). 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 (5.1). Wobec tego równanie to posiada nieskończenie wiele rozwiązań. □

Uwaga 5.3. Zauważmy, że każde równanie postaci (5.1) takie, że $\mathrm{NWD}(a_1, \ldots, a_n) \mid b$, można przy pomocy algorytmu Euklidesa sprowadzić do równania postaci

$$y_1 + 0 \cdot y_2 + \ldots + 0 \cdot y_n = c \tag{5.2}$$

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 $a_i = q_ia_1 + r_i$ 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:

$$z_1 = x_1 + q_2x_2 + \ldots + q_nx_n. \tag{5.3}$$

Stąd:

$$x_1 = z_1 - (q_2x_2 + \ldots + q_nx_n). \tag{5.4}$$

Teraz zauważamy, że jeżeli $(x_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania (5.1), to dla z_1 danego wzorem (5.3), $(z_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania:

$$a_1z_1 + r_2x_2 + \ldots + r_nx_n = b. \tag{5.5}$$

Na odwrót, jeśli $(z_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania (5.5), to dla x_1 danego wzorem (5.4), $(x_1, x_2, \ldots, x_n)$ jest rozwiązaniem równania (5.1).

Stąd problem znalezienia wszystkich rozwiązań równania (5.1) został sprowadzony do problemu znalezienia wszystkich rozwiązań równania (5.5). 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 (5.5) jest mniejszy od $|a_1|$, które jest najmniejszym co do modułu niezerowym współczynnikiem przy niewiadomych w równaniu (5.1).

Następnie z równaniem (5.5) postępujemy według tej samej procedury, którą stosowaliśmy do równania (5.1). 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 (5.2). 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 (5.1) i zauważamy, że będą one zależały od dokładnie $n - 1$ parametrów całkowitych.

Zilustrujmy algorytm przedstawiony w uwadze 5.3 następującymi przykładami.

Przykład 5.4. 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 5.2 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 5.5. 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

$$z_1 = z + 3x + 17y. \tag{5.6}$$

Wtedy

$$z = z_1 - 3x - 17y \tag{5.7}$$

oraz $-5x - 5y + 15z_1 = 75$, czyli po skróceniu przez -5:

$$x + y - 3z_1 = -15. \tag{5.8}$$

Wobec tego $y = k \in \mathbb{Z}$ i $z_1 = l \in \mathbb{Z}$ są dowolne oraz $x = -15 + 3l - k$. Ze wzoru (5.7), $z = l - 3(-15 + 3l - k) - 17k = l + 45 - 9l + 3k - 17k$, 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.

Zadanie 5.6. Rozwiązać liniowe równanie diofantyczne

$$21x + 112y + 144z = 1.$$

Uwaga 5.7. Niech $(u_1, u_2, \ldots, u_n)$ będzie ustalonym rozwiązaniem równania diofantycznego (5.1), tzn. $a_1u_1 + a_2u_2 + \ldots + a_nu_n = b$. Będziemy je nazywali **rozwiązaniem szczególnym** tego równania.

Jeżeli $(y_1, y_2, \ldots, y_n)$ jest rozwiązaniem diofantycznego równania jednorodnego $a_1x_1+a_2x_2+\ldots+a_nx_n = 0$, to $a_1(u_1+y_1)+a_2(u_2+y_2)+$ $+\ldots+a_n(u_n+y_n) = (a_1u_1+a_2u_2+\ldots+a_nu_n)+(a_1y_1+a_2y_2+\ldots+$ $+a_ny_n) = b+0 = b$, czyli $(u_1+y_1, u_2+y_2, \ldots, u_n+y_n)$ jest rozwiązaniem równania diofantycznego (5.1).

Na odwrót, niech $(z_1, z_2, \ldots, z_n)$ będzie rozwiązaniem równania diofantycznego (5.1). Wtedy $a_1z_1+a_2z_2+\ldots+a_nz_n = b$ oraz $a_1(z_1-u_1)+$ $+a_2(z_2-u_2)+\ldots+a_n(z_n-u_n) = (a_1z_1+a_2z_2+\ldots+a_nz_n)-(a_1u_1+a_2u_2+$ $+\ldots+a_nu_n) = b-b = 0$, więc $(z_1-u_1, z_2-u_2, \ldots, z_n-u_n)$ jest wtedy rozwiązaniem diofantycznego równania jednorodnego $a_1x_1+a_2x_2+\ldots+$ $+a_nx_n = 0$, przy czym $z_i = u_i + (z_i - u_i)$ dla $i = 1, 2, \ldots, n$.

W ten sposób wykazaliśmy, że **wszystkie rozwiązania równania diofantycznego (5.1) są sumami dowolnego rozwiązania szczególnego tego równania i dowolnego rozwiązania równania jednorodnego** $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0$.

Uwaga 5.8. Niech $a_1, a_2 \ldots, a_n \in \mathbb{Z}$, gdzie $n \geqslant 2$, przy czym $a_i \neq 0$ dla pewnego $i = 1, 2, \ldots, n$. Oznaczmy przez A zbiór wszystkich ciągów $(x_1, x_2, \ldots, x_n)$ liczb całkowitych takich, że $a_1x_1+a_2x_2+\ldots+a_nx_n = 0$. Oczywiście $\theta = (0, 0, \ldots, 0) \in A$. Jeśli $\alpha = (x_1, x_2, \ldots, x_n) \in A$ i $\beta =$ $= (y_1, y_2, \ldots, y_n) \in A$ oraz $\alpha + \beta = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$, to liczby $x_i+y_i \in \mathbb{Z}$ dla $i = 1, 2, \ldots, n$ oraz $a_1(x_1+y_1)+a_2(x_2+y_2)+\ldots+$ $+a_n(x_n+y_n) = (a_1x_1+a_2x_2+\ldots+a_nx_n)+(a_1y_1+a_2y_2+\ldots+a_ny_n) =$ $= 0 + 0 = 0$, więc $\alpha + \beta \in A$. Stąd przez prostą indukcję pokazujemy, że dla dowolnego $m \in \mathbb{N}$ i dla dowolnych $\alpha_1, \ldots, \alpha_m \in A$ mamy, że $\alpha_1 + \ldots + \alpha_n \in A$. Dalej, niech dla $k \in \mathbb{Z}$: $k \cdot \alpha = (kx_1, kx_2, \ldots, kx_n)$. Wtedy $kx_i \in \mathbb{Z}$ dla $i = 1, 2, \ldots, n$ oraz $a_1(kx_1) + a_2(kx_2) + \ldots +$ $+a_n(kx_n) = k \cdot (a_1x_1 + a_2x_2 + \ldots + a_nx_n) = k \cdot 0 = 0$, więc $k \cdot \alpha \in A$. Wobec tego dla każdego $m \in \mathbb{N}$ i dla dowolnych $\alpha_1, \ldots, \alpha_m \in A$ oraz $k_1, \ldots, k_m \in \mathbb{Z}$ mamy, że $\alpha = k_1 \cdot \alpha_1 + k_2 \cdot \alpha_2 + \ldots + k_m \cdot \alpha_m \in A$, przy czym α nazywamy wówczas **kombinacją liniową** ciągów $\alpha_1, \ldots, \alpha_m$ o współczynnikach całkowitych $k_1, \ldots, k_n$.

Niech $\alpha_1, \ldots, \alpha_m \in A$. Mówimy, że układ $(\alpha_1, \ldots, \alpha_m)$ jest **li-**

niowo niezależny, jeżeli dla dowolnych $k_1, \ldots, k_m \in \mathbb{Z}$ z tego, że $k_1 \cdot \alpha_+ \ldots + k_m \cdot \alpha_m = \theta$ wynika, że $k_1 = \ldots = k_m = 0$. Mówimy, że układ $(\alpha_1, \ldots, \alpha_m)$ **generuje** A, jeżeli każdy ciąg $\alpha \in A$ jest kombinacją liniową ciągów $\alpha_1, \ldots, \alpha_m$. Mówimy, że układ $(\alpha_1, \ldots, \alpha_m)$ jest **bazą** A, jeżeli ten układ jest liniowo niezależny i generuje A.

W nawiązaniu do uwagi 5.3 zastosowanej do $b = 0$, oznaczmy przez B zbiór wszystkich ciągów $(z_1, x_2, \ldots, x_n)$ liczb całkowitych takich, że $a_1 z_1 + r_2 x_2 + \ldots + r_n x_n = 0$. Pokazaliśmy tam, że $(x_1, x_2, \ldots, x_n) \in A$ wtedy i tylko wtedy, gdy $(z_1, x_2, \ldots, x_n) \in B$.

Zatem funkcja $f\colon A \to B$ dana wzorem

$$f((x_1, x_2, \ldots, x_n)) = (z_1, x_2, \ldots, x_n),$$

gdzie $z_1 = x_1 + q_2 x_2 + \ldots + q_n x_n$, jest bijekcją i funkcja g do niej odwrotna dana jest wzorem $g((z_1, x_2, \ldots, x_n)) = (x_1, x_2, \ldots, x_n)$ dla $x_1 = z_1 - (q_2 x_2 + \ldots + q_n x_n)$.

Standardowe sprawdzenie pokazuje, że dla dowolnych $\alpha, \beta \in A$ oraz $k \in \mathbb{Z}$ mamy, że $f(\alpha + \beta) = f(\alpha) + f(\beta)$ i $f(k \cdot \alpha) = k \cdot f(\alpha)$. Stąd przez indukcję można wykazać, że

$$f(k_1 \cdot \alpha_1 + \ldots + k_m \cdot \alpha_m) = k_1 \cdot f(\alpha_1) + \ldots + k_m \cdot f(\alpha_m)$$

dla dowolnego $m \in \mathbb{N}$ i dla dowolnych $\alpha_1, \ldots, \alpha_m \in A$ i $k_1, \ldots, k_m \in \mathbb{Z}$. Ponadto analogiczne własności ma funkcja g. Wynika stąd, że układ $(\beta_1, \ldots, \beta_m)$ jest bazą B wtedy i tylko wtedy, gdy $(g(\beta_1), \ldots, g(\beta_m))$ jest bazą A.

Na mocy uwagi 5.3 po skończonej liczbie kroków dojdziemy do równania równoważnego równaniu $a_1 x_1 + \ldots + a_n x_n = 0$, które będzie miało postać: $y_1 + 0 \cdot y_2 + \ldots + 0 \cdot y_n = 0$. Zbiorem rozwiązań tego ostatniego równania diofantycznego jest zbiór

$$C = \{(0, y_2, \ldots, y_n) : y_2, \ldots, y_n \in \mathbb{Z}\}.$$

Stąd bazą C jest układ $(\varepsilon_2, \ldots, \varepsilon_n)$, gdzie ε_k jest ciągiem n wyrazowym posiadającym jedynkę na k -tej pozycji i zera na pozostałych miejscach dla $k = 2, 3, \ldots, n$. Stosując teraz skończenie razy przekształcenia typu g uzyskamy, że A posiada bazę $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$.

Zatem każde rozwiązanie równania diofantycznego jednorodnego $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0$ jest kombinacją liniową o współczynnikach całkowitych ciągów $\alpha_1, \ldots, \alpha_{n-1}$.

Jeżeli $u_1, u_2, \ldots, u_n \in \mathbb{Z}$ i $b = a_1u_1 + \ldots + a_nu_n$, to na mocy uwagi 5.7 wszystkie rozwiązania równania diofantycznego

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

dane są wzorem:

$$(x_1, \ldots, x_n) = (u_1, u_2, \ldots, u_n) + t_1 \cdot \alpha_1 + \ldots + t_{n-1} \cdot \alpha_{n-1},$$

gdzie elementy $t_1, \ldots, t_{n-1} \in \mathbb{Z}$ są dowolne i nazywamy je **parametrami**.

Zadanie 5.9. 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?

Zadanie 5.10. 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.

5.2 Diofantyczne równania liniowe z dwiema niewiadomymi

Ogólna postać diofantycznego równania liniowego z dwiema niewiadomymi:

$$ax + by = c, \tag{5.9}$$

gdzie a, b, c są danymi liczbami całkowitymi takimi, że $a \neq 0$ lub $b \neq 0$.

Twierdzenie 5.11. *Diofantyczne równanie liniowe* (5.9) *posiada rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(a, b) \mid c$. *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* (5.9) *dane są wzorami:*

$$\begin{cases} x = x_0 + \frac{b}{NWD(a,b)} \cdot k \\ y = y_0 - \frac{a}{NWD(a,b)} \cdot k \end{cases}, \tag{5.10}$$

gdzie k *jest dowolną liczbą całkowitą.*

Dowód. Pierwsza część twierdzenia wynika od razu z twierdzenia 5.2. Niech dalej $\mathrm{NWD}(a,b) \mid c$. Wtedy z twierdzenia 5.2 istnieją $x_0, y_0 \in \in \mathbb{Z}$ takie, że $ax_0 + by_0 = c$. Dla dowolnego $k \in \mathbb{Z}$ liczby x i y dane wzorem (5.10) są całkowite oraz $ax + by = ax_0 + by_0 + \frac{ab}{NWD(a,b)} \cdot k - + \frac{ab}{NWD(a,b)} \cdot k = ax_0 + by_0 = c$, czyli (x, y) jest rozwiązaniem równania (5.9).

Na odwrót, niech para (x, y) będzie rozwiązaniem równania (5.9). Wtedy $ax + by = ax_0 + by_0$, skąd $a(x - x_0) = b(y_0 - y)$. Zatem $\frac{a}{NWD(a,b)}(x - x_0) = \frac{b}{NWD(a,b)}(y_0 - y)$. Liczby $\frac{a}{NWD(a,b)}$ i $\frac{b}{NWD(a,b)}$ są względnie pierwsze, więc z zasadniczego twierdzenia arytmetyki otrzymujemy, że $\frac{b}{NWD(a,b)} \mid x - x_0$. Zatem $x - x_0 = \frac{b}{NWD(a,b)} \cdot k$ dla pewnego $k \in \mathbb{Z}$ i $x = x_0 + \frac{b}{NWD(a,b)} \cdot k$ oraz $\frac{a}{NWD(a,b)} \cdot \frac{b}{NWD(a,b)} \cdot k = \frac{b}{NWD(a,b)}(y_0 - + y)$. Stąd dla $b \neq 0$, $y_0 - y = \frac{a}{NWD(a,b)} \cdot k$, czyli $y = y_0 - \frac{a}{NWD(a,b)} \cdot k$. Jeżeli zaś $b = 0$, to $x = x_0$ i $a \neq 0$ oraz $\mathrm{NWD}(a,b) = |a|$, skąd $\frac{a}{NWD(a,b)} = \pm 1$, więc $y = y_0 - \frac{a}{NWD(a,b)} \cdot k$ dla $k = \pm(y_0 - y)$ i wtedy $x = x_0 + \frac{b}{NWD(a,b)} \cdot k$. □

Uwaga 5.12. Opiszemy metodę wyznaczania pewnych 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 $b = q_1 a + r_1$ 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 $a = q_2 r_1 + r_2$ 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 $r_2 = a - q_2 r_1 = a - q_2(b - q_1 a) = a(1+q_2 q_1)+b(-q_2)$, więc $\mathrm{NWD}(a,b) = a(1+q_2 q_1) + b(-q_2)$. 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 $r_1 = q_3 r_2 + r_3$ 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:

$$r_{i-1} = q_{i+1} \cdot r_i + r_{i+1} \quad \text{dla każdego } \ i = 0, 1, \ldots, n. \tag{5.11}$$

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 (5.11), $r_{i+1} = r_{i-1} - q_{i+1} r_i = (ax_{i-1} + by_{i-1}) - q_{i+1}(ax_i + by_i) = a(x_{i-1} - q_{i+1}x_i) + b(y_{i-1} - q_{i+1}y_i)$, 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 $x_n, y_n \in \mathbb{Z}$. Ponadto $r_n = \mathrm{NWD}(a,b)$, więc $\mathrm{NWD}(a,b) = a \cdot x_n + b \cdot y_n$.

Przykład 5.13. Zilustrujemy uwagę 5.12 wyznaczając liczby całkowite x, y spełniające równanie diofantyczne:

$$252x + 574y = \mathrm{NWD}(252, 574).$$

Zapiszmy kolejne dzielenia z resztą w algorytmie Euklidesa wyznacza-

nia NWD(252, 574):

$$\begin{aligned} 574 &= 2 \cdot 252 + 70 \\ 252 &= 3 \cdot 70 + 42 \\ 70 &= 1 \cdot 42 + 28 \\ 42 &= 1 \cdot 28 + 14 \\ 28 &= 2 \cdot 14 \end{aligned} \quad . \tag{5.12}$$

Zatem ostatnia dodatnią reszta jest liczba 14, więc NWD(252, 574) = = 14. Teraz kolejno, z pierwszej równości $70 = 252 \cdot (-2) + 574 \cdot 1$, więc po podstawieniu w drugiej równości za 70, $42 = 252 \cdot 1 - (252 \cdot \cdot(-2) + 574 \cdot 1) \cdot 3 = 252 \cdot 7 + 574 \cdot (-3)$. 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 $252 \cdot 16 + 574 \cdot (-7) = \text{NWD}(252, 574)$.

Na mocy twierdzenia 5.11, 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 5.14. Metoda opisana w uwadze 5.12 i twierdzenie 5.11 umożliwiają szybkie rozwiązywanie równań diofantycznych postaci $ax + by = c$. Mianowicie najpierw obliczamy $d = \text{NWD}(a, b)$. Jeśli $d \nmid c$, to równanie nasze nie posiada rozwiązania. W przypadku, gdy $d \mid c$, metodą opisaną w uwadze 5.12 znajdujemy $u, v \in \mathbb{Z}$ takie, że $au + bv = d$. Wtedy $x_0 = \frac{c}{d}u$ i $y_0 = \frac{c}{d}v$ są liczbami całkowitymi i $ax_0 + by_0 = c$. Zatem na mocy twierdzenia 5.11 wszystkie rozwiązania równania diofantycznego $ax + by = c$ dane są wzorami (5.10).

Przykład 5.15. Zastosujemy uwagę 5.14 do wyznaczenia wszystkich rozwiązań równania diofantycznego:

$$15x + 98y = 4.$$

Ponieważ $\text{NWD}(15, 98) = \text{NWD}(15, 8) = \text{NWD}(8, -1) = 1$ 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 5.11 wszystkie rozwiązania naszego równania diofantycznego dane są zatem wzorami: $x = -52 + 98k$, $y = 8 - 15k$, gdzie k jest dowolną liczbą całkowitą.

Zadanie 5.16. Rozwiązać liniowe równanie diofantyczne

$$89x + 233y = 1.$$

5.3 Twierdzenie Sylvestera

Twierdzenie 5.17. (Sylvester). *Niech a i b będą dowolnymi, 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 5.11 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 $0 \leqslant y = y_0 - ka \leqslant a - 1$ oraz dla $x = x_0 + ka$ na mocy twierdzenia 5.11 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. □

Zadanie 5.18. Wypisz wszystkie elementy zbioru $\mathbb{N}_0 \setminus A$, gdzie $A = \{5x + 8y : x, y \in \mathbb{N}_0\}$.

Zadanie 5.19. Niech a i b będą względnie pierwszymi liczbami naturalnymi i niech $A = \{ax + by : x, y \in \mathbb{N}_0\}$. Udowodnij, że zbiór $\mathbb{N}_0 \setminus A$ ma dokładnie $\frac{(a-1)(b-1)}{2}$ elementów.

Wniosek 5.20. *Niech $n_0 \in \mathbb{N}_0$ i niech a i b będą względnie pierwszymi liczbami naturalnymi. Wówczas każdą liczbę naturalną c taką, że $c \geqslant (a-1)(b-1) + an_0$ można zapisać w postaci $c = ax + by$ dla pewnych $x, y \in \mathbb{N}_0$ takich, że $x \geqslant n_0$.*

Dowód. Z założeń wynika, że $c - an_0 \geqslant (a-1)(b-1) = ab - a - b + 1 > ab - a - b$, więc z twierdzenia 5.17 mamy, że $c - an_0 = ax + by$ dla pewnych $x, y \in \mathbb{N}_0$. Zatem $c = a(x + n_0) + by$ i $x + n_0 \geqslant n_0$. □

Wniosek 5.21. *Niech $a_1, a_2, \ldots, a_n$, gdzie $n \geqslant 2$ będą względnie pierwszymi liczbami naturalnymi. Wówczas istnieje $K_n \in \mathbb{N}_0$ takie, że każda liczba naturalna $c \geqslant K_n$ jest postaci $c = a_1x_1 + a_2x_2 + \ldots + a_nc_n$ dla pewnych $x_1, x_2, \ldots, x_n \in \mathbb{N}_0$.*

Dowód. Zastosujemy indukcję względem liczby naturalnej $n \geqslant 2$. Dla $n = 2$ na mocy twierdzenia 5.17 wystarczy obrać $K_2 = (a_1 - 1)(a_2 - 1)$.

Załóżmy, że teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ przy dowolnych względnie pierwszych liczbach $a_1, \ldots, a_n$ i niech $a_1, \ldots, a_n$, a_{n+1} będą dowolnymi względnie pierwszymi liczbami naturalnymi. Z twierdzenia 1.14 istnieją względnie pierwsze liczby $b_1, \ldots, b_n \in \mathbb{N}$ takie, że $a_i = db_i$ dla $i = 1, \ldots, n$. Zatem na mocy założenia indukcyjnego istnieje $K_n \in \mathbb{N}_0$ takie, że każda liczba naturalna $c \geqslant K_n$ jest postaci $c = b_1x_1 + \ldots + b_nx_n$ dla pewnych $x_1, \ldots, x_n \in \mathbb{N}_0$. Ponadto z twierdzenia 1.21 i stąd, że liczby $a_1, \ldots, a_n, a_{n+1}$ są względnie pierwsze wynika, że $\mathrm{NWD}(d, a_{n+1}) = 1$, więc na mocy wniosku 5.20 istnieje $L \in \mathbb{N}_0$ takie, że każda liczba naturalna $c \geqslant L$ jest postaci $c = du + a_{n+1}x_{n+1}$ dla pewnych $u, x_{n+1} \in \mathbb{N}_0$ takich, że $u \geqslant K_n$. Ponadto, jak pokazaliśmy, $u = b_1x_1 + \ldots + b_nx_n$ dla pewnych $x_1, \ldots, x_n \in \mathbb{N}_0$, więc $c = a_xx_1 + \ldots + a_nx_n + a_{n+1}x_{n+1}$, bo $db_i = a_i$ dla $i = 1, \ldots, n$. Wystarczy zatem obrać $K_{n+1} = L$. □

Uwaga 5.22. Z wniosku 5.21 wynika, że dla dowolnej liczby naturalnej $n \geqslant 2$ i dla dowolnych względnie pierwszych liczb naturalnych $a_1, a_2, \ldots, a_n$ istnieje największa liczba całkowita $g(a_1, a_2, \ldots, a_n)$, która nie jest postaci $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ dla pewnych nieujemnych liczb całkowitych $x_1, x_2, \ldots, x_n$. Z twierdzenia Sylvestera mamy, że $g(a_1, a_2) = (a_1 - 1) \cdot (a_2 - 1) - 1 = a_1a_2 - a_1 - a_2$. Znany jest też

wzór na $g(a_1, a_2, a_3)$, ale nie jest znany wzór na $g(a_1, a_2, \ldots, a_n)$, gdy n jest dowolną liczbą naturalną (jest to tak zwany Problem Monety Frobeniusa).

Problem Monety Frobeniusa jest związany z wieloma działami matematyki, i ogólniej nauki. Na przykład, techniki wypracowane przy badaniu tego problemu znajdują zastosowanie w badaniu: algebraicznych kodów geometrycznych, wypełnianiu płaszczyzny zadanymi figurami geometrycznymi, generowaniu wektorów losowych, grafów Hamiltona etc. Z tym problemem związanych jest wiele otwartych pytań; część z nich oraz dodatkowe informacje o Problemie Monety może zainteresowany czytelnik znaleźć w monografii [32] poświęconej tym zagadnieniom.

Zadanie 5.23. Wypisz wszystkie elementy zbioru $\mathbb{N}_0 \setminus A$, gdzie $A = \{15x + 21y + 35z : x, y, z \in \mathbb{N}_0\}$.

Zadanie 5.24. Niech a, b, c będą względnie pierwszymi liczbami naturalnymi takimi, że $a \mid b$. Udowodnij, że wtedy $g(a, b, c) = g(a, c) = = ac - a - c$.

Następny przykład był zadaniem na 24. Międzynarodowej Olimpiadzie Matematycznej.

Przykład 5.25. Niech a, b, c będą parami względnie pierwszymi liczbami naturalnymi i niech $A = \{abx + acy + bcz : x, y, z \in \mathbb{N}_0\}$. Udowodnimy, że $d = 2abc - ab - ac - bc \notin A$ oraz każda liczba całkowita $n > d$ należy do A.

Przypuśćmy, że $d \in A$. Wtedy $d = abx + acy + bcz$ dla pewnych $x, y, z \in \mathbb{N}_0$. Zatem $2abc - ab - ac - bc = abx + acy + bcz$, skąd $a \mid bc(z+1)$. Dodatkowo $\mathrm{NWD}(a, b) = \mathrm{NWD}(a, c) = 1$, więc na mocy stwierdzenia 1.25 liczby a i bc są względnie pierwsze. Zatem z zasadniczego twierdzenia arytmetyki, $a \mid z + 1$, skąd $z + 1 \geqslant a$, czyli $z \geqslant a - 1$. Analogicznie dowodzimy, że $y \geqslant b - 1$ i $x \geqslant c - 1$. Stąd $d = abx + acy + bcz \geqslant ab(c - +1) + ac(b-1) + bc(a-1) = 3abc - ab - ac - bc > 2abc - ab - ac - bc = d$, co prowadzi do sprzeczności. Wobec tego $d \notin A$.

Zauważmy, że $(a - 1)(bc - 1) + a(b - 1)(c - 1) = abc - a - bc + +1 + abc - ab - ac + a = 2abc - ab - ac - bc + 1 = d + 1$, skąd

$d+1 \in \mathbb{N}_0$. Weźmy dowolną liczbę całkowitą $k \geqslant d+1$. Wtedy $k \in \mathbb{N}_0$ i $n_0 = (b-1)(c-1) \in \mathbb{N}_0$ oraz $k \geqslant (a-1)(bc-1)+an_0$. Liczby naturalne a i bc są względnie pierwsze, więc na mocy wniosku 5.20 istnieją $x_0, z \in \in \mathbb{N}_0$ takie, że $ax_0 + bcz = k$ i $x_0 \geqslant n_0$. Z twierdzenia 5.17 mamy, że $x_0 = bx + cy$ dla pewnych $x, y \in \mathbb{N}_0$. Zatem $k = abx + acy + bcz$, gdzie $x, y, z \in \mathbb{N}_0$. Wobec tego $k \in A$.

Zadanie 5.26. Niech a i b będą względnie pierwszymi liczbami naturalnymi. Udowodnij, że jeżeli $k \in \mathbb{N}$ i $(a-1)(b-1) \leqslant k < ab$, to istnieje dokładnie jedna para (x, y) nieujemnych liczb całkowitych taka, że $k = ax + by$. Natomiast równanie $ab = ax + by$ ma dokładnie dwa rozwiązania dla $x, y \in \mathbb{N}_0$. A co będzie dla $k > ab$?

Zadanie 5.27. Niech a, b, c, d będą parami względnie pierwszymi liczbami naturalnymi. Udowodnij, że wtedy $g(abc, abd, acd, bcd) = \\ = 3abcd - abc - abd - acd - bcd$.

Rozdział 6

Równanie diofantyczne drugiego stopnia z dwiema niewiadomymi

Ogólne równanie diofantyczne drugiego stopnia z dwiema niewiadomymi x i y ma postać:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{6.1}$$

gdzie liczby całkowite a, b, c, d, e, f są dane, przy czym $a \neq 0$ lub $b \neq 0$ lub $c \neq 0$.

W tym rozdziale będą omówione metody rozwiązywania takich równań. Duże znaczenie będą miały dla nas następujace liczby związane z równaniem (6.1):

$$\Delta = b^2 - 4ac \quad \text{oraz} \quad \Gamma = 4acf + bde - ae^2 - cd^2 - fb^2. \tag{6.2}$$

Standardowe sprawdzenie pokazuje, że zachodzi wzór:

$$(2ae - bd)^2 - \Delta(d^2 - 4af) = -4a\Gamma. \tag{6.3}$$

Ponadto, ponieważ $(p + q + q)^2 = p^2 + q^2 + r^2 + 2pq + 2pr + 2qr$ dla $p, q, r \in \mathbb{Z}$, więc dla $F(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$ mamy tożsamość:

$$4a \cdot F(x, y) = (2ax + by + d)^2 - \Delta y^2 + (4ad - 2bd)y + 4af - d^2. \tag{6.4}$$

Ze wzorów (6.3) i (6.4) uzyskujemy tożsamość:

$$-4a\Delta \cdot F(x,y) = (\Delta y - (2ae - bd))^2 - \Delta(2ax + by + d)^2 + 4a\Gamma. \quad (6.5)$$

6.1 Przypadek $a = c = 0$

Rozważmy najpierw przypadek, gdy $a = c = 0$. Wtedy $b \neq 0$ i równanie (6.1) przybiera postać:

$$bxy + dx + ey + f = 0, \quad (6.6)$$

więc po pomnożeniu obu stron przez b jest równoważne równaniu: $b^2xy + bdx + bey + bf = 0$, a to z kolei jest równoważne równaniu:

$$(bx + e)(by + d) = ed - bf. \quad (6.7)$$

Zajmijmy się najpierw przypadkiem, gdy $ed - bf = 0$. Na mocy (6.2) jest to równoważne temu, że $\Gamma = 0$. Wtedy mamy następujące możliwości:

- $b \nmid e$ i $b \nmid d$. Wtedy równanie (6.6) nie posiada rozwiązania.
- $b \mid e$ i $b \mid d$. Wtedy mamy nieskończenie wiele rozwiązań: $x = -\frac{e}{b}$ i $y \in \mathbb{Z}$ oraz $x \in \mathbb{Z}$ i $y = -\frac{d}{b}$.
- $b \mid e$ i $b \nmid d$. Wtedy mamy nieskończenie wiele rozwiązań: $x = -\frac{e}{b}$ i $y \in \mathbb{Z}$.
- $b \nmid e$ i $b \mid d$. Wtedy mamy nieskończenie wiele rozwiązań: $x \in \mathbb{Z}$ i $y = -\frac{d}{b}$.

Teraz rozważymy przypadek, gdy $ed - bf \neq 0$. Niech X będzie zbiorem wszystkich liczb całkowitych δ dzielących liczbę $ed - bf$ i takich, że $b \mid e - \delta$ oraz $b \mid \frac{ed-bf}{\delta}$. Wtedy X jest zbiorem skończonym i liczba rozwiązań równania (6.6) jest równa $|X|$, czyli jest skończona. Ponadto, gdy $X = \emptyset$, to równanie (6.6) nie posiada rozwiązania. Natomiast dla $X \neq \emptyset$ wszystkie rozwiązania są postaci: $x = \frac{\delta - e}{b}$ i $y = \frac{ed-bf}{b\delta}$ dla $\delta \in X$.

Wobec tego dalej należy rozważać jedynie przypadki, gdy $a \neq 0$ lub $c \neq 0$. Jednak zamiana zmiennej x na y pozwala nam ograniczyć się do jednego przypadku, gdy $a \neq 0$. Okazuje się, że tu także będziemy mieli różne możliwości zależne od wartości Δ i Γ.

Zadanie 6.1. Wyznacz wszystkie rozwiązania następujących równań diofantycznych:

(a) $6xy+3x+2y+1 = 0$, (b) $xy+2x+y+2 = 0$, (c) $xy+x+2y+2 = 0$, (d) $xy+x+y+1 = 0$, (e) $3xy+4x+2y-9 = 0$, (f) $5xy+3x+2y+1 = 0$.

6.2 Przypadek $a \neq 0$ i $\Delta = 0$

Teraz zakładamy, że $a \neq 0$ i $\Delta = b^2 - 4ac = 0$. Wtedy na mocy wzoru (6.4) równanie (6.1) jest równoważne równaniu:

$$(2ax + by + d)^2 - Ey = F, \tag{6.8}$$

gdzie $E = 2bd - 4ae$ i $F = d^2 - 4af$. Możliwe są zatem następujące przypadki:

• $E = F = 0$. Wtedy $2ax + by + d = 0$, więc na mocy twierdzenia 5.11, jeśli $\mathrm{NWD}(2a, b) \nmid d$, to równanie (6.8) nie posiada rozwiązania, zaś w przeciwnym przypadku posiada ono nieskończenie wiele rozwiązań.

• $E = 0$ i $F \neq 0$. Jeżeli F nie jest kwadratem liczby naturalnej, to równanie (6.8) nie posiada rozwiązania. Jeżeli zaś $F = k^2$ dla pewnego $k \in \mathbb{N}$, to równanie (6.8) jest równoważne temu, że $2ax+by+d = k$ lub $2ax + by + d = -k$. Zatem w tym przypadku również równanie (6.8) nie posiada rozwiązania lub posiada nieskończenie wiele rozwiązań.

• $E \neq 0$. Jeżeli nie istnieje $k \in \mathbb{Z}$ takie, że $E \mid k^2 - F$, to równanie (6.8) nie posiada rozwiązania. Załóżmy, że $(2ax_0+by_0+d)^2-Ey_0 = F$ dla pewnych $x_0, y_0 \in \mathbb{Z}$. Oznaczmy $k_0 = 2x_0 + by_0 + d$. Wtedy $k_0 \in \mathbb{Z}$ i $k_0^2 - Ey_0 = F$. Stąd dla $k \in \mathbb{Z}$: $y = \frac{(k_0+2aEk)^2-F}{E} = y_0 + 4ak_0k + +4a^2k^2E \in \mathbb{Z}$ oraz $(k_0 + 2aEk)^2 - Ey = F$. Szukamy $x \in \mathbb{Z}$ takiego, że $2ax+by+d = k_0+2aEk$, czyli $2ax+b(y_0+4ak_0k+4a^2k^2E)+d = = 2ax_0 + by_0 + d + 2aEk$, co jest równoważne temu, że $x = x_0 + +Ek-2k_0k-2aEbk^2$. Z postaci y wynika zatem, że w tym przypadku równanie (6.8) posiada nieskończenie wiele rozwiązań.

Podsumowując, uzyskaliśmy, że **jeżeli $a \neq 0$ i $\Delta = 0$, to równanie (6.1) nie posiada rozwiązania lub posiada nieskończenie wiele rozwiązań**.

Zadanie 6.2. Wyznacz wszystkie rozwiązania następujących równań diofantycznych:

(a) $36x^2 + 24xy + 4y^2 + 36x + 12y + 9 = 0$,
(b) $4x^2 + 12xy + 9y^2 + 4x + 6y + 1 = 0$,
(c) $4x^2 + 12xy + 9y^2 + 4x + 6y - 1 = 0$,
(d) $4x^2 + 12xy + 9y^2 + 4x + 6y - 8 = 0$,
(e) $4x^2 + 12xy + 9y^2 + 4x + y + 2 = 0$,
(f) $4x^2 + 12xy + 9y^2 + 4x + y + 3 = 0$.

6.3 Przypadek $a \neq 0$ i $\Delta < 0$

Niech teraz $\Delta = b^2 - 4ac < 0$. Wtedy $a \neq 0$ oraz $\Delta = -m$ dla pewnego $m \in \mathbb{N}$. Ze wzoru (6.5) wynika, że równanie (6.1) jest równoważne równaniu:

$$(my + 2ae - bd)^2 + m(2ax + by + d)^2 = -4a\Gamma. \tag{6.9}$$

Jeśli $a\Gamma > 0$, to równanie (6.9) nie posiada rozwiązania. Jeśli $\Gamma = 0$, to równanie (6.9) jest równoważne temu, że $my + 2ae - bd = 0$ i $2ax + by + d = 0$, więc albo nie posiada ono rozwiązania albo posiada dokładnie jedno rozwiązanie. Niech teraz $a\Gamma < 0$. Wtedy $|my + 2ae - bd| \leqslant \sqrt{-4a\Gamma}$, skąd wynika, że y może przyjmować jedynie skończenie wiele wartości i w konsekwencji tego x też przyjmuje jedynie skończenie wiele wartości.

Wobec tego, **gdy $\Delta < 0$ to zbiór rozwiązań równania (6.1) jest skończony** (i może być pusty!).

Zadanie 6.3. Wyznacz wszystkie rozwiązania następujących równań diofantycznych:

(a) $12x^2 + 4xy + y^2 + 8x + 4y + 4 = 0$,
(b) $4x^2 + 4xy + 3y^2 + 8x + 4y + 6 = 0$,
(c) $4x^2 + 4xy + 3y^2 + 8x + 4y - 23 = 0$.

6.4 Przypadek $a \neq 0$ i $\Delta = m^2$ dla pewnego $m \in \mathbb{N}$

Niech $a \neq 0$ i $\Delta = m^2$ dla pewnego $m \in \mathbb{N}$. Wtedy ze wzoru (6.5) wynika, że równanie (6.1) jest równoważne równaniu:

$$(m^2y - (2ae - 4bd))^2 - m^2(2ax + by + d)^2 = -4a\Gamma,$$

a to z kolei jest równoważne równaniu:

$$(2max + m(b - m)y + e_1) \cdot (2max + m(b + m)y + e_2) = 4a\Gamma, \quad (6.10)$$

gdzie $e_1 = md - 2ae + bd$ i $e_2 = md + 2ae - bd$.

Jeżeli $\Gamma = 0$, to równanie (6.10) jest równoważne temu, że $2max + m(b-m)y+e_1 = 0$ lub $2max+m(b+m)y+e_2 = 0$, więc w tym przypadku mamy zbiór pusty rozwiązań lub zbiór nieskończony na mocy twierdzenia 5.11.

Jeżeli $\Gamma \neq 0$, to $2max + m(b - m)y + e_1$ jest dzielnikiem liczby $4a\Gamma$, zaś $2max + m(b + m)y + e_2$ jest dzielnikiem dopełniającym tej liczby, przy czym $(2max + m(b - m)y + e_1) - (2max + m(b + m)y + e_2) = -2m^2y + 2bd - 4ae$, więc w tym przypadku zbiór rozwiązań jest skończony (może być pusty!).

Zadanie 6.4. Wyznacz wszystkie rozwiązania następujących równań diofantycznych:

(a) $x^2 + 2xy - 3y^2 + 2x + 2y + 1 = 0$,
(b) $x^2 + 2xy - 3y^2 + 3x + 4y + 2 = 0$,
(c) $x^2 + 2xy - 3y^2 + 2x + 2y - 4 = 0$,
(d) $x^2 + 6xy + 8y^2 + 3x + 6y = 2$.

6.5 Przypadek, gdy $a \neq 0$ i $\Delta \in \mathbb{N}$ oraz $\Delta \neq k^2$ dla $k \in \mathbb{N}$

Niech teraz $a \neq 0$ i $\Delta \in \mathbb{N}$ oraz $\Delta \neq k^2$ dla każdego $k \in \mathbb{N}$. Wówczas na mocy (6.5) równanie (6.1) jest równoważne równaniu:

$$(\Delta y - (2ae - bd))^2 - \Delta(2ax + by + d)^2 = -4a\Gamma. \quad (6.11)$$

Rozważmy najpierw przypadek, gdy $\Gamma = 0$. Z niewymierności liczby $\sqrt{\Delta}$ wynika, że wtedy $2ax + by + d = 0$ i $\Delta y - (2ae - bd) = 0$. Stąd w tym przypadku równanie (6.1) nie posiada rozwiązania albo posiada dokładnie jedno rozwiązanie.

Niech dalej $\Gamma \neq 0$. Wtedy $C = -4a\Gamma \neq 0$. Załóżmy, że para (x_0, y_0) jest rozwiązaniem równania (6.11). Wtedy para (X_0, Y_0), gdzie $Y_0 = 2ax_0 + by_0 + d$ i $X_0 = y_0 - (2ae - bd)$ jest rozwiązaniem równania

$$X^2 - \Delta Y^2 = C. \tag{6.12}$$

Przypuśćmy, że para (X, Y) liczb całkowitych jest rozwiązaniem równania (6.12). Znajdziemy warunki konieczne i dostateczne na to aby istniały liczby całkowite x i y takie, że $Y = 2ax + by + d$ oraz $X = y - (2ae - bd)$. Oczywiście wtedy (x, y) jest rozwiązaniem równania (6.11), przy czym dla różnych par (X, Y) uzyskamy różne odpowiadające im pary (x, y). Ponieważ $y = X + (2ae - bd)$, więc potrzeba i wystarcza aby $2a \mid Y - b(X + (2ae - bd)) - d$. Ponadto $2a \mid Y_0 - b(X_0 + (2ae - bd)) - d$, więc potrzeba i wystarcza aby był spełniony warunek:

$$2a \mid (Y - Y_0) - b(X - X_0). \tag{6.13}$$

Wykorzystamy teraz następujący lemat, który udowodnimy w następnym rozdziale (patrz uwaga 7.15):

Lemat 6.5. *Niech D będzie liczbą naturalną taką, że $D \neq k^2$ dla każdego $k \in \mathbb{N}$. Wówczas dla dowolnej liczby naturalnej $m \geqslant 2$ istnieje nieskończenie wiele par (s, t) liczb naturalnych takich, że $s \equiv 1 \pmod{m}$ i $t \equiv 0 \pmod{m}$ oraz $s^2 - Dt^2 = 1$.*

Zastosujmy ten lemat dla $D = \Delta$ i $m = 2|a|$. Uzyskamy, że istnieje nieskończony zbiór X par (s, t) liczb naturalnych takich, że $s \equiv 1 \pmod{m}$ i $t \equiv 0 \pmod{m}$ oraz $s^2 - \Delta t^2 = 1$. Niech $X_\tau = X_0 s + \Delta Y_0 t$ i $Y_\tau = X_0 t + Y_0 s$ dla $\tau = (s, t) \in X$. Wtedy $X_\tau, Y_\tau \in \mathbb{Z}$ oraz $X_\tau \equiv X_0 \pmod{m}$ i $Y_\tau \equiv Y_0 \pmod{m}$, skąd $2a \mid X_\tau - X_0$ i $2a \mid Y_\tau - Y_0$. Ponadto $X_\tau^2 - Y_\tau^2 = X_0^2 s^2 + 2st\Delta X_0 Y_0 + \Delta^2 Y_0^2 t^2 - \Delta X_0^2 t^2 - 2\Delta X_0 Y_0 ts - \Delta Y_0^2 s^2 = (X_0^2 - \Delta Y_0^2)s^2 - \Delta t^2 (X_0^2 - \Delta Y_0^2) = C \cdot s^2 - \Delta t^2 C = C(s^2 - \Delta t^2) =$

$= C \cdot 1 = C$. Zatem para (X_τ, Y_τ) jest rozwiązaniem równania (6.12) i spełnia warunek (6.13). Zatem dla każdego $\tau = (s,t) \in X$ istnieje para (x_τ, y_τ) liczb całkowitych, która jest rozwiązaniem równania (6.11). Jeżeli $\tau = (s,t), \rho = (u,v) \in X$ są takie, że $(X_\tau, Y_\tau) = (X_\rho, Y_\rho)$, to ponieważ $X_\tau + Y_\tau\sqrt{\Delta} = (s + t\sqrt{\Delta}) \cdot (X_0 + Y_0\sqrt{\Delta})$ i $X_\rho + Y_\rho\sqrt{\Delta} = (u + v\sqrt{\Delta}) \cdot (X_0 + Y_0\sqrt{\Delta})$ oraz $X_0 + Y_0\sqrt{\Delta} \neq 0$ (gdyż $X_0^2 - \Delta Y_0^2 = C \neq 0$), więc $s + t\sqrt{\Delta} = u + v\sqrt{\Delta}$, skąd $s = u$ i $t = v$, czyli $\tau = \rho$.

Wobec tego otrzymujemy nieskończenie wiele rozwiązań (x_τ, y_τ) równania (6.11) i w ten sposób udowodniliśmy następujące twierdzenie Gaussa:

Twierdzenie 6.6. *Jeżeli równanie diofantyczne* (6.1) *posiada rozwiązanie, przy czym Δ jest liczbą naturalną, która nie jest kwadratem liczby naturalnej oraz $\Gamma \neq 0$, to równanie to posiada nieskończenie wiele rozwiązań.*

Wniosek 6.7. *Jeżeli $a, b, c, k \in \mathbb{Z}$, $\Delta = b^2 - 4ac \in \mathbb{N}$, $k \neq 0$ i Δ nie jest kwadratem liczby naturalnej oraz równanie diofantyczne*

$$ax^2 + bxy + cy^2 = k$$

posiada rozwiązanie, to posiada ono nieskończenie wiele rozwiązań.

Dowód. Przy oznaczeniach twierdzenia 6.6 mamy, że $f = -k$ oraz $d = e = 0$. Zatem $\Gamma = k \cdot \Delta \neq 0$. Wobec tego na mocy twierdzenia 6.6 równanie diofantyczne $ax^2 + bxy + cy^2 = k$ posiada nieskończenie wiele rozwiazań. □

Zadanie 6.8. Wyznacz wszystkie rozwiązania równań diofantycznych:

(a) $x^2 + 3xy + y^2 - x + y - 1 = 0$,

(b) $x^2 + 5xy - 5y^2 + x - 5y - 1 = 0$.

Zadanie 6.9. Zastosuj rozumowanie z tego paragrafu do wykazania, że równanie diofantyczne $x^2 + 5xy - 5y^2 - x + y - 1 = 0$ posiada nieskończenie wiele rozwiązań i opisz te rozwiązania za pomocą rozwiązań równania diofantycznego $X^2 - 45Y^2 = 1$.

Zadanie 6.10. Uzasadnij, że równanie $x^2 + xy - y^2 = 1$ posiada nieskończenie wiele rozwiązań w liczbach naturalnych. Czy potrafisz opisać wszystkie rozwiązania tego równania w liczbach naturalnych?

Rozdział 7

Równanie Pella

7.1 Dowód istnienia rozwiązania

Stwierdzenie 7.1. *Jeżeli $D, x, y \in \mathbb{N}$ i $x^2 - Dy^2 = 1$, to D nie jest kwadratem liczby naturalnej.*

Dowód. Przypuśćmy, że $D = k^2$ dla pewnego $k \in \mathbb{N}$. Wtedy $1 = x^2 - k^2y^2 = (x+ky)(x-ky)$, skąd $x+ky \mid 1$, co jest niemożliwe, gdyż $x + ky > 1$. Wobec tego D nie jest kwadratem liczby naturalnej. □

Okazuje się, że jeśli liczba naturalna D nie jest kwadratem liczby naturalnej, to równanie:

$$x^2 - Dy^2 = 1 \tag{7.1}$$

zwane **równaniem Pella** lub **nieoznaczonym równaniem Fermata**, posiada rozwiązanie w liczbach naturalnych. 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 usytematyzował 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 tak zwanych **ułamków łańcuchowych**. 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. [40], s. 240). Dużo ciekawych informacji, konkretnych przykładów i analiz równań "typu Pella" można znaleźć w pracy A. Nowickiego [31].

Dowód twierdzenia 7.1 oprzemy na następującym lemacie odkrytym przez Dirichleta:

Lemat 7.2. *Niech α będzie dowolną niewymierną liczbą rzeczywistą. Wówczas dla każdego naturalnego N istnieją względnie pierwsze liczby całkowite p i q takie, że $0 < q \leqslant N$ oraz*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}.$$

Dowód. Przypomnijmy, że przez $\lfloor x \rfloor$ oznaczamy część całkowitą liczby rzeczywistej x, czyli największą liczbą całkowitą k mniejszą lub równą liczbie x. Wówczas $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$, skąd $0 \leqslant x - \lfloor x \rfloor < 1$. Zatem dla niewymiernych x jest $0 < x - \lfloor x \rfloor < 1$.

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 $n\alpha - \lfloor n\alpha \rfloor$ są niewymierne i należą do przedziału $(0, 1]$. Tych liczb jest dokładnie $N + 1$, a przedziałów mamy dokładnie N, więc w pewnym przedziale $(\frac{k}{N}, \frac{k+1}{N}]$ leżą pewne dwie takie liczby: $x = n\alpha - \lfloor n\alpha \rfloor$ i $y = m\alpha - \lfloor m\alpha \rfloor$, gdzie $1 \leqslant m < n \leqslant N + 1$. Stąd $|x - y| < \frac{1}{N}$. Wobec tego

$$|(n - m)\alpha - (\lfloor n\alpha \rfloor - \lfloor m\alpha \rfloor)| < \frac{1}{N}.$$

Dalej, $a = n - m \in \mathbb{N}$, oraz $a \leqslant N$, $b = \lfloor n\alpha \rfloor - \lfloor m\alpha \rfloor \in \mathbb{Z}$ i $|a\alpha - b| < \frac{1}{N}$. Oznaczmy $d = \mathrm{NWD}(a, b)$. Wtedy na mocy twierdzenia 1.14 istnieją

względnie pierwsze liczby całkowite p i q takie, że $a = dq$ i $b = dp$, skąd $0 < q \leqslant N$ oraz $d|q\alpha - p| < \frac{1}{N}$, a zatem $|\alpha - \frac{p}{q}| < \frac{1}{dqN} \leqslant \frac{1}{qN}$, co kończy nasz dowód. □

W dalszej części tego rozdziału D oznacza liczbę naturalną, która nie jest kwadratem liczby naturalnej.

Twierdzenie 7.3. *Równanie Pella $x^2 - Dy^2 = 1$ posiada rozwiązanie w liczbach naturalnych.*

Dowód. Opierając się na lemacie 7.2 skonstruujemy przez indukcję liczby całkowite $p_1, p_2, \ldots$ i liczby naturalne $q_1, q_2, \ldots$ takie, że

$$\left|\sqrt{D} - \frac{p_1}{q_1}\right| > \left|\sqrt{D} - \frac{p_2}{q_2}\right| > \left|\sqrt{D} - \frac{p_3}{q_3}\right| > \ldots \tag{7.2}$$

oraz

$$\left|\sqrt{D} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2} \quad \text{dla każdego } n \in \mathbb{N}_0. \tag{7.3}$$

Z założenia wynika, że liczba rzeczywista $\alpha = \sqrt{D}$ jest niewymierna. Zatem stosując lemat 7.2 dla $N = 2$ znajdziemy $p_1 \in \mathbb{Z}$ i $q_1 \in \mathbb{N}$ takie, że $q_1 \leqslant 2$ i $|\sqrt{D} - \frac{p_1}{q_1}| < \frac{1}{2q_1}$, skąd $|\sqrt{D} - \frac{p_1}{q_1}| < \frac{1}{q_1^2}$.

Przypuśćmy, że dla pewnego $n \in \mathbb{N}$ skonstruowaliśmy $p_1, \ldots, p_n \in \in \mathbb{Z}$ i $q_1, \ldots, q_n \in \mathbb{N}$ takie, że $|\sqrt{D} - \frac{p_i}{q_i}| < \frac{1}{q_i^2}$ dla $i = 1, 2, \ldots, n$ oraz $|\sqrt{D} - \frac{p_1}{q_1}| > |\sqrt{D} - \frac{p_2}{q_2}| > \ldots > |\sqrt{D} - \frac{p_n}{q_n}|$. Ponadto $|\sqrt{D} - \frac{p_n}{q_n}| > 0$, więc istnieje $M \in \mathbb{N}$ takie, że $|\sqrt{D} - \frac{p_n}{q_n}| > \frac{1}{M}$. Z lematu 7.2 istnieją $p_{n+1} \in \mathbb{Z}$ i $q_{n+1} \in \mathbb{N}$ takie, że $q_{n+1} \leqslant M$ oraz $|\sqrt{D} - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{Mq_{n+1}}$, skąd $|\sqrt{D} - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{q_{n+1}^2}$ oraz $|\sqrt{D} - \frac{p_{n+1}}{q_{n+1}}| < |\sqrt{D} - \frac{p_n}{q_n}|$. Wobec tego zapowiedziana teza została wykazana przez indukcję.

Niech $n \in \mathbb{N}$ oraz $x = p_n$ i $y = q_n$. Wtedy na mocy (7.3) mamy, 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 $|\sqrt{D} + \frac{x}{y}| \leqslant$ $\leqslant |\sqrt{D}| + |\frac{x}{y}| < \frac{1}{y^2} + 2\sqrt{D} \leqslant 1 + 2\sqrt{D}$. Zatem $|x^2 - Dy^2| = y^2|D - \frac{x^2}{y^2}| =$ $= y^2|\sqrt{D} - \frac{x}{y}| \cdot |\sqrt{D} + \frac{x}{y}|$, czyli $|x^2 - Dy^2| < y^2 \cdot \frac{1}{y^2} \cdot (1 + 2\sqrt{D})$, a więc $|p_n^2 - Dq_n^2| < 1 + 2\sqrt{D}$ dla każdego $n \in \mathbb{N}$.

Wobec tego zbiór $\{p_n^2 - Dq_n^2 : n \in \mathbb{N}\}$ jest skończony, więc istnieje $c \in \mathbb{Z}$ takie, że $p_n^2 - Dq_n^2 = c$ dla nieskończenie wielu $n \in \mathbb{N}$. Z niewymierności $\sqrt{D}$ wynika, że $c \neq 0$. Ponieważ z dzielenia przez c mamy dokładnie $|c|$ reszt, więc dla pewnych $r, s \in \{0, 1, \ldots, |c| - 1\}$ oraz dla nieskończenie wielu $n \in \mathbb{N}$ mamy, że $p_n^2 - Dq_n^2 = c$, $p_n \equiv r \pmod{|c|}$ i $q_n \equiv s \pmod{|c|}$.

W szczególności istnieją różne liczby naturalne m i n takie, że $p_m^2 - Dq_m^2 = p_n^2 - Dq_n^2 = c$, $p_m \equiv p_n \pmod{|c|}$ i $q_m \equiv q_n \pmod{|c|}$. Stąd $p_m p_n - Dq_m q_n \equiv p_m^2 - Dq_m^2 = c \equiv 0 \pmod{|c|}$ i $p_n q_m - p_m q_n \equiv p_m q_m - +p_m q_m \equiv 0 \pmod{|c|}$, czyli $p_m p_n - Dq_m q_n = cx_0$ oraz $p_n q_m - p_m q_n = = cy_0$ dla pewnych $x_0, y_0 \in \mathbb{Z}$. Jeśli $y_0 = 0$, to $p_n q_m = p_m q_n$, skąd $\frac{p_m}{q_m} = \frac{p_n}{q_n}$, co na mocy (7.2) przeczy temu, że $m \neq n$. Wobec tego $y_0 \neq 0$.

Dalej, $c^2 x_0^2 - Dc^2 y_0^2 = (p_m p_n - Dq_m q_n)^2 - D(p_n q_m - p_m q_n)^2 = = p_m^2 p_n^2 - 2Dp_m p_n q_m q_n + D^2 q_m^2 q_n^2 - Dp_n^2 q_m^2 + 2Dp_m p_n q_m q_n - Dp_m^2 q_n^2 = = p_n^2(p_m^2 - Dq_m^2) - Dq_n^2(p_m^2 - Dq_m^2) = p_n^2 c - Dq_n^2 c = c(p_n^2 - Dq_n^2) = c^2$ i po skróceniu przez $c^2 \neq 0$, $x_0^2 - Dy_0^2 = 1$. Jednak pokazaliśmy, że $y_0 \neq 0$, 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. □

7.2 Rozwiązanie minimalne

Omówimy teraz pojęcie tak zwanego **rozwiązania minimalnego** równania $x^2 - Dy^2 = 1$. W tym celu udowodnimy następujące dwa lematy.

Lemat 7.4. *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 7.5. *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, $y \geqslant y_0$. Ponadto $x^2 - Dy^2 = x_0^2 - Dy_0^2$, 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 $k^2 < x_0^2$ oraz $k^2 - Dy^2 = x_0^2 - Dy_0^2$, więc $D(y^2 - y_0^2) = k^2 - x_0^2 < 0$, skąd $y^2 < y_0^2$ i $y < y_0$. Zatem $k + y\sqrt{D} < x_0 + y_0\sqrt{D}$, 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 $y \in \mathbb{N}$. □

Załóżmy, że dla pewnego całkowitego C równanie

$$x^2 - Dy^2 = C$$

posiada rozwiązanie w liczbach naturalnych. Wówczas parę (x_0, y_0) liczb naturalnych spełniającą którykolwiek z równoważnych warunków

$(i) - (iv)$ lematu 7.5 nazywamy **rozwiązaniem minimalnym (fundamentalnym)** tego równania.

Przykład 7.6. Niech $a \in \mathbb{N}$ i $a > 1$ oraz $D = a^2 - 1$. Wtedy $D \in \mathbb{N}$ i $a^2 - D \cdot 1^2 = 1$. Zatem na mocy stwierdzenia 7.1, D nie jest kwadratem liczby naturalnej. Ponadto 1 jest najmniejszą liczbą naturalną. Wobec tego na mocy lematu 7.5, para $(a, 1)$ jest rozwiązaniem minimalnym równania $x^2 - (a^2 - 1)y^2 = 1$.

Przykład 7.7. Niech $a \in \mathbb{N}$ i $D = a^2 + 1$. Wtedy $D \in \mathbb{N}$ oraz $(2a^2 + 1)^2 - D(2a)^2 = 1$. Zatem na mocy stwierdzenia 7.1, D nie jest kwadratem liczby naturalnej. 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 $1 = x^2 - Dy^2 \geqslant (ay + 1)^2 - Dy^2 = (ay + 1)^2 - (a^2 + 1)y^2 = 1 + 2ay - y^2$. Zatem $y^2 \geqslant 2ay$, skąd $y \geqslant 2a$. W konsekwencji tego i na mocy lematu 7.5, $(2a^2 + 1, 2a)$ jest rozwiązaniem minimalnym równania $x^2 - (a^2 + 1)y^2 = 1$.

Przykład 7.8. Niech $a \in \mathbb{N}$. Wtedy $D = a^2 + 2 \in \mathbb{N}$. Ponadto $(a^2 + 1)^2 - Da^2 = 1$, więc na mocy stwierdzenia 7.1, D nie jest kwadratem liczby naturalnej. 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 7.5, $(a^2 + 1, a)$ jest rozwiązaniem minimalnym równania $x^2 - (a^2 + 2)y^2 = 1$.

7.3 Opis wszystkich rozwiązań

Możemy teraz sformułować podstawowe twierdzenie o równaniu Pella:

Twierdzenie 7.9. *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 oraz dla każdego $n \in \mathbb{N}_0$:*

$$x_{n+1} = x_0 x_n + D y_0 y_n \quad \text{i} \quad y_{n+1} = y_0 x_n + x_0 y_n.$$

W szczególności każde równanie Pella posiada nieskończenie wiele rozwiązań w liczbach naturalnych.

Dowód. Z twierdzenia 7.3 zbiór rozwiązań w liczbach naturalnych równania Pella $x^2 - Dy^2 = 1$ jest niepusty. Stąd na mocy lematu 7.5 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 $n \in \mathbb{N}_0$. Dodatkowo $x_{n+1} = x_0x_n + Dy_0y_n > x_n$ 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 7.5, $x_0 + y_0\sqrt{D} \leqslant x + y\sqrt{D}$. Ponadto $x_0 + y_0\sqrt{D} > 1$, 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

$$1 \leqslant \frac{x + y\sqrt{D}}{(x_0 + y_0\sqrt{D})^m} < x_0 + y_0\sqrt{D}. \tag{7.4}$$

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 $x_{m-1}^2-Dy_{m-1}^2 = 1$. Wobec tego

$$\frac{x + y\sqrt{D}}{(x_0 + y_0\sqrt{D})^m} = (xx_{m-1}-Dyy_{m-1})+(yx_{m-1}-xy_{m-1})\sqrt{D} = a+b\sqrt{D},$$

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 (7.4), $a + b\sqrt{D} \geqslant 1$. Dalej,

$$a^2 - Db^2 = (xx_{m-1} - Dyy_{m-1})^2 - D(yx_{m-1} - xy_{m-1})^2 =$$

$$= x^2x_{m-1}^2 - 2Dxx_{m-1}yy_{m-1} + D^2y^2y_{m-1}^2 - Dy^2x_{m-1}^2 +$$

$$+2Dxx_{m-1}yy_{m-1} - Dx^2y_{m-1}^2 =$$

$$= x^2(x_{m-1}^2 - Dy_{m-1}^2) - Dy^2(x_{m-1}^2 - Dy_{m-1}^2) = x^2 \cdot 1 - Dy^2 \cdot 1 = 1.$$

Przypuśćmy, że $a + b\sqrt{D} > 1$. Wtedy z lematu 7.4, $a, b \in \mathbb{N}$ oraz na mocy (7.4), $a + b\sqrt{D} < x_0 + y_0\sqrt{D}$, więc zgodnie z lematem 7.5, 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. □

Uwaga 7.10. Zauważmy, że przy oznaczeniach twierdzenia 7.9 dla dowolnego $n \in \mathbb{N}_0$ mamy, że $x_n - y_n\sqrt{D} = \frac{x_n^2 - Dy_n^2 D}{x_n + y_n\sqrt{D}} = \frac{1}{x_n + y_n\sqrt{D}} = \frac{1}{(x_0 + y_0\sqrt{D})^{n+1}} = (\frac{1}{x_0 + y_0\sqrt{D}})^{n+1} = (x_0 - y_0\sqrt{D})^{n+1}$ oraz $x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^{n+1}$, więc $2x_n = (x_0 + y_0\sqrt{D})^{n+1} + (x_0 - y_0\sqrt{D})^{n+1}$ i $2y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^{n+1} - (x_0 - y_0\sqrt{D})^{n+1}$. Stąd mamy następujące wzory jawne na wszystkie rozwiązania równania Pella $x^2 - Dy^2 = 1$ w liczbach naturalnych:

$$\begin{cases} x_n = \frac{(x_0 + y_0\sqrt{D})^{n+1} + (x_0 - y_0\sqrt{D})^{n+1}}{2} \\ y_n = \frac{(x_0 + y_0\sqrt{D})^{n+1} - (x_0 - y_0\sqrt{D})^{n+1}}{2\sqrt{D}} \end{cases} \quad \text{dla } n \in \mathbb{N}_0. \tag{7.5}$$

Z twierdzenia 7.9 oraz z przykładów 7.6 - 7.8 otrzymujemy od razu następujące wnioski:

Wniosek 7.11. *Niech $a \in \mathbb{N}$ i $a > 1$. Wówczas wszystkimi rozwiązania równania Pella $x^2 - (a^2 - 1)y^2 = 1$ w liczbach naturalnych są pary (x_n, y_n) dla $n \in \mathbb{N}_0$ takie, że:*

$$x_n + y_n\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^{n+1}. \tag{7.6}$$

Wniosek 7.12. *Niech $a \in \mathbb{N}$. Wówczas wszystkimi rozwiązania równania Pella $x^2 - (a^2+1)y^2 = 1$ w liczbach naturalnych są pary (x_n, y_n) dla $n \in \mathbb{N}_0$ takie, że:*

$$x_n + y_n\sqrt{a^2+1} = (2a^2 + 1 + 2a\sqrt{a^2+1})^{n+1}. \tag{7.7}$$

Wniosek 7.13. *Niech $a \in \mathbb{N}$. Wówczas wszystkimi rozwiązania równania Pella $x^2 - (a^2+2)y^2 = 1$ w liczbach naturalnych są pary (x_n, y_n) dla $n \in \mathbb{N}_0$ takie, że:*

$$x_n + y_n\sqrt{a^2+2} = (a^2 + 1 + a\sqrt{a^2+2})^{n+1}. \tag{7.8}$$

Lemat 7.14. *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 $y > 0$. Ponadto $y \in \mathbb{Z}$, więc $y \in \mathbb{N}$. Przypuśćmy, że $x \leqslant 0$. Wtedy $|x| = -x < y\sqrt{D} - 1$, bo $x + y\sqrt{D} > 1$ oraz $y \in \mathbb{N}$ 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 $1 > y\sqrt{D}$ oraz $y \geqslant 1$ i $\sqrt{D} > 1$, więc otrzymujemy sprzeczność. Zatem $x > 0$, czyli $x \in \mathbb{N}$. □

Uwaga 7.15. Jako przykład zastosowania twierdzenia 7.9 udowodnimy teraz lemat 6.5. Niech zatem D będzie liczbą naturalną taką, że $D \neq k^2$ dla każdego $k \in \mathbb{N}$ i niech $m \geqslant 2$ będzie liczbą naturalną. Wówczas $\Delta = m^2 D$ jest liczbą naturalną i Δ nie jest kwadratem liczby naturalnej. Zatem na mocy twierdzenia 7.9 istnieje rozwiązanie minimalne (x_0, y_0) równania Pella $x^2 - \Delta y^2 = 1$ oraz dla każdego $n \in \mathbb{N}_0$ istnieją $x_n, y_n \in \mathbb{N}$ takie, że $x_n + y_n\sqrt{\Delta} = (x_0 + y_0\sqrt{\Delta})^{n+1}$ i $x_n^2 - \Delta y_n^2 = 1$. Stąd $x_0^2 \equiv 1 \pmod{m}$ i dla nieparzystych $n \in \mathbb{N}$ mamy, że $x_n + y_n m\sqrt{D} = (x_0 + y_0 m\sqrt{D})^{n+1}$. Stosując wzór dwumianowy Newtona widzimy, że $x_n \equiv x_0^{n+1} \pmod{m}$ oraz $x_0^{n+1} = (x_0^2)^{(n+1)/2}$ i $x_0^2 \equiv 1 \pmod{m}$, więc $x_n \equiv 1 \pmod{m}$. Wtedy para (x_n, my_n) jest rozwiązaniem równania Pella $x^2 - Dy^2 = 1$ dla każdej nieparzystej liczby naturalne n. Kończy to dowód lematu 6.5.

Twierdzenie 7.16. *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 7.9 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 $\beta \geqslant \alpha$. 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 7.14 wynika, że $u, v \in \mathbb{N}$. Stąd oraz z minimalności (u_0, v_0) i z lematu 7.5, $\frac{\beta}{\alpha} = = u + v\sqrt{D} \geqslant \beta$, 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 7.9, $\beta^2 = \alpha^m$ 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 7.17. Znajdziemy rozwiązanie minimalne następującego 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 7.16 rozwiązaniem minimalnym równania Pella $x^2 - 13y^2 = 1$ jest $(18^2 + 13 \cdot 5^2, 2 \cdot 18 \cdot 5) = (649, 180)$.

7.4 Równania związane z równaniem Pella

Przykład 7.18. Pokażemy, że dla liczb naturalnych $a > 2$ równanie $x^2 - (a^2 - 2)y^2 = -1$ nie posiada rozwiązania w liczbach naturalnych. Najpierw udowodnimy, że dla $a \geqslant 2$, $(a^2 - 1, a)$ jest minimalnym rozwiązaniem równania Pella $x^2 - (a^2 - 2)y^2 = 1$. Rzeczywiście, $(a^2 - 1)^2 - (a^2 - 2)a^2 = a^4 - 2a^2 + 1 - a^4 + 2a^2 = 1$ oraz $a^2 - 1 \in \mathbb{N}$, bo $a > 1$. Niech (u, v) będzie rozwiązaniem minimalnym równania Pella $x^2 - (a^2 - 2)y^2 = 1$. Z twierdzenia 7.9, wszystkie rozwiązania równania Pella $x^2 - (a^2 - 2)y^2 = 1$ są postaci (u_m, v_m), gdzie ciągi (u_m) i (v_m) są rosnące oraz $u_m + v_m\sqrt{a^2 - 2} = (u + v\sqrt{a^2 - 2})^m$ dla $m \in \mathbb{N}$. Zatem $(a^2 - 1) + a\sqrt{a^2 - 2} = (u + v\sqrt{a^2 - 2})^m$ dla pewnego $m \in \mathbb{N}$. Stąd, jeśli $m \geqslant 2$, to $a = v_m \geqslant v_2 = 2uv$. Ponadto $u^2 - (a^2 - 2)v^2 > 0$ i $a^2 - 2 > (a - 1)^2$, bo $a \geqslant 2$, więc $u^2 > ((a - 1)v)^2$, czyli $u > (a - 1)v \geqslant a - 1$. Zatem $2uv \geqslant 2u > 2(a - 1) \geqslant a$, bo $a \geqslant 2$. Stąd, $v_m \geqslant v_2 = 2uv > a = v_m$, co prowadzi do sprzeczności. Wobec tego $m = 1$ i $(a^2 - 1, a)$ jest rozwiązaniem minimalnym równania Pella $x^2 - (a^2 - 2)y^2 = 1$.

Niech dalej $a > 2$. Przypuśćmy, że równanie $x^2 - (a^2 - 2)y^2 = -1$ posiada rozwiązanie w liczbach naturalnych. Wtedy istnieje rozwiązanie minimalne (r, s) tego równania. Jednakże, jak pokazaliśmy, $(a^2 - 1, a)$ jest rozwiązaniem minimalnym równania Pella $x^2 - (a^2 - 2)y^2 = 1$, więc na mocy twierdzenia 7.16, $a^2 - 1 = r^2 + (a^2 - 2)s^2$ i $a = 2rs$. Ponadto, $r^2 - (a^2 - 2)s^2 = -1$, więc jeśli $s = 1$, to $r^2 = a^2 - 3$. Ponadto $a \geqslant 3$, więc $(a - 1)^2 < a^2 - 3 < a^2$, skąd $a - 1 < r < a$, co prowadzi do sprzeczności. Wobec tego $s \geqslant 2$ i stąd $a^2 - 1 = r^2 + (a^2 - 1)s^2 \geqslant 1 + (a^2 - 2) \cdot 4 > 1 + (a^2 - 2) = a^2 - 1$. Sprzeczność. Wobec tego dla liczb naturalnych $a > 2$ równanie $x^2 - (a^2 - 2)y^2 = -1$ nie posiada rozwiązania w liczbach naturalnych.

Twierdzenie 7.19. *Załóżmy, że liczba naturalna D nie jest kwadratem liczby całkowitej i równanie $x^2 - Dy^2 = -1$ posiada rozwiązanie w liczbach naturalnych. Jeśli (u_0, v_0) jest rozwiązaniem minimalnym tego równania, to wszystkie jego rozwiązania w liczbach naturalnych są*

postaci (u_n, v_n), *gdzie* $u_n+v_n\sqrt{D} = (u_0+v_0\sqrt{D})^{2n+1}$ *dla* $n = 0, 1, 2, \ldots$.

Dowód. Niech $u, v \in \mathbb{N}$ i $u^2 - Dv^2 = -1$. Z lematu 7.5, $u_0 + v_0\sqrt{D} \leqslant u + v\sqrt{D}$. Jeśli $u_0 + v_0\sqrt{D} = u + v\sqrt{D}$, to $(u, v) = (u_0, v_0)$. Niech dalej, $u_0 + v_0\sqrt{D} < u + v\sqrt{D}$. Wtedy

$$1 < \frac{u + v\sqrt{D}}{u_0 + v_0\sqrt{D}} = \frac{(u + v\sqrt{D})(u_0 - v_0\sqrt{D})}{u_0^2 - Dv_0^2} =$$

$$= \frac{uu_0 - Dvv_0) + (vu_0 - uv_0)\sqrt{D}}{-1} = (Dvv_0 - uu_0) + (uv_0 - vu_0)\sqrt{D},$$

przy czym $(Dvv_0 - uu_0)^2 - D(uv_0 - vu_0)^2 = D^2v^2v_0^2 - 2Dvv_0uu_0 + u^2u_0^2 - Du^2v_0^2 + 2Duv_0vu_0 - Dv^2u_0^2 = u_0^2(u^2 - Dv^2) - Dv_0^2(u^2 - Dv^2) = (u_0^2 - Dv_0^2)(u^2 - Dv^2) = (-1) \cdot (-1) = 1$. Zatem na mocy lematu 7.4, $Dvv_0 - uu_0, uv_0 - vu_0 \in \mathbb{N}$. Z twierdzenia 7.16 wynika, że $(u_0^2 + Dv_0^2, 2u_0v_0)$ jest rozwiązaniem minimalnym równania Pella $x^2 - Dy^2 = 1$ oraz $(u_0^2 + Dv_0^2) + 2u_0v_0\sqrt{D} = (u_0 + v_0\sqrt{D})^2$, więc na mocy twierdzenia 7.9, $(Dvv_0 - uu_0) + (uv_0 - vu_0)\sqrt{D} = (u_0 + v_0\sqrt{D})^{2m}$ dla pewnego $m \in \mathbb{N}$. Zatem $\frac{u+v\sqrt{D}}{u_0+v_0\sqrt{D}} = (u_0 + v_0\sqrt{D})^{2m}$, skąd $u + v\sqrt{D} = (x_0 + y_0\sqrt{D})^{2m+1}$, czyli $(u, v) = (u_m, v_m)$.

Na odwrót, niech $u = u_n$ i $v = v_n$ dla pewnego $n \in \mathbb{N}_0$. Wtedy $u + v\sqrt{D} = (u_0 + v_0\sqrt{D})^{2n+1} = ((u_0 + v_0\sqrt{D})^2)^n(u_0 + v_0\sqrt{d}) = ((u_0^2 + Dv_0^2) + 2u_0v_0\sqrt{D})^n(u_0 + v_0\sqrt{D})$. Na mocy twierdzeń 7.16 i 7.9, $((u_0^2 + Dv_0^2) + 2u_0v_0\sqrt{D})^n = a + b\sqrt{D}$ dla pewnych $a, b \in \mathbb{N}$ takich, że $a^2 - Db^2 = 1$, więc $u + v\sqrt{D} = (a + b\sqrt{D})(u_0 + v_0\sqrt{D}) = (au_0 + Dbv_0) + (av_0 + bu_0)\sqrt{D}$. Zatem $u = au_0 + Dbv_0$ i $v = av_0 + bu_0$, skąd $u^2 - Dv^2 = a^2u_0^2 + 2Dau_0bv_0 + D^2b^2v_0^2 - Da^2v_0^2 - 2Dav_0bu_0 - Db^2u_0^2 = a^2(u_0^2 - Dv_0^2) - Db^2(u_0^2 - Dv_0^2) = (a^2 - Db^2)(u_0^2 - Dv_0^2) = 1 \cdot (-1) = -1$. Zatem (u, v) jest rozwiązaniem w liczbach naturalnych równania $x^2 - Dy^2 = -1$. □

Twierdzenie 7.20. *Niech* $a \in \mathbb{N}$. *Wówczas wszystkimi rozwiązaniami równania* $x^2 - (a^2 + 2)y^2 = -2$ *w liczbach naturalnych są pary* (u_n, v_n) *dla* $n \in \mathbb{N}_0$ *takie, że:*

$$u_n + v_n\sqrt{a^2 + 2} = (a + \sqrt{a^2 + 2})(a^2 + 1 + a\sqrt{a^2 + 2})^n. \tag{7.9}$$

Dowód. Najpierw wykażemy, że dla każdego $n \in \mathbb{N}_0$: $u_n, v_n \in \mathbb{N}$ i $u_n^2-(a^2+2)v_n^2 = -2$. Dla $n = 0$, $u_0 = a$ i $v_0 = 1$, więc $u_0^2-(a^2+2)v_0^2 = a^2 - (a^2 + 2) = -2$. Niech dalej $n > 0$. Wtedy $n = s + 1$ dla pewnego $s \in \mathbb{N}_0$ i na mocy wniosku 7.13 istnieją $x_s, y_s \in \mathbb{N}$ takie, że $x_s + y_s\sqrt{a^2+2} = (a^2 + 1 + a\sqrt{a^2+2})^{s+1}$ oraz $x_s^2 - (a^2 + 2)y_s^2 = 1$. Ponadto $u_n+v_n\sqrt{a^2+2} = (a+\sqrt{a^2+2})(x_s+y_s\sqrt{a^2+2}) = (ax_s+(a^2+2)y_s)+(ay_s+x_s)\sqrt{a^2+2}$, więc $u_n = ax_s+(a^2+2)y_s \in \mathbb{N}$ i $v_n = ay_s+x_s \in \mathbb{N}$. Dalej, $u_n^2-(a^2+2)v_n^2 = a^2x_s^2+2(a^2+2)ax_sy_s+(a^2+2)^2y_s^2-(a^2+2)a^2y_s^2-2(a^2+2)ay_sx_s-(a^2+2)x_s^2 = -2x_s^2+(2a^2+4)y_s^2 = (-2) \cdot (x_s^2 - (a^2 + 2)y_s^2) = (-2) \cdot 1 = -2$. Zatem para (u_n, v_n) jest rozwiązaniem równania $x^2 - (a^2 + 2)y^2 = -2$ w liczbach naturalnych i dodatkowo, na mocy lematu 7.5, $(a, 1)$ jest minimalnym rozwiązaniem tego równania, gdyż 1 jest najmniejszą liczbą naturalną i $a^2 - (a^2 + 2) \cdot 1^2 = -2$.

Załóżmy, że istnieje para $(x, y) \neq (u_n, v_n)$ liczb naturalnych taka, że $x^2 - (a^2 + 2)y^2 = -2$ dla wszystkich $n \in \mathbb{N}_0$. Wtedy z lematu 7.5 mamy, że $x > a$ i $y > 1$. Ponieważ $x^2 - (a^2 + 2)y^2 = -2$, zatem $x^2 - a^2y^2 \equiv 0 \pmod 2$ i $x^2 \equiv x \pmod 2$ oraz $ay \equiv a^2y^2 \pmod 2$, więc $x - ay \equiv 0 \pmod 2$, czyli $\frac{x-ay}{2} \in \mathbb{Z}$. Dodatkowo $x^2 - a^2y^2 = 2y^2 - 2 > 0$, bo $y > 1$, więc $x - ay > 0$ i stąd $\frac{x-ay}{2} \in \mathbb{N}$.

Dodatkowo $x \equiv ay \pmod 2$, więc $ax \equiv a^2y \equiv (a^2 + 2)y \pmod 2$, skąd $\frac{(a^2+2)y-ax}{2} \in \mathbb{Z}$. Ponadto

$$(a^2 + 2)^2y^2 - a^2x^2 = (a^2 + 2)(x^2 + 2) - a^2x^2 = 2a^2 + 2x^2 + 4 > 0,$$

więc $(a^2 + 2)y > ax$ i wobec tego $\frac{(a^2+2)y-ax}{2} \in \mathbb{N}$. Teraz,

$$\frac{x + y\sqrt{a^2+2}}{a + \sqrt{a^2+2}} = \frac{(a^2 + 2)y - ax}{2} + \frac{x - ay}{2}\sqrt{a^2+2}$$

oraz

$$\left(\frac{(a^2 + 2)y - ax}{2}\right)^2 - (a^2 + 2)\left(\frac{x - ay}{2}\right)^2 =$$

$$= \frac{-2x^2 + (2a^2 + 4)y^2}{4} = -\frac{x^2 - (a^2 + 2)y^2}{2} = -\frac{-2}{2} = 1.$$

Stąd na mocy wniosku 7.13 mamy, że $\frac{(a^2+2)y-ax}{2} + \frac{x-ay}{2}\sqrt{a^2+2} = x_s + y_s\sqrt{a^2+2}$ dla pewnego $s \in \mathbb{N}_0$. Wobec tego

$$x + y\sqrt{a^2+2} = (a+\sqrt{a^2+2})(a^2+1+a\sqrt{a^2+2})^{s+1},$$

co prowadzi do sprzeczności. □

Przykład 7.21. Udowodnimy, że istnieje nieskończenie wiele trójek (x, y, z) liczb naturalnych nieparzystych takich, że $x^2+y^2 = z^2+1$. Na mocy twierdzenia 7.9 istnieje nieskończenie wiele par (u, v) liczb naturalnych takich, że $u^2 - 8v^2 = 1$. Oczywiście dla takich par $2 \nmid u$. Stąd liczby naturalne $x = u$, $y = 2v^2 - 1$ i $z = 2v^2 + 1$ są nieparzyste oraz $x^2 + y^2 = u^2 + 4v^4 - 4v^2 + 1 = 8v^2 + 1 + 4v^4 - 4v^2 + 1 = 4v^4 + 4v^2 + 2 = (2v^2+1)^2 + 1 = z^2 + 1$, co kończy nasz dowód.

Przykład 7.22. Wyznaczymy wszystkie pary (x, y) liczb naturalnych takich, że $x^2 - 4xy + y^2 = 1$. Jeżeli $x = y \in \mathbb{N}$, to $x^2 - 4xy + y^2 = -2x^2 \neq 1$. Zatem $x \neq y$ i ze względu na symetrię wystarczy najpierw opisać takie rozwiązania (x, y), że $x > y$. Ponieważ $(x-2y)^2 - 3y^2 = 1$, więc $(x-2y)^2 > 3y^2$, co jest równoważne temu, że $x - 2y < -\sqrt{3}y$ lub $x - 2y > \sqrt{3}y$. W pierwszym przypadku $x < (2-\sqrt{3})y < y$, co prowadzi do sprzeczności, więc $x - 2y > \sqrt{3}y$, skąd $x - 2y = u \in \mathbb{N}$ i $u^2 - 3y^2 = 1$. Na odwrót, jeśli $u, y \in \mathbb{N}$ i $u^2 - 3y^2 = 1$, to $x = u + 2y \in \mathbb{N}$, $x > y$ i $x^2 - 4xy + y^2 = 1$.

Rozwiązaniem minimalnym równania Pella $u^2 - 3y^2 = 1$ jest para $(u_0, y_0) = (2, 1)$. Zatem na mocy twierdzenia 7.9 wszystkie rozwiązania tego równania w liczbach naturalnych są dane wzorami rekurencyjnymi: $u_{n+1} = 2u_n + 3y_n$ i $y_{n+1} = u_n + 2y_n$ dla $n \in \mathbb{N}_0$. Ponadto, $x_0 = u_0 + 2y_0 = 4$ i $y_0 = 1$, więc dla $n \in \mathbb{N}_0$: $x_{n+1} = u_{n+1} + 2y_{n+1} = 2u_n + 3y_n + 2(u_n + 2y_n) = 4u_n + 7y_n = 4(x_n - 2y_n) + 7y_n = 4x_n - y_n$ oraz $y_{n+1} = x_n - 2y_n + 2y_n = x_n$. Wobec tego $x_{n+1} = 4x_n - y_n$ i $y_{n+1} = x_n$ dla $n \in \mathbb{N}_0$. Prze prostą indukcję można pokazać, że $x_n > y_n$ dla każdego $n \in \mathbb{N}_0$, więc $x_{n+1} > x_n$ dla $n \in \mathbb{N}_0$ i wobec tego nasze równanie posiada nieskończenie wiele rozwiązań w liczbach naturalnych.

Pozostałe rozwiązania równania $x^2 - 4xy + y^2 = 1$ w liczbach naturalnych, to pary (y_n, x_n) dla $n \in \mathbb{N}_0$.

Zadanie 7.23. Wyznacz wszystkie liczby trójkątne, które są kwadratami liczb naturalnych, tzn. wyznacz wszystkie pary (x, y) liczb naturalnych takie, że $\frac{x(x+1)}{2} = y^2$.

Zadanie 7.24. Udowodnij, że dla każdej liczby naturalnej a istnieje nieskończenie wiele par (x, y) liczb naturalnych spełniających równanie:

$$(a^2 + 1)(x^2 + 1) = y^2.$$

Twierdzenie 7.25. *Dla dowolnej liczby pierwszej p postaci $4k + 1$ istnieją liczby naturalne x i y takie, że $x^2 - py^2 = -1$.*

Dowód. Na mocy twierdzenia 7.4 równanie Pella $x^2 - py^2 = 1$ posiada rozwiązanie minimalne (x_0, y_0). Jeśli $2 \nmid y_0$, to $y_0^2 \equiv 1 \pmod 4$ oraz $p \equiv 1 \pmod 4$, więc $py_0^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$, skąd $x_0^2 \equiv py_0^2 + 1 \equiv$ $\equiv 1 + 1 \equiv 2 \pmod 4$, co jest niemożliwe. Zatem $y_0 = 2b$ dla pewnego $b \in \mathbb{N}$ oraz $x_0^2 - 4pb^2 = 1$, więc x_0 jest nieparzyste, czyli $x_0 = 2a - 1$ dla pewnego $a \in \mathbb{N}$. Stąd $(2a-1)^2 - 4pb^2 = 1$, czyli $4a^2 - 4a + 1 - 4pb^2 = 1$, a więc $a(a-1) = pb^2$, skąd $a > 1$. Z pierwszości p, $p \mid a - 1$ lub $p \mid a$. W pierwszym przypadku, $a - 1 = ps$ dla pewnego $s \in \mathbb{N}$ i $(ps+1)s = b^2$. Ponadto liczby s i $ps + 1$ są względnie pierwsze, więc z twierdzenia 1.28 otrzymujemy, że $s = u^2$ i $ps + 1 = v^2$ dla pewnych $u, v \in \mathbb{N}$. Stąd $v^2 - pu^2 = 1$ oraz $a = ps + 1 = v^2$, więc $v \leqslant a$ i $x_0 = 2a - 1 > a$, gdyż $a > 1$, więc $v < x_0$, co przeczy minimalności (x_0, y_0).

Wobec tego $p \mid a$, czyli $a = ps$ dla pewnego $s \in \mathbb{N}$ i $s(ps - 1) = b^2$. Jednak liczby s i $ps - 1$ są względnie pierwsze, więc na mocy twierdzenia 1.28, $s = u^2$ i $ps - 1 = v^2$ dla pewnych $u, v \in \mathbb{N}$, czyli $v^2 - pu^2 = -1$. $\square$

Rozdział 8

Równanie Pitagorasa

8.1 Opis wszystkich rozwiązań

Równaniem Pitagorasa nazywamy równanie

$$x^2 + y^2 = z^2, \tag{8.1}$$

w którym niewiadome x, y i z są liczbami naturalnymi.

Oczywiście, każdemu rozwiązaniu równania Pitagorasa odpowiada pewien trójkąt prostokatny o bokach, których długości są liczbami naturalnymi i vice versa. W literaturze rozwiązanie (x, y, z) równiania (8.1) nazywa sie często **trójką pitagorejską**. Pojęcie trójki pitagorejskiej i jej związek z twierdzeniem Pitagorasa jest kamieniem węgielnym kilku dziedzin czystej matematyki, w tym teorii liczb, geometrii elementarnej i algebraicznej oraz matematyki stosowanej. W szczególności w XXI wieku rozkwitł nowy kierunek badań związany z problemem generowania trójek pitagorejskich ze względu na jego znaczenie w kryptografii i tworzeniu algorytmów generowania liczb losowych. Biorąc pod uwagę dużą liczbę publikacji na ten temat, nie sposób przytoczyć choćby ułamka odpowiednich odniesień, w związku z czym zainteresowanego czytelnika kierujemy do monografii [23] i [38], które zawierają przegląd obszernej literatury.

Definicja 8.1. 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 8.2. *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 z elementarnej teorii liczb, liczby naturalne $a = \frac{x}{d}, b = \frac{y}{d}, c = \frac{z}{d}$ są względnie pierwsze. Ponadto, $x^2 + y^2 = z^2$, 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 8.3. *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 $p \mid b$. Dodatkowo $a^2 + b^2 = c^2$, 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 $p \mid c$. Ponadto $b^2 = c^2 - a^2$, 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 $p \mid c$. Dodatkowo $a^2 = c^2 - b^2$, 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 $4 \mid a^2 + b^2$. 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 8.4. *Trójka (a, b, c) liczb naturalnych takich, że liczba a jest parzysta, 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 8.3, $\mathrm{NWD}(a, b) = \mathrm{NWD}(a, c) = 1$ oraz $\mathrm{NWD}(b, c) = 1$, $a = 2k$ dla pewnego $k \in \mathbb{N}$ i liczba b jest nieparzysta oraz liczba c też jest nieparzysta. Ponadto $c > b$ i $4k^2 = a^2 = c^2 - b^2 = (c - b)(c + b)$ oraz liczby $c - b$ i $c + b$ są parzyste, więc $\frac{c-b}{2}, \frac{c+b}{2} \in \mathbb{N}$ i $\frac{c-b}{2} \cdot \frac{c+b}{2} = k^2$. 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 1.28 mamy, że $\frac{c-b}{2} = n^2$ i $\frac{c+b}{2} = m^2$ dla pewnych liczb naturalnych m i n oraz $m^2 > n^2$, 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 $b = \frac{c+b}{2} - \frac{c-b}{2} = m^2 - n^2$. 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 $p \mid c$. Liczby b i c są nieparzyste, gdyż liczby m i n są różnej parzystości, 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. □

Zadanie 8.5. Zastosuj wzory z twierdzenia 8.4 do wypisania wszystkich rozwiązań pierwotnych równania Pitagorasa dla $m \leqslant 20$.

Przykład 8.6. Na mocy twierdzenia 8.4 dla każdego $k \in \mathbb{N}$, $(4k^2 - 1, 4k, 4k^2 + 1)$ jest rozwiązaniem pierwotnym równania Pitagorasa. Wobec tego istnieje nieskończenie wiele rozwiązań pierwotnych równania Pitagorasa.

Zadanie 8.7. Udowodnij, że istnieje nieskończenie wiele trójek (x, y, z) liczb naturalnych takich, że $x^2 + y^2 = z^4$.

Zadanie 8.8. Udowodnij, że istnieje nieskończenie wiele trójek (x, y, z) liczb naturalnych takich, że $x^4 + y^2 = z^2$.

8.2 Rozwiązania w kolejnych liczbach naturalnych

W tym paragrafie omówimy wszystkie rozwiązania równania Pitagorasa $x^2 + y^2 = z^2$ takie, że co najmniej jedna z par (x, y), (y, x), (x, z), (y, z) jest postaci $(k, k+1)$ dla pewnego $k \in \mathbb{N}$. Nasz problem sprowadza się zatem do znalezienia wszystkich rozwiązań w liczbach naturalnych równań:

$$x^2 + y^2 = (x + 1)^2 \tag{8.2}$$

oraz

$$x^2 + (x + 1)^2 = z^2. \tag{8.3}$$

Równanie (8.2) można zapisać w postaci $y^2 = 2x+1$. Oczywiście $x > 1$ i y jest nieparzyste, więc $y = 2k + 1$ dla pewnego $k \in \mathbb{N}$, skąd $x = = 2k^2 + 2k$. W ten sposób udowodniliśmy następujące

Stwierdzenie 8.9. *Wszystkie rozwiązania równania* (8.2) *w liczbach naturalnych dane są wzorami:* $x = 2k^2 + 2k$, $y = 2k + 1$ *dla* $k \in \mathbb{N}$.

Znalezienie wszystkich rozwiązań równania (8.3) jest nieco bardziej skomplikowane. W rozwiązaniu wykorzystamy naszą wiedzę dotyczącą równania Pella.

Stwierdzenie 8.10. *Wszystkie rozwiązania równania* (8.3) *w liczbach naturalnych dane są wzorami rekurencyjnymi:* $x_1 = 3$, $z_1 = 5$ *oraz* $x_{n+1} = 3x_n + 2z_n + 1$ *i* $z_{n+1} = 4x_n + 3z_n + 2$ *dla* $n \in \mathbb{N}$. *W szczególności tych rozwiązań jest nieskończenie wiele.*

Dowód. Równanie (8.3) możemy zapisać w postaci równoważnej:

$$(2x+1)^2 - 2z^2 = -1. \tag{8.4}$$

Zauważmy, że jeżeli $a, b \in \mathbb{N}$, $a > 1$ i $a^2 - 2b^2 = -1$, to $2 \nmid a$, skąd $a = 2k+1$ dla pewnego $k \in \mathbb{N}$ i wtedy $(k, b) = (\frac{a-1}{2}, b)$ jest rozwiązaniem równania (8.4), a zatem ta para jest też rozwiązaniem równania (8.3). Wobec tego wszystkie rozwiązania równania (8.3) w liczbach naturalnych są postaci $(\frac{u-1}{2}, v)$, gdzie (u, v) jest rozwiązaniem równania $u^2 - 2v^2 = -1$ w liczbach naturalnych. Jasne, że para $(1, 1)$ jest rozwiązaniem minimalnym tego równania. Zatem na mocy twierdzenia 7.19 wszystkie rozwiązania w liczbach naturalnych równania $u^2 - 2v^2 = -1$ są postaci (u_n, v_n), gdzie $u_n + v_n\sqrt{2} = (1+\sqrt{2})^{2n+1}$ dla $n = 0, 1, 2, \ldots$. Oczywiście $u_n > 1$ wtedy i tylko wtedy, gdy $n \in \mathbb{N}$.

Dalej, dla $n \in \mathbb{N}$: $u_n - v_n\sqrt{2} = \frac{u_n^2 - 2v_n^2}{u_n + v_n\sqrt{2}} = \frac{-1}{u_n + v_n\sqrt{2}} = (\frac{-1}{1+\sqrt{2}})^{2n+1} = (1-\sqrt{2})^{2n+1} = -(\sqrt{2}-1)^{2n+1}$, więc po dodaniu i odjęciu stronami uzyskanych równości: $2u_n = (1+\sqrt{2})^{2n+1} - (\sqrt{2}-1)^{2n+1}$ i $2v_n\sqrt{2} = (1+\sqrt{2})^{2n+1} + (\sqrt{2}-1)^{2n+1}$. Zatem $u_n = \frac{(1+\sqrt{2})^{2n+1} - (\sqrt{2}-1)^{2n+1}}{2}$ i $v_n = \frac{(1+\sqrt{2})^{2n+1} + (\sqrt{2}-1)^{2n+1}}{2\sqrt{2}}$. Stąd mamy jawne wzory na wszystkie rozwiązania równania (8.3) w liczbach naturalnych:

$$x_n = \frac{(1+\sqrt{2})^{2n+1} - (\sqrt{2}-1)^{2n+1} - 2}{4},$$

$$z_n = \frac{(1+\sqrt{2})^{2n+1} + (\sqrt{2}-1)^{2n+1}}{2\sqrt{2}}$$

dla $n \in \mathbb{N}$. Możemy też wyprowadzić wzory rekurencyjne. Mianowicie dla każdego $n \in \mathbb{N}_0$ mamy, że $u_{n+1} + v_{n+1}\sqrt{2} = (1+\sqrt{2})^2 \cdot (u_n + v_n\sqrt{2}) = (3+2\sqrt{2}) \cdot (u_n + v_n\sqrt{2}) = (3u_n + 4v_n) + (2u_n + 3v_n)\sqrt{2}$, skąd $u_{n+1} = 3u_n + 4v_n$ i $v_{n+1} = 2u_n + 3v_n$. Zatem $u_1 = 7$ i $v_1 = 5$ oraz Dla $n \in \mathbb{N}$: $2x_{n+1} + 1 = u_{n+1} = 3(2x_n + 1) + 4z_n$ i $z_{n+1} = 2(2x_n + 1) + 3z_n$,

czyli $x_{n+1} = 3x_n + 2z_n + 1$ oraz $z_{n+1} = 4x_n + 3z_n + 2$, przy czym $x_1 = \frac{u_1-1}{2} = 3$ i $z_1 = v_1 = 5$. □

Zadanie 8.11. Zastosuj wzory podane w stwierdzenie 8.10 do wypisania ośmiu początkowych rozwiązań równania $x^2 + (x+1)^2 = z^2$ w liczbach naturalnych.

Zadanie 8.12. Wyznacz wszystkie liczby naturalne x i y takie, że $x^2 + (x+2)^2 = y^2$.

8.3 Zastosowania równania Pitagorasa

Twierdzenie 8.13. *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 stąd, $d^2 \mid z$. 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 $\mathrm{NWD}(x, y) = 1$, więc $\mathrm{NWD}(x^2, y^2) = 1$. Ponadto $(x^2)^2 + (y^2)^2 = z^2$, więc (x^2, y^2, z) jest rozwiązaniem pierwotnym równania Pitagorasa. Ze stwierdzenia 8.3 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 8.4 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 8.3, n jest parzyste. Wobec tego m jest nieparzyste i na mocy twierdzenia 8.4 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. 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, $rs(r^2+s^2) = t^2$, więc z twierdzenia 1.28 uzyskujemy, że $r = a^2$, $s = b^2$ 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, $c \geqslant z$. Jednak $c^2 = m < m^2+n^2 = z$, 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 8.13 otrzymujemy jako wniosek dowód Wielkiego twierdzenia Fermata dla wykładnika 4 (o Wielkim twierdzeniu Fermata piszemy szerzej w podrozdziale 16.4):

Wniosek 8.14. *Równanie $x^4+y^4 = z^4$ nie posiada rozwiązania w liczbach naturalnych x, y, z.*

Twierdzenie 8.15. *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 8.3 liczby z i y^2 są różnej parzystości.

Niech najpierw liczba z będzie parzysta. Wtedy z twierdzenia 8.4 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 8.4 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 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 1.28 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 8.4 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 1.28 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 1.28 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 8.4 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 1.28 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 8.16. *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 8.15. □

Zadanie 8.17. 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 8.18. Udowodnij twierdzenie Eulera, które głosi, że nie istnieje trójkąt prostokątny o bokach i środkowych, których długości są liczbami naturalnymi.

Rozdział 9

Pewne równania diofantyczne stopnia trzeciego i czwartego

9.1 Równanie $x^4 + 9x^2y^2 + 27y^4 = z^2$

Modyfikując metodę użytą przez J. Cela w [10] udowodnimy następujące:

Twierdzenie 9.1. *Nie istnieją liczby naturalne x, y, z takie, że:*

$$x^4 + 9x^2y^2 + 27y^4 = z^2. \tag{9.1}$$

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje najmniejsza liczba naturalna z taka, że $z^2 = x^4 + 9x^2y^2 + 27y^4$ dla pewnych $x, y \in \mathbb{N}$. Wyprowadzimy stąd wiele naturalnych wniosków.

Po pierwsze, załóżmy, że $p \mid x$ i $p \mid y$ dla pewnego $p \in \mathbb{P}$. Wtedy $p^4 \mid z^2$, skąd $p^2 \mid z$. Zatem $z = p^2z_1$, $x = px_1$ i $y = py_1$ dla pewnych $x_1, y_1, z_1 \in \mathbb{N}$ i po podstawieniu do równania (9.1) i skróceniu przez p^4 otrzymujemy zależność: $z_1^2 = x_1^4+9x_1^2y_1^2+27y_1^4$. Dodatkowo $z_1 = \frac{z}{p^2} < z$, więc przeczy to minimalności z. Wobec tego $\mathrm{NWD}(x, y) = 1$.

Po drugie, przypuśćmy, że $2 \mid x$. Wtedy z kroku pierwszego, $2 \nmid y$, skąd $y^2 \equiv 1 \pmod 4$ i dodatkowo, $4 \mid z^2 - 27y^4$. Jednakże $-27 \equiv 1$

(mod 4) oraz $y^4 \equiv (y^2)^2 \equiv 1 \pmod 4$, więc $4 \mid z^2+1$, skąd $2 \nmid z$. Zatem $z^2 \equiv 1 \pmod 4$, czyli $z^2+1 \equiv 2 \pmod 4$ i mamy sprzeczność. Wobec tego: $2 \nmid x$. Jeśli także $2 \nmid y$, to $x^2 \equiv 1 \pmod 8$ i $y^2 \equiv 1 \pmod 8$, skąd $x^4 \equiv 1 \pmod 8$, $x^2y^2 \equiv 1 \pmod 8$ i $y^4 \equiv 1 \pmod 8$, a zatem $z^2 \equiv$ $\equiv 1+9+27 \equiv 5 \pmod 8$, co prowadzi do sprzeczności. Wobec tego $2 \mid y$. Stąd i z (9.1) uzyskujemy dodatkowo, że $2 \nmid z$.

Po trzecie, załóżmy, że $3 \mid x$. Wtedy $3^3 \mid z^2$, skąd $3^2 \mid z$ i $z = 9z_1$ oraz $x = 3x_1$ dla pewnych $x_1, z_1 \in \mathbb{N}$. Zatem $3^4x_1^2 + 3^4x_1^2y^2 + 27y^4 = 3^4z_1^2$, skąd $3x_1^4+3x_1^2y^2+y^4 = 3z_1^2$. Wobec tego $3 \mid y^4$, a więc $3 \mid y$, co przeczy temu, że $\mathrm{NWD}(x,y) = 1$. Zatem $3 \nmid x$. Stąd na mocy zależności (9.1), $3 \nmid z$.

Po czwarte, przypuśćmy, że $p \mid x$ i $p \mid z$ dla pewnego $p \in \mathbb{P}$. Wtedy $p \neq 3$ i z równania (9.1), $p \mid 27y^4$, skąd $p \mid 3$ lub $p \mid y$ co daje sprzeczność, bo jak pokazaliśmy, $p \neq 3$ i $\mathrm{NWD}(x,y) = 1$. Zatem $\mathrm{NWD}(x,z) = 1$.

Podsumujmy uzyskane do tej pory zależności:

$$\mathrm{NWD}(x,y) = \mathrm{NWD}(x,z) = 1, \;\; 2 \nmid x, \; 3 \nmid x, \;\; 2 \mid y, \;\; 2 \nmid z, \;\; 3 \nmid z. \tag{9.2}$$

Zatem $y = 2y_1$ dla pewnego $y_1 \in \mathbb{N}$, $\frac{z+x^2}{2} \in \mathbb{N}$, $\frac{z-x^2}{2} \in \mathbb{N}$, gdyż na mocy (9.1), $z^2 > x^4$, czyli $z > x^2$. Zauważmy, że równość (9.1) może być zapisana w postaci:

$$27y_1^4 = \left(\frac{z+x^2}{2} + 9y_1^2\right)\left(\frac{z-x^2}{2} - 9y_1^2\right). \tag{9.3}$$

Ponieważ $\frac{z+x^2}{2} + 9y_1^2 > 0$ oraz $\left(\frac{z+x^2}{2} + 9y_1^2\right)\left(\frac{z-x^2}{2} - 9y_1^2\right) > 0$, więc $\frac{z+x^2}{2} + 9y_1^2, \frac{z-x^2}{2} - 9y_1^2 \in \mathbb{N}$. Jeśli liczby $\frac{z+x^2}{2} + 9y_1^2$ i $\frac{z-x^2}{2} - 9y_1^2$ nie są względnie pierwsze, to posiadają wspólny dzielnik pierwszy p, który dzieli ich sumę, czyli liczbę z. Ponadto $p^2 \mid 27y_1^4$, czyli $p^2 \mid (9y_1^2)^2$, skąd $p \mid 9y_1^2$. Dodatkowo p dzieli $\left(\frac{z+x^2}{2} + 9y_1^2\right) - \left(\frac{z-x^2}{2} - 9y_1^2\right) = x^2 + 18y_1^2$, więc $p \mid x^2$, skąd $p \mid x$. Zatem $p \mid z$ i $p \mid x$, co przeczy (9.2). Wobec tego liczby $\frac{z+x^2}{2} + 9y_1^2$ i $\frac{z-x^2}{2} - 9y_1^2$ są względnie pierwsze i na mocy twierdzenia 1.28 istnieją względnie pierwsze liczby naturalne a, b takie, że $y_1 = ab$, $\frac{z+x^2}{2} + 9y_1^2 = 27a^4$ oraz $\frac{z-x^2}{2} - 9y_1^2 = b^4$ albo $\frac{z+x^2}{2} + 9y_1^2 = a^4$ i $\frac{z-x^2}{2} - 9y_1^2 = 27b^4$. W pierwszym przypadku $27a^4 - b^4 = x^2 + 18y_1^2$,

czyli $27a^4 - b^4 = x^2 + 18a^2b^2$, skąd na mocy (9.2), $b^4 \equiv -1 \pmod 3$, więc $3 \nmid b$ i $b^2 \equiv 1 \pmod 3$, czyli $b^4 \equiv 1 \pmod 3$. Zatem $-1 \equiv 1 \pmod 3$ i mamy sprzeczność. Wobec tego:

$$y_1 = ab, \quad \frac{z + x^2}{2} + 9y_1^2 = a^4, \quad \frac{z - x^2}{2} - 9y_1^2 = 27b^4 \text{ i } \mathrm{NWD}(a, b) = 1. \tag{9.4}$$

Stąd zaś uzyskujemy zależność:

$$x^2 + 18a^2b^2 = a^4 - 27b^4. \tag{9.5}$$

Na mocy (9.2) liczba x jest nieparzysta, więc ze wzoru (9.5) liczby a i b są różnej parzystości. Jeśli $2 \mid a$, to z (9.4), $2 \nmid b$ i wobec tego $b^2 \equiv 1 \pmod 8$, skąd $b^4 \equiv 1 \pmod 8$ oraz $8 \mid 18a^2b^2$ i $a^4 = x^2 + 18a^2b^2 + 27b^4 \equiv \equiv 1 + 0 + 27 \cdot 1 \equiv 4 \pmod 8$ oraz $16 \mid a^4$, co prowadzi do sprzeczności. Zatem $2 \nmid a$ i w konsekwencji $2 \mid b$. Stąd $\frac{b^2}{2} \in \mathbb{N}$ oraz $\frac{a^2+x}{2}, \frac{a^2-x}{2} \in \mathbb{N}$, bo z (9.5), $a^4 > x^2$, czyli $a^2 - x > 0$ oraz liczby a i x są nieparzyste. Zauważmy, że wzór (9.5) można zapisać w postaci:

$$27b^4 = \left(\frac{a^2 + x}{2} - \frac{9}{2}b^2\right)\left(\frac{a^2 - x}{2} - \frac{9}{2}b^2\right). \tag{9.6}$$

Jeśli liczby $u = \frac{a^2+x}{2} - \frac{9}{2}b^2$ i $v = \frac{a^2-x}{2} - \frac{9}{2}b^2$ nie są względnie pierwsze, to posiadają wspólny dzielnik pierwszy p. Wtedy $p \mid u - v$ i $p \mid u + v$, skąd $p \mid x$ i $p \mid a^2 - 9b^2$. Stąd mamy też, że $p \mid 27b^4$ i na mocy (9.2), $p \neq 3$, bo $p \mid x$, więc $p \mid b$. Zatem $p \mid y_1$ i $y = 2y_1$, czyli $p \mid y$. Wobec tego $p \mid x$ i $p \mid y$, co przeczy (9.2). Zatem $\mathrm{NWD}(u, v) = 1$. Ponadto z (9.6), $uv > 0$. Jeśli $u < 0$ i $v < 0$, to $u + v < 0$, czyli $a^2 - 9b^2 < 0$. Z (9.5) wynika, że $a^4 - 9a^2b^2 = x^2 + 9a^2b^2 + 27b^4 > 0$ i $a^2 > 0$, więc $a^2 - 9b^2 > 0$ i mamy sprzeczność. Wobec tego jest $u, v > 0$, czyli $u, v \in \mathbb{N}$. Teraz podobnie argumentując jak przy rozważaniu równości (9.3) uzyskujemy istnienie względnie pierwszych liczb naturalnych m i n takich, że $mn = b$ oraz $\frac{a^2+x}{2} - \frac{9}{2}b^2 = 27m^4$ i $\frac{a^2-x}{2} - \frac{9}{2}b^2 = n^4$ albo $\frac{a^2+x}{2} - \frac{9}{2}b^2 = m^4$ i $\frac{a^2-x}{2} - \frac{9}{2}b^2 = 27n^4$.

W pierwszym przypadku po dodaniu stronami otrzymujemy, że $27m^4 + n^4 = a^2 - 9b^2$, skąd $a^2 = n^4 + 9n^2m^2 + 27m^4$. Ponadto, $a \leqslant y_1 < y < z$, więc mamy sprzeczność z minimalnością liczby z.

Podobnie w drugim przypadku, $27n^4 + m^4 = a^2 - 9b^2$, skąd $a^2 = m^4 + 9m^2n^2 + 27n^4$ i $a < z$, więc mamy sprzeczność z minimalnością liczby z.

Przypuszczenie, że równanie (9.1) posiada rozwiązanie w liczbach naturalnych x, y, z doprowadziło nas ostatecznie do sprzeczności. Wobec tego to równanie nie posiada rozwiązania w liczbach naturalnych. □

9.2 Równanie $x^3 + y^3 = 2z^3$

Twierdzenie 9.2. *Liczby całkowite x, y, z spełniają równanie:*

$$x^3 + y^3 = 2z^3 \tag{9.7}$$

wtedy i tylko wtedy, gdy $x = y = z$ lub $x = -y$ i $z = 0$.

Dowód. Jeśli $x = y = z$, to $x^3 + y^3 = 2x^3 = 2z^3$. Podobnie, jeśli $x = -y$ i $z = 0$, to $x^3 + y^3 = 0 = z^3$.

Na odwrót, załóżmy, że liczby całkowite x, y, z spełniają równanie (9.7), przy czym $x \neq y$ oraz $x \neq -y$. Jeśli $z = 0$, to $0 = (x + y)(x^2 - xy + y^2)$ i $x + y \neq 0$, więc $0 = x^2 - xy + y^2 = (x - \frac{y}{2})^2 + \frac{3}{4}y^2$, co prowadzi do sprzeczności. Zatem $z \neq 0$. Stąd w szczególności $x \neq 0$ lub $y \neq 0$. Możemy zakładać, że z jest niezerową liczbą całkowitą o najmniejszym module, dla której istnieją różne $x, y \in \mathbb{Z}$ takie, że $2z^3 = x^3 + y^3$. Jeśli liczby x i y mają wspólny dzielnik pierwszy p, to $p^3 \mid 2z^3$. Jeśli $p = 2$, to $p^2 \mid z^3$, skąd $p \mid z$, a jeśli $p > 2$, to też stąd $p \mid z$. Zatem $x = px_1$, $y = py_1$ i $z = pz_1$, więc $2p^3z_1^3 = p^3x_1^3 + p^3y_1^3$, czyli $2z_1^3 = x_1^3 + y_1^3$. Ponadto $z_1 = \frac{z}{p}$, więc $z_1 \neq 0$ i $x_1 = \frac{x}{p} \neq \frac{y}{p} = y_1$, skąd $|z_1| < |z|$ i mamy sprzeczność z minimalnością modułu liczby z. Wobec tego liczby x i y są względnie pierwsze. Z zależności (9.7) wynika dodatkowo, że te liczby są tej samej parzystości. Stąd x i y są nieparzyste i $x + y = 2u$ oraz $x - y = 2v$ dla pewnych $u, v \in \mathbb{Z}$, przy czym $u, v \neq 0$, bo $x \neq \pm y$. Zatem $x = u + v$ i $y = u - v$ oraz $\mathrm{NWD}(x, y) = 1$, więc stąd $\mathrm{NWD}(u, v) = 1$. Ponadto, $(u + v)^3 + (u - v)^3 = 2z^3$, skąd

$$u(u^2 + 3v^2) = z^3. \tag{9.8}$$

Możliwe są teraz dwa przypadki: $3 \nmid u$ oraz $3 \mid u$. W przypadku pierwszym, jeśli istnieje $p \in \mathbb{P}$ takie, że $p \mid u$ i $p \mid u^2 + 3v^2$, to $p \neq 3$ i $p \mid 3v^2$, skąd $p \mid v$, wbrew temu, że $\mathrm{NWD}(u, v) = 1$. Wobec tego w tym przypadku liczby u i $u^2 + 3v^2$ są względnie pierwsze. Z (9.8) na mocy twierdzenia 1.28 uzyskujemy, że $u = z_1^3$ i $u^2 + 3v^2 = z_2^3$ dla pewnych $z_1, z_2 \in \mathbb{Z}$ oraz $\mathrm{NWD}(z_1^3, z_2^3) = 1$, więc $\mathrm{NWD}(z_1, z_2) = 1$. Ponadto $3 \nmid u$, więc $3 \nmid z_1$. Dalej, $3v^2 = z_2^3 - z_1^6 = (z_2 - z_1^2)(z_2^2 + z_2 z_1^2 + z_1^4)$, czyli $3v^2 = (z_2 - z_1^2)((z_2 - z_1^2)^2 + 3z_2 z_1^2)$. Oznaczmy $t = z_2 - z_1^2$. Jeśli $p \in \mathbb{P}$ jest taka, że $p \mid t$ i $p \mid z_1$, to $p \mid z_2$, wbrew temu, że $\mathrm{NWD}(z_1, z_2) = 1$. Zatem $\mathrm{NWD}(t, z_1) = 1$ oraz $(z_2 - z_1^2)^2 + 3z_2 z_1^2 = t^2 + 3(z_2 - z_1^2)z_1^2 + 3z_1^4 = t^2 + 3tz_1^2 + 3z_1^4$, więc $t(t^2 + 3tz_1^2 + 3z_1^4) = 3v^2$, skąd $3 \mid t$. Zatem $t = 3t_1$ dla pewnego $t_1 \in \mathbb{Z}$ oraz $t_1(9t_1^2 + 9t_1 z_1^2 + 3z_1^4) = v^2$. Stąd $3 \mid v$, czyli $v = 3v_1$ dla pewnego $v_1 \in \mathbb{Z}$. Zatem $9 \mid 3t_1 z_1^4$ i ponieważ $3 \nmid z_1$, to $3 \mid t_1$, czyli $t_1 = 3t_2$ dla pewnego $t_2 \in \mathbb{Z}$. Stąd $t_2(27t_2^2 + 9t_2 z_1^2 + z_1^4) = v_1^2$. Ponadto $\mathrm{NWD}(t, z_1) = 1$, więc $\mathrm{NWD}(t_2, z_1) = 1$ i wobec tego $\mathrm{NWD}(t_2, 27t_2^2 + 9t_2 z_1^2 + z_1^4) = 1$. Z twierdzenia 1.28 istnieją $b \in \mathbb{N}_0$ i $c \in \mathbb{Z}$ takie, że $t_2 = b^2$ i $27b^4 + 9b^2 z_1^2 + z_1^4 = c^2$. Dodatkowo $z_1 \neq 0$, więc $|z_1| \in \mathbb{N}$ i $t_2 \neq 0$, bo $t_2 \mid 3v^2$ i $v = x - y \neq 0$. Zatem $b \in \mathbb{N}$, więc $|c| \in \mathbb{N}$. W takim razie równanie $x^4 + 9x^2y^2 + 27y^4 = z^2$ posiada rozwiązanie w liczbach naturalnych, wbrew twierdzeniu 9.1.

Pozostaje do rozważenia przypadek, gdy $3 \mid u$. Wtedy $3 \nmid v$, gdyż $\mathrm{NWD}(u, v) = 1$ i $u = 3u_1$ dla pewnego $u_1 \in \mathbb{Z}$. Ponadto $u = x + y \neq 0$, więc $u_1 \neq 0$. Korzystając z (9.8) uzyskujemy, że $3 \mid z$, czyli $z = 3z_1$ dla pewnego niezerowego $z_1 \in \mathbb{Z}$. Zatem $3u_1(9u_1^2 + 3v^2) = 27z_1^3$, a więc $u_1(3u_1^2 + v^2) = 3z_1^3$. Jednak $3 \nmid v$, więc $3 \nmid 3u_1^2 + v^2$, a zatem $3 \mid u_1$ i $u_1 = 3u_2$ dla pewnego niezerowego $u_2 \in \mathbb{Z}$. Stąd $u_2(27u_2^2 + v^2) = z_1^3$. Dodatkowo $\mathrm{NWD}(u, v) = 1$ i $u = 9u_2$, więc $\mathrm{NWD}(u_2, v) = 1$, skąd $\mathrm{NWD}(u_2, 27u_2^2 + v^2) = 1$ i z twierdzenia 1.28 wynika, że $u_2 = a^3$ i $27u_2^2 + v^2 = b^3$ dla pewnych względnie pierwszych liczb całkowitych a i b, przy czym $ab = z_1$, więc $a, b \neq 0$. Ponadto $3 \nmid v$, więc $3 \nmid b$ i $27a^6 + v^2 = b^3$. Podstawmy $t = b - 3a^2$. Wtedy $t \in \mathbb{Z}$ i $3 \nmid t$ oraz $27a^6 + v^2 = (t + 3a^2)^3$, skąd $v^2 = t(t^2 + 9ta^2 + 27a^4)$. Jeśli $p \in \mathbb{P}$ jest takie, że $p \mid t$ i $p \mid t^2 + 9ta^2 + 27a^4$, to $p \neq 3$ i $p \mid 27a^4$, skąd $p \mid a$. Jednak $p \mid t$ i $t = b - 3a^2$, więc $p \mid b$. Stąd $p \mid a$ i $p \mid b$, co przeczy temu, że $\mathrm{NWD}(a, b) = 1$. Zatem liczby t i $t^2 + 9ta^2 + 27a^4$ są względnie pierwsze i na mocy

twierdzenia 1.28, $t = a_1^2$ oraz $t^2+9ta^2+27a^4 = a_2^2$ dla pewnych niezerowych liczb całkowitych a_1 i a_2. Wobec tego $|a_1|^4+9|a_1|^2|a|^2+27|a|^4 = |a_2|^2$, przy czym $|a_1|, |a_2|, |a| \in \mathbb{N}$, co przeczy twierdzeniu 9.1.

Kończy to dowód naszego twierdzenia. □

Wniosek 9.3. *Nie istnieje ciąg arytmetyczny złożony z sześcianów trzech różnych liczb naturalnych.*

Dowód. Załóżmy, że istnieją różne liczby naturalne a, b, c takie, że (a^3, b^3, c^3) jest ciągiem arytmetycznym. Wtedy $b^3 - a^3 = c^3 - b^3$, skąd $c^3 + a^3 = 2b^3$. Ponadto $b \neq 0$, więc z twierdzenia 9.2 uzyskujemy, że $c = a$ i mamy sprzeczność. □

Wniosek 9.4. *Wszystkimi rozwiązaniami w liczbach całkowitych x i y równania:*

$$x^3 - 2y^3 = 1 \tag{9.9}$$

są $x = y = -1$ oraz $x = 1$ i $y = 0$. W szczególności to równanie nie posiada rozwiązania w liczbach naturalnych.

Dowód. Niech $x, y \in \mathbb{Z}$ będą takie, że $x^3-2y^3 = 1$. Wtedy $x^3+(-1)^3 = 2y^3$, więc na mocy twierdzenia 9.2 mamy, że $x = -1 = y$ lub $x = -(-1) = 1$ i $y = 0$. Ponadto $(-1)^3 - 2 \cdot (-1)^3 = 1$ i $1^3 - 2 \cdot 0^3 = 1$. □

Wniosek 9.5. *Wszystkimi rozwiązaniami w liczbach całkowitych x i y równania:*

$$x^3 - 2y^3 = -1 \tag{9.10}$$

są $x = y = 1$ oraz $x = -1$ i $y = 0$. W szczególności jedynym rozwiązaniem tego równania w liczbach naturalnych jest $x = y = 1$.

Dowód. Niech $x, y \in \mathbb{Z}$ będą takie, że $x^3 - 2y^3 = -1$. Wtedy $x^3 + 1^3 = 2y^3$, więc z twierdzenia 9.2 mamy, że $x = 1 = y$ lub $x = -1$ i $y = 0$. Ponadto $1^3 - 2 \cdot 1^3 = -1$ i $(-1)^3 - 2 \cdot 0^3 = -1$. □

Przypomnijmy, że liczby postaci $t_n = \binom{n+1}{2} = \frac{n(n+1)}{2}$ dla $n \in \mathbb{N}$ nazywamy **liczbami trójkątnymi**. Ich nazwa pochodzi stąd, że $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ i liczby $1, 2, 3, \ldots, n$ można ustawić w trójkąt, wykorzystując to, że k jest sumą k jedynek dla $k = 1, 2, \ldots, n$.

Wniosek 9.6. *Liczba* 1 *jest jedyną liczbą trójkątną będącą sześcianem liczby naturalnej.*

Dowód. Oczywiście $t_1 = 1 = 1^3$. Załóżmy, że istnieje liczba naturalna $n > 1$ taka, że $t_n = m^3$ dla pewnego $m \in \mathbb{N}$. Wtedy $n(n+1) = 2m^3$ i $m > 1$, bo $t_n \geqslant n > 1$.

Jeśli $2 \mid n$, to $n = 2k$ dla pewnego $k \in \mathbb{N}$ i wtedy $k(2k+1) = m^3$. Ponadto $\mathrm{NWD}(k, 2k+1) = \mathrm{NWD}(k, 1) = 1$, więc z twierdzenia 1.28 otrzymujemy, że $k = a^3$ i $2k + 1 = b^3$ dla pewnych $a, b \in \mathbb{N}$. Stąd $b^3 - 2a^3 = 1$ i mamy sprzeczność z wnioskiem 9.4.

Wobec tego $2 \nmid n$. Stąd po uwzględnieniu, że $n > 1$ mamy $n \geqslant 3$ i $n = 2k+1$ dla pewnego $k \in \mathbb{N}$. Zatem $(2k+1)(k+1) = m^3$. Oznaczmy $s = k+1$. Wtedy $s > 1$ i $2k+1 = 2s-1$ oraz $s(2s-1) = m^3$. Dodatkowo $\mathrm{NWD}(s, 2s-1) = \mathrm{NWD}(s, -1) = 1$, więc z twierdzenia 1.28 mamy, że $s = a^3$ i $2s - 1 = b^3$ dla pewnych $a, b \in \mathbb{N}$, przy czym $a > 1$, bo $s > 1$. Stąd $b^3 - 2a^3 = -1$ i mamy sprzeczność z wnioskiem 9.5. □

Wniosek 9.7. *Jedynym rozwiązaniem w liczbach naturalych x i y równania*

$$x^2 - y^3 = 1 \tag{9.11}$$

jest $x = 3$, $y = 2$.

Dowód. Oczywiście $3^2 - 2^3 = 1$. Niech $x, y \in \mathbb{N}$ będą takie, że $x \neq 3$ oraz $x^2 - y^3 = 1$. Wtedy $x^2 = y^3 + 1 \geqslant 2$, skąd $x \geqslant 2$ oraz dla $x = 2$, $y^3 = 3$, co jest niemożliwe. Zatem $x > 3$. Z równości $x^2 - y^3 = 1$ wynika, że liczby x i y są różnej parzystości. Jeśli x jest parzyste, to $\mathrm{NWD}(x+1, x-1) = \mathrm{NWD}(x-1, 2) = 1$ i $(x-1)(x+1) = y^3$, więc z twierdzenia 1.28 otrzymujemy, że $x-1 = a^3$ i $x+1 = b^3$ dla pewnych $a, b \in \mathbb{N}$. Stąd $2 = b^3 - a^3 = (b-a)(b^2+ab+a^2)$, a zatem $a^2+ab+b^2 \mid 2$. Ponadto $a^2 + ab + b^2 \geqslant 3$, więc mamy sprzeczność.

Zatem x musi być nieparzyste, czyli $x = 2k + 1$ dla pewnego $k \in \{2, 3, \ldots\}$, bo $x > 3$ i uzyskujemy, że $2k(2k + 2) = y^3$. Wobec tego $2 \mid y^3$ i stąd $2 \mid y$, a zatem $y = 2c$ dla pewnego $c \in \mathbb{N}$ oraz $4k(k + 1) = 8c^3$, skąd $\frac{k(k+1)}{2} = c^3$. Dodatkowo $k \geqslant 2$, więc mamy sprzeczność z wnioskiem 9.6. □

Wniosek 9.8. *Jedynymi liczbami naturalnmi x, y, m, n spełniającymi równanie*

$$x^{2m} - y^{3n} = 1 \tag{9.12}$$

są $m = n = 1$, $x = 3$, $y = 2$.

Dowód. Niech $m, n, x, y \in \mathbb{N}$ spełniają równanie (9.12). Wówczas $a^2 - b^3 = 1$ dla $a = x^m$ i $b = y^n$. Ponadto $a, b \in \mathbb{N}$, więc z wniosku 9.7 mamy, że $a = 3$ i $b = 2$. Zatem $x^m = 3$ i $y^n = 2$, skąd $x = 3$, $m = 1$, $y = 2$ i $n = 1$. Implikacja odwrotna jest oczywista. □

Wniosek 9.9. *Wszystkimi rozwiązaniami równania* (9.11) *w liczbach wymiernych x i y są: $x = 0$, $y = 1$; $x = \pm 1$, $y = 0$; $x = \pm 3$, $y = 2$.*

Dowód. Bezpośrednie sprawdzenie pokazuje, że $x = 0$, $y = 1$; $x = \pm 1$, $y = 0$; $x = \pm 3$, $y = 2$ są rozwiązaniami równania (9.11). Załóżmy, że istnieje inna para (x, y) liczb wymiernych taka, że $x^2 - y^3 = 1$. Wtedy $x \neq 0$, bo inaczej $y = -1$, a ponieważ $(-x)^2 = x^2$, więc możemy zakładać, że $x > 0$. Jeśli $x = 1$, to $y = 0$, co prowadzi do sprzeczności z naszymi założeniami. Zatem $x \neq 1$ i stąd $y \neq 0$. Podobnie, $x \neq 3$, skąd $y \neq 2$. Istnieją względnie pierwsze liczby naturalne a, b takie, że $x = \frac{a}{b}$ i istnieją względnie pierwsze liczby całkowite k, n takie, że $y = \frac{k}{n}$ oraz $k \neq 0$ i $n > 0$. Stąd $\frac{a^2}{b^2} - \frac{k^3}{n^3} = 1$, a zatem $a^2n^3 - k^3b^2 = n^3b^2$. Stąd $n^3 \mid k^3b^2$, więc z zasadniczego twierdzenia arytmetyki, $n^3 \mid b^2$. Ponadto, $b^2 \mid a^2n^3$, więc znowu z zasadniczego twierdzenia arytmetyki, $b^2 \mid n^3$. Wobec tego $n^3 \leqslant b^2$ i $b^2 \leqslant n^3$, skąd $b^2 = n^3$. Ponieważ $b, n \in \mathbb{N}$, więc z twierdzenia o jednoznaczności rozkładu uzyskujemy stąd, że $b = M^3$ i $n = M^2$ dla pewnego $M \in \mathbb{N}$. Wobec tego mamy zależność: $a^2 - k^3 = M^6$. Ponadto, $\mathrm{NWD}(a, b) = 1$ i $\mathrm{NWD}(k, n) = 1$, więc $\mathrm{NWD}(a, M) = \mathrm{NWD}(k, M) = 1$.

Możliwe są teraz tylko dwa przypadki:
I. $2 \mid a$ lub $2 \mid M$ oraz II. $2 \nmid a$ i $2 \nmid M$.

W przypadku I mamy, że k jest nieparzyste, więc z równości $k^3 = a^2 - M^6 = (a - M^3)(a - M^3)$ wynika, że liczby $a - M^3$ i $a + M^3$ są nieparzyste. Jeśli $p \in \mathbb{P}$ i $p \mid a + M^3$ oraz $p \mid a - M^3$, to $p \neq 2$ oraz $p \mid (a + M^3) + (a - M^3)$, czyli $p \mid 2a$, skąd $p \mid a$, więc $p \mid M^3 = (a + M^3) - a$.

Zatem $p \mid M$, co przeczy temu, że $\mathrm{NWD}(a, M) = 1$. Zatem w tym przypadku liczby $a - M^3$ i $a + M^3$ są względnie pierwsze. Ponadto $(a - +M^3)(a + M^3) = k^3$, więc z twierdzenia 1.28 uzyskujemy, że $a - M^3 = = u^3$ oraz $a + M^3 = v^3$ dla pewnych $u, v \in \mathbb{Z}$. Dodatkowo $a \neq \pm b = = \pm M^3$, więc $u \neq 0$ i $v \neq 0$. Stąd po odjęciu stronami tych równości uzyskujemy, że $v^3 + (-u)^3 = 2M^3$. Dodatkowo $M > 0$, więc z twierdzenia 9.2 mamy, że $v = -u = M$, co przeczy temu, że $u \in \mathbb{N}$.

W drugim przypadku z równości $k^3 = (a - M^3)(a + M^3)$ wynika, że $2 \mid k$. Zatem $k = 2K$ dla pewnego $K \in \mathbb{Z}$. Stąd $2K^3 = \frac{a-M^3}{2} \cdot \frac{a+M^3}{2}$ i z nieparzystości liczb a i M liczby $\frac{a-M^3}{2}$ i $\frac{a+M^3}{2}$ są całkowite. Jeśli $p \in \in \mathbb{P}$ jest ich wspólnym dzielnikiem, to p dzieli ich sumę i ich różnicę, skąd $p \mid a$ i $p \mid M^3$, czyli $p \mid M$, co przeczy temu, że $\mathrm{NWD}(a, M) = = 1$. Zatem liczby $\frac{a-M^3}{2}$ i $\frac{a+M^3}{2}$ są względnie pierwsze i twierdzenia o jednoznaczności rozkładu mamy, że istnieją $u, v \in \mathbb{Z}$ takie, że albo $\frac{a-M^3}{2} = 2u^3$ i $\frac{a+M^3}{2} = v^3$ albo $\frac{a-M^3}{2} = u^3$ i $\frac{a+M^3}{2} = 2v^3$. W pierwszym przypadku mamy, że $v^3 - 2u^3 = M^3$, więc $v^3 + (-M)^3 = 2u^3$. Z twierdzenia 9.2 wynika, że $v = -M = u$ lub $v = M$ i $u = 0$. Wtedy $a = -M^3 < 0$ albo $a = M^3$, skąd $x = 1$, co przeczy naszym założeniom o x i y. Natomiast w drugim przypadku, $M^3 + u^3 = 2v^3$, więc z twierdzenia 9.2 uzyskujemy, że $M = u = v$ albo $u = -M$ i $v = 0$, skąd $a = 3M^3$ i $x = 3$ albo $a = -M^3 < 0$ i też obie możliwości prowadzą do sprzeczności.

Kończy to dowód naszego wniosku. □

Twierdzenie 9.10. *Nie istnieją liczby naturalne x, y, z takie, że $x^4 + x^2y^2 + y^4 = z^2$.*

Dowód. Przypuśćmy, że tak nie jest. Wtedy na mocy zasady minimum istnieje najmniejsza liczba naturalna z taka, że $x^4 + x^2y^2 + y^4 = z^2$ dla pewnych $x, y \in \mathbb{N}$. Niech $d = \mathrm{NWD}(x, y)$. Wtedy $d \in \mathbb{N}$ oraz $d \mid x$ i $d \mid y$, więc $d^4 \mid x^4$, $d^4 \mid x^2y^2$ i $d^4 \mid y^4$, więc $d^4 \mid z^2$, skąd $d^2 \mid z$ na mocy twierdzenia 1.30. Wobec tego $\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2} \in \mathbb{N}$ i $\frac{z}{d^2} \leqslant z$ oraz $(\frac{x}{d})^4 + (\frac{x}{d})^2(\frac{y}{d})^2 + (\frac{y}{d})^4 = (\frac{z}{d^2})^2$. Zatem z minimalności z uzyskujemy, że $d = 1$, czyli $\mathrm{NWD}(x, y) = 1$.

Jeśli liczby x i y są nieparzyste, to ze stwierdzenia 4.1, $x^2 \equiv 1 \pmod 4$ i $y^2 \equiv 1 \pmod 4$, skąd $x^4 + x^2y^2 + y^4 \equiv 3 \pmod 4$, czyli

$z^2 \equiv 3 \pmod 4$, wbrew stwierdzeniu 4.1. Zatem liczby x i y są różnej parzystości. Ze względu na symetryczność rozpatrywanego równania możemy bez zmniejszania ogólności zakładać dalej, że liczba x jest parzysta, a liczba y jest nieparzysta.

Nasze równanie możemy teraz zapisać w postaci równoważnej: $4z^2 = 4x^2 + 4x^2y^2 + 4y^4 = (2x^2 + y^2)^2 + 3y^4$, co można przekształcić do postaci

$$3y^4 = (2z - 2x^2 - y^2)(2z + 2x^2 + y^2).$$

Jeśli $3 \mid 2z - 2x^2 - y^2$ i $3 \mid 2z + 2x^2 + y^2$, to $3^2 \mid 3y^4$, skąd $3 \mid y$ oraz $3 \mid 4z$, skąd $3 \mid z$ i dodatkowo $3 \mid 2x^2$, skąd $3 \mid x$, wbrew temu, że $\mathrm{NWD}(x, y) = 1$. Wobec tego $3 \mid 2z - 2x^2 - y^2$ i $3 \nmid 2z + 2x^2 + y^2$ albo $3 \nmid 2z - 2x^2 - y^2$ i $3 \mid 2z + 2x^2 + y^2$.

W pierwszym przypadku $y^4 = \frac{2z-2x^2-y^2}{3} \cdot (2z+2x^2+y^2)$. Jeśli liczby w nawiasach nie są względnie pierwsze, to mają pewien wspólny dzielnik pierwszy p. Ponadto te liczby są nieparzyste i $3 \nmid 2z+2x^2+y^2$, więc $p > 3$ oraz $p \mid 3y^4$ i $p \mid 4z$, skąd $p \mid y$ i $p \mid z$. Dodatkowo $p \mid 2z+2x^2+y^2$, więc $p \mid 2x^2$, skąd $p \mid x$, co przeczy temu, że $\mathrm{NWD}(x, y) = 1$. Zatem liczby naturalne $\frac{2z-2x^2-y^2}{3}$ i $2z + 2x^2 + y^2$ są względnie pierwsze i na mocy twierdzenia 1.28, $\frac{2z-2x^2-y^2}{3} = a^4$ i $2z + 2x^2 + y^2 = b^4$ oraz $y = ab$ dla pewnych względnie pierwszych $a, b \in \mathbb{N}$. Stąd $4x^2 = b^4-2a^2b^2-3a^4$. Ponadto $2 \mid x$, więc $8 \mid b^4 - 2a^2b^2 - 3a^4$ oraz liczby a i b są nieparzyste, więc ze stwierdzenia 4.1, $a^2 \equiv 1 \pmod 8$ i $b^2 \equiv 1 \pmod 8$, skąd $b^4 - 2a^2b^2 - 3a^4 \equiv 1 - 2 - 3 \equiv 4 \pmod 8$, co prowadzi do sprzeczności.

W drugim przypadku $y^4 = (2z - 2x^2 - y^2) \cdot \frac{2z+2x^2+y^2}{3}$ i analogicznie jak w pierwszym przypadku pokazujemy, że liczby naturalne $2z-2x^2-+y^2$ i $\frac{2z+2x^2+y^2}{3}$ są względnie pierwsze. Zatem z twierdzenia 1.28 wynika, że $2z - 2x^2 - y^2 = a^4$, $\frac{2z+2x^2+y^2}{3} = b^4$ i $y = ab$ dla pewnych względnie pierwszych liczb nieparzystych $a, b \in \mathbb{N}$. Stąd $4x^2 = = 3b^4 - 2a^2b^2 - a^4 = (b^2 - a^2)(3b^2 + a^2)$. Na mocy stwierdzenia 4.1, $3b^2 + a^2 \equiv 4 \pmod 8$, co oznacza, że $\frac{3b^2+a^2}{4} \in \mathbb{N}$ i $2 \nmid \frac{3b^2+a^2}{4}$. Jeżeli $p \in \mathbb{P}$ i $p \mid b^2 - a^2$ oraz $p \mid \frac{3b^2+a^2}{4}$, to $p > 2$ i $p \mid 4b^2$, skąd $p \mid b$ i $p \mid a$, co jest niemożliwe. Zatem liczby naturalne $\frac{3b^2+a^2}{4}$ i $b^2 - a^2$ są względnie pierwsze i ich iloczyn jest równy x^2. Z twierdzenia 1.28 mamy, że

$b^2 - a^2 = m^2$, $\frac{3b^2+a^2}{4} = n^2$ dla pewnych $m, n \in \mathbb{N}$. Zatem $b^2 = a^2 + m^2$ i na mocy twierdzenia 8.4, $b = r^2 + s^2$, $m = 2rs$ oraz $a = r^2 - s^2$ dla pewnych $r, s \in \mathbb{N}$. Stąd $n^2 = r^4 + r^2s^2 + s^4$. Ponadto $n^2m^2 = x^2$, więc $n \leqslant x$ i $z^2 > x^4$, więc $n \leqslant x \leqslant x^2 < z$, co przeczy minimalności z.

□

Rozdział 10

Twierdzenie Chao Ko

10.1 Od Catalana do Mihăilescu

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 w [19], że hipoteza Catalana jest prawdziwa dla parzystych m. W rozdziale 14 podajemy uwspółcześnioną wersję oryginalnego dowodu Lebesgue'a. Warto wspomnieć, że ten Lebesgue to inna osoba niż bardziej znamy Henri Léon Lebesgue (1875-1941), od którego pochodzi tak zwana miara Lebesgue'a.

Przypadek parzystego n ma jednak długą historię. W 1738 roku L. Euler udowodnił hipotezę Catalana (por. [15]) w przypadku, gdy $2 \mid n$ i $3 \mid m$. Nasz dowód tego wyniku jest podany we wniosku 9.8. 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. W następnym paragrafie zaprezentujemy uproszczoną wersję oryginalnego dowodu twierdzenia Chao Ko.

Pierwszy dowód hipotezy Catalana podał dopiero w 2002 roku rumuński matematyk Pred Mihăilescu (por. [24]). Dowód ten jest zadziwiająco krótki, lecz bazuje na specyficznych własnościach tak zwanych ciał[1] cyklotomicznych. Od tej pory tę hipotezę nazywamy twierdzeniem Mihăilescu.

Dużo ciekawych informacji o hipotezie Catalana i próbach jej udowodnienia można znaleźć w artykule przeglądowym [22] oraz monografii [33].

10.2 Twierdzenie Chao Ko

Lemat 10.1. *Niech $p \in \mathbb{P}$ i niech a i b będą różnymi liczbami całkowitymi. Wówczas $a-b \mid a^p - b^p$ oraz*

$$\frac{a^p - b^p}{a-b} \equiv (a-b)^{p-1} \pmod{p}.$$

W szczególności $p \mid \frac{a^p-b^p}{a-b}$ wtedy i tylko wtedy, gdy $p \mid a-b$.

Dowód. Niech $c = a - b$. Ponieważ $a \neq b$, więc $c \neq 0$ i $a = b + c$. Ze wzoru dwumianowego Newtona

$$a^p - b^p = (b+c)^p - b^p =$$

$$\sum_{k=1}^{p} \binom{p}{k} b^{p-k} c^k = c \sum_{k=1}^{p} \binom{p}{k} b^{p-k} c^{k-1},$$

skąd $c \mid a^p - b^p$, czyli $a - b \mid a^p - b^p$. Ponadto $\frac{a^p-b^p}{a-b} = \sum_{k=1}^{p} \binom{p}{k} b^{p-k} c^{k-1}$ oraz z pierwszości liczby p wynika, że $p \mid \binom{p}{k}$ dla $k = 1, 2, \ldots, p-1$. Wobec tego

$$\frac{a^p - b^p}{a-b} = (a-b)^{p-1} + pb^{p-1} + pb(a-b)K \tag{10.1}$$

[1] Podstawowe informacje o ciałach znajdują się w VI części tej książki

dla pewnego całkowitego K. Stąd $\frac{a^p-b^p}{a-b} \equiv (a-b)^{p-1} \pmod{p}$. Zatem, jeżeli $p \mid \frac{a^p-b^p}{a-b}$, to $p \mid (a-b)^{p-1}$, skąd z pierwszości p, $p \mid a-b$. Ponadto, jeśli $p \mid a-b$, to $p \mid (a-b)^{p-1}$ i stąd $p \mid \frac{a^p-b^p}{a-b}$. □

Lemat 10.2. *Niech $p \in \mathbb{P}$ i niech a i b będą różnymi, względnie pierwszymi liczbami całkowitymi. Wtedy $a-b \mid a^p-b^p$ oraz:*
(i) jeżeli $p \mid a-b$, to $\mathrm{NWD}(a-b, \frac{a^p-b^p}{a-b}) = p$,
(ii) jeżeli $p \nmid a-b$, to $\mathrm{NWD}(a-b, \frac{a^p-b^p}{a-b}) = 1$.

Dowód. Z lematu 10.1, $a-b \mid a^p-b^p$. Natomiast ze wzoru (10.1) wynika, że, $\mathrm{NWD}(a-b, \frac{a^p-b^p}{a-b}) = \mathrm{NWD}(a-b, pb^{p-1})$. Ponadto $\mathrm{NWD}(a-b, b) = \mathrm{NWD}(b, a) = 1$, więc $\mathrm{NWD}(a-b, pb^{p-1}) = \mathrm{NWD}(a-b, p)$. Wobec tego

$$\mathrm{NWD}(a-b, \tfrac{a^p-b^p}{a-b}) = \mathrm{NWD}(a-b, p) = \begin{cases} p & \text{jeśli } p \mid a-b \\ 1 & \text{jeśli } p \nmid a-b \end{cases}, \text{ gdyż}$$

$p \in \mathbb{P}$. □

Następny lemat został odkryty i udowodniony przez T. Nagella w [28]. Prezentujemy własną wersję dowodu tego wyniku w oparciu o rezultaty uzyskane przez nas dla równania Pella.

Lemat 10.3. *Jeżeli p jest nieparzystą liczbą pierwszą i $x, y \in \mathbb{N}$ oraz $x^2 = y^p + 1$, to $2 \mid y$, $p \mid y+1$ i $p \mid x$.*

Dowód. Załóżmy, że $2 \nmid y$. Wtedy $2 \mid y^p + 1$ i $x^2 = y^p + 1$, więc $2 \mid x$. Wobec tego $(x-1)(x+1) = y^p$ oraz jeśli $d = \mathrm{NWD}(x-1, x+1)$, to $2 \nmid d$ oraz $d \mid (x+1)-(x-1) = 2$, skąd $d = 1$, czyli $\mathrm{NWD}(x-1, x+1) = 1$. Z twierdzenia 1.28 mamy zatem, że $x-1 = u^p$ i $x+1 = v^p$ dla pewnych $u, v \in \mathbb{N}$. Stąd $v^p - u^p = 2$. Ponadto $v^p - u^p = (v-u)(v^{p-1} + {+}v^{p-2}u + \ldots + vu^{p-2} + u^{p-1})$, więc $v^{p-1} + v^{p-2}u + \ldots + vu^{p-2} + u^{p-1} \mid 2$, skąd $p \leqslant v^{p-1} + v^{p-2}u + \ldots + vu^{p-2} + u^{p-1} \leqslant 2$ i mamy sprzeczność. Wobec tego $2 \mid y$ i w szczególności $y > 1$.

Załóżmy, że $p \nmid x$. Wtedy $p \nmid y^p + 1$. Dodatkowo $y^p + 1 = (y+1)(y^{p-1} - y^{p-2} + y^{p-3} - \ldots - y + 1)$, więc $p \nmid y+1$. Ponadto $y^p + 1 = y^p - (-1)^p$, $y+1 = y-(-1)$ oraz $\mathrm{NWD}(y, -1) = 1$. Zatem z lematu 10.2 (ii), liczby $y+1$ i $y^{p-1} - y^{p-2} + y^{p-3} - \ldots - y + 1$ są względnie pierwsze i z twierdzenia 1.28 mamy, że $y+1 = s^2$ oraz $y^{p-1} - y^{p-2} + y^{p-3} - \ldots - y +$

$+1 = r^2$ dla pewnych względnie pierwszych liczb naturalnych r i s. Jednak $2 \mid y$, więc s jest nieparzyste. Ponadto $y > 1$, więc $s > 1$. Dalej, $y = s^2 - 1$ i $x^2 - y^p = 1$, więc $x^2 - (s^2-1)(y^{\frac{p-1}{2}})^2 = 1$. Z wniosku 7.11 istnieje $m \in \mathbb{N}$ takie, że:

$$x + y^{\frac{p-1}{2}}\sqrt{s^2-1} = (s + \sqrt{s^2-1})^m. \tag{10.2}$$

Ze wzoru dwumianowego Newtona,

$$(s+\sqrt{s^2-1})^m = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{2k} s^{m-2k}(s^2-1)^k +$$

$$+\sqrt{s^2-1} \cdot \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2k+1} s^{m-2k-1}(s^2-1)^k.$$

Stąd

$$x = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{2k} s^{m-2k}(s^2-1)^k = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{2k} s^{m-2k} y^k \equiv s^m \pmod{y}$$

oraz

$$y^{\frac{p-1}{2}} = \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2k+1} s^{m-2k-1}(s^2-1)^k. \tag{10.3}$$

Zatem $x \equiv s^m \pmod{y}$ i $ms^{m-1} \equiv 0 \pmod{y}$. Ponadto $y = s^2 - 1$, więc $\mathrm{NWD}(y, s) = 1$, skąd $\mathrm{NWD}(s^{m-1}, y) = 1$ i wobec tego $m \equiv 0 \pmod{y}$, czyli $y \mid m$. Dodatkowo $2 \mid y$, więc $2 \mid m$, czyli $m = 2n$ dla pewnego $n \in \mathbb{N}$. Stąd i ze wzoru (10.3), $s \mid y^{\frac{p-1}{2}}$. Jednakże $\mathrm{NWD}(s, y) = 1$, więc $s = 1$. Wcześniej pokazaliśmy, że $s > 1$, więc mamy sprzeczność. Wobec tego $p \mid x$. Jeśli $p \nmid y + 1$, to z lematu 10.1, $p \nmid \frac{y^p+1}{y+1}$, skąd $p \nmid y^p + 1$, czyli $p \nmid x^2$, co prowadzi do sprzeczności. W konsekwencji tego $p \mid y + 1$. □

Następne twierdzenie zostało po raz pierwszy udowodnione przez Chao Ko w [11]. W pracy [12] podano prostszy dowód. W naszym dowodzie opieramy się na pomysłach z [12], przy czym nieco upraszczamy to rozumowanie przez wyeliminowanie lematu 3 z tego artykułu.

Twierdzenie 10.4. *Niech p będzie liczbą pierwszą większą od 3. Wówczas równanie $x^2 = y^p + 1$ nie posiada rozwiązania w liczbach naturalnych.*

Dowód. Załóżmy, że $x^2 = y^p + 1$ dla pewnych $x, y \in \mathbb{N}$ i dla pewnej liczby pierwszej $p > 3$. Wtedy $x > 1$ i z lematu 10.3, $2 \mid y$, $p \mid y + 1$ oraz $p \mid x$. Ponadto stąd $2 \nmid x$, więc $2 \mid x - 1$ i z lematu 10.2 mamy, że $\mathrm{NWD}(x - 1, x + 1) = 2$. Istnieją zatem względnie pierwsze liczby naturalne u i v takie, że $u > v$ oraz $x + 1 = 2u$ i $x - 1 = 2v$. Ponadto $2^2uv = y^p$ oraz $y = 2z$ dla pewnego $z \in \mathbb{N}$, więc $uv = 2^{p-2}z^p$. Dodatkowo $\mathrm{NWD}(u, v) = 1$, więc stąd mamy dwa możliwe przypadki:
I. $2^{p-2} \mid u$ i $2 \nmid v$ oraz II. $2^{p-2} \mid v$ i $2 \nmid u$.

Rozważmy przypadek I. Wtedy $u = 2^{p-2}w$ dla pewnego $w \in \mathbb{N}$ oraz $\mathrm{NWD}(w, v) = 1$ i $wv = z^p$. Zatem z twierdzenia 1.28 otrzymujemy, że $w = a^p$ i $v = b^p$ dla pewnych względnie pierwszych liczb naturalnych a i b. Ponadto $z = ab$, $u = 2^{p-2}a^p$ i $x + 1 = 2^{p-1}a^p$ oraz $x - 1 = 2b^p$ i $2 \nmid b$, bo $2 \nmid v$. Wobec tego $2 = (x + 1) - (x - 1) = 2^{p-1}a^p - 2b^b$, skąd $b^p = 2^{p-2}a^p - 1$ oraz $2x = (x + 1) + (x - 1) = 2^{p-1}a^p + 2b^p$, czyli $x = 2^{p-2}a^p + b^p = 2^{p-2}a^p + 2^{p-2}a^p - 1$, a zatem $x = 2^{p-1}a^p - 1$. Wobec tego $\frac{x+3}{2} = \frac{2^{p-1}a^p+2}{2} = 2^{p-2}a^p + 1 = b^p + 2$. Dalej, $2^{p-2}a^p = 1 + b^p$, więc $2^p a^p = 4 + 4b^p$ i wobec tego, $(b^2)^p + (2a)^p = (b^p)^2 + 4b^p + 4 = (b^p + 2)^2$. Zatem

$$(b^2)^p + (2a)^p = (b^p + 2)^2 = \left(\frac{x + 3}{2}\right)^2. \tag{10.4}$$

Dodatkowo $p \mid x$ i $p > 3$, więc $p \nmid x+3$, skąd $p \nmid \frac{x+3}{2}$. Ponadto, $2 \nmid b$ oraz $\mathrm{NWD}(a, b) = 1$, więc $\mathrm{NWD}(b^2, 2a) = 1$. Jednak $(b^2)^p+(2a)^p = (b^2+2a)\cdot \cdot\frac{(b^2)^p+(2a)^p}{b^2+2a}$, gdzie $\frac{(b^2)^p+(2a)^p}{b^2+2a} \in \mathbb{N}$ na mocy lematu 10.1, więc $p \nmid b^2 + 2a$ i na mocy lematu 10.2 liczby $b^2 + 2a$ i $\frac{(b^2)^p+(2a)^p}{b^2+2a}$ są względnie pierwsze. Zatem z twierdzenia 1.28 mamy, że $b^2 + 2a = c^2$ dla pewnego $c \in \mathbb{N}$. Dodatkowo $b^p = 2^{p-2}a^p - 1 = 2^{p-3}a^p + (2^{p-3}a^p - 1) \geqslant a^p$, więc $b \geqslant a$ i stąd $b^2 < c^2 = b^2 + 2a \leqslant b^2 + 2b < (b + 1)^2$, więc $b < c < b + 1$, co prowadzi do sprzeczności.

Rozważmy przypadek II. Wtedy $v = 2^{p-2}w$ dla pewnego $w \in \mathbb{N}$ oraz $\mathrm{NWD}(w, u) = 1$ i $wu = z^p$. Zatem z twierdzenia 1.28 uzyskujemy, że $w = a^p$ i $u = b^p$ dla pewnych względnie pierwszych liczb naturalnych

a i b. Ponadto, $z = ab$, $v = 2^{p-2}a^p$ i $x + 1 = 2b^p$ oraz $x - 1 = 2^{p-1}a^p$ i $2 \nmid b$, bo $2 \nmid u$. Wobec tego $2 = (x + 1) - (x - 1) = 2b^p - 2^{p-1}a^p$, skąd $b^p = 2^{p-2}a^p + 1$ oraz $2x = (x + 1) + (x - 1) = 2b^p + 2^{p-1}a^p$, czyli $x = b^p + 2^{p-2}a^p = 2b^p - 1$, a zatem $x = 2b^p - 1$. Wobec tego $\frac{x-3}{2} = \frac{2b^p-4}{2} = b^p - 2$. Dalej, $2^{p-2}a^p = b^p - 1$, więc $2^p a^p = 4b^p - 4$ i stąd, $(b^2)^p - (2a)^p = (b^p)^2 - 4b^p + 4 = (b^p - 2)^2$. Zatem

$$(b^2)^p - (2a)^p = (b^p - 2)^2 = \left(\frac{x-3}{2}\right)^2. \tag{10.5}$$

Dodatkowo $p \mid x$ i $p > 3$, więc $x - 3 > 0$ i $p \nmid x - 3$, skąd $p \nmid \frac{x-3}{2}$. Ponadto, $2 \nmid b$ i $\mathrm{NWD}(a, b) = 1$, więc $\mathrm{NWD}(b^2, 2a) = 1$. Mamy też, że $(b^2)^p - (2a)^p = (b^2 - 2a) \cdot \frac{(b^2)^p-(2a)^p}{b^2-2a}$, gdzie $\frac{(b^2)^p-(2a)^p}{b^2-2a} \in \mathbb{N}$ na mocy lematu 10.1, więc $p \nmid b^2 - 2a$ i na mocy lematu 10.2 liczby $b^2 - 2a$ i $\frac{(b^2)^p-(2a)^p}{b^2-2a}$ są względnie pierwsze. Zatem z twierdzenia 1.28 otrzymujemy, że $b^2 - 2a = c^2$ dla pewnego $c \in \mathbb{N}$. Dodatkowo $b^p = 2^{p-2}a^p + 1 > a^p$, więc $b > a$ i stąd $-2a > -2b$, a zatem $-2a > -2b + 1$, bo $-2a \neq -2b + 1$. Wobec tego $(b - 1)^2 < c^2 = b^2 - 2a < b^2$, więc $b - 1 < c < b$, co prowadzi do sprzeczności.

Kończy to dowód naszego twierdzenia. □

Wniosek 10.5. *Niech m, n, x, y będą liczbami naturalnymi takimi, że $n > 1$ oraz $x^{2m} - y^n = 1$. Wtedy $m = 1$, $n = x = 3$ i $y = 2$.*

Dowód. Jeśli $2 \mid n$, to $n = 2l$ dla pewnego $l \in \mathbb{N}$ i wówczas $(y^l)^2 < (x^m)^2 = (y^l)^2 + 1 < (y^l + 1)^2$, skąd $y^l < x^m < y^l + 1$, co prowadzi do sprzeczności. Zatem $2 \nmid n$. Jeśli $3 \mid n$, to teza wynika z wniosku 9.8. Niech dalej $3 \nmid n$. Ponieważ $n > 1$ i $2 \nmid n$ i $3 \nmid n$, więc n posiada dzielnik pierwszy $p > 3$, czyli $n = pk$ dla pewnego $k \in \mathbb{N}$. Zatem $a^2 = b^p + 1$ dla $a = x^m \in \mathbb{N}$ i $b = y^k \in \mathbb{N}$, co przeczy twierdzeniu Chao Ko. □

Zadanie 10.6. Znajdź wszystkie liczby naturalne x i y takie, że $x^y - y^x = 1$.

Zadanie 10.7. Niech $m, n, x, y \in \mathbb{N}$, $m, n > 1$ i $x^n - y^m = 1$. Udowodnij, że wtedy liczby m i n są względnie pierwsze.

Część III

Ułamki łańcuchowe i ich zastosowania

Rozdział 11

Ułamki łańcuchowe

11.1 Podstawy teoretyczne

Ułamki łańcuchowe początkowo były używane głównie do rozwiązywania równań diofantycznych, w szczególności równania Pella. W XX wieku ułamki łańcuchowe stały się bardziej powszechne w innych działach matematyki. Na przykład Robert M. Corless w artykule [14] 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 [7] i [18].

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:

$$\langle a_0, a_1, \ldots, a_n \rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n \rangle} \quad \text{dla} \quad n = 1, 2, \ldots. \tag{11.1}$$

Przykład 11.1. Ze wzoru (11.1) 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 11.2. *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 (11.1), $\langle a_1\rangle = a_1 \geqslant 1$. 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 (11.1), $\langle a_1, a_2, \ldots, a_n, a_{n+1}\rangle = a_1 + \frac{1}{\langle a_2, \ldots, a_{n+1}\rangle}$. 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 (11.1), $\langle a_1\rangle = a_1 > 1$. Jeśli zaś $n > 1$, to z (i) oraz z (11.1), $\langle a_1, a_2, \ldots, a_n\rangle = a_1 + \frac{1}{\langle a_2, \ldots, a_n\rangle} > a_1 \geqslant 1$, skąd $\langle a_1, a_2, \ldots, a_n\rangle > 1$. Na mocy (11.1), $\langle a_0, a_1, \ldots, a_n\rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n\rangle}$, 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:

$$\langle a_0, \ldots, a_n, \ldots, a_{n+m}\rangle = \langle a_0, \ldots, a_{n-1}, \langle a_n, \ldots, a_{n+m}\rangle\rangle. \tag{11.2}$$

Na mocy (11.1) wzór (11.2) zachodzi dla $n = 1$ przy dowolnym $m \in \mathbb{N}$. Przypuśćmy, że wzór (11.2) zachodzi dla pewnego naturalnego n przy dowolnym $m \in \mathbb{N}$. Wtedy dla dowolnego $m \in \mathbb{N}$ na mocy (11.1) 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 (11.1):

$$\langle a_0, a_1, \ldots, a_{n+1+m}\rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+1+m}\rangle\rangle} =$$

$$= \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+1+m}\rangle\rangle,$$

co oznacza, że wzór (11.2) zachodzi też dla liczby $n+1$. Wobec tego na mocy zasady indukcji matematycznej wzór (11.2) zachodzi dla dowolnych $n, m \in \mathbb{N}$.

Stosując wzór (11.2) dla $m = 1$ uzyskujemy następującą zależność:

$$\langle a_0, a_1, \ldots, a_{n-1}, a_n, a_{n+1}\rangle = \left\langle a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right\rangle. \quad (11.3)$$

Lemat 11.3. *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:*

$$\lim_{n\to\infty} \langle a_0, a_1, \ldots, a_k, b_n\rangle = \langle a_0, a_1, \ldots, a_k, \lim_{n\to\infty} b_n\rangle. \quad (11.4)$$

Dowód. Ponieważ $b_n \geqslant 1$ dla każdego $n \in \mathbb{N}$ i ciąg (b_n) jest zbieżny, więc $b = \lim_{n\to\infty} b_n \geqslant 1$ i $\langle a_0, a_1, \ldots, a_k, b\rangle$ jest dobrze zdefiniowane. Wzór (11.4) 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 $\lim_{n\to\infty} \langle a_0, b_n\rangle = \lim_{n\to\infty} \left(a_0 + \frac{1}{b_n}\right) = a_0 + \frac{1}{b} = \langle a_0, b\rangle$. Przypuśćmy teraz, że teza zachodzi dla pewnego $k \in \mathbb{N}_0$. Wtedy dla $k+1$ na mocy wzoru (11.3) 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 $\lim_{n\to\infty} \langle a_{k+1}, b_n\rangle = \langle a_{k+1}, b\rangle \geqslant 1$, więc stąd i z założenia indukcyjnego otrzymujemy, że $\lim_{n\to\infty} \langle a_0, \ldots, a_{k+1}, b_n\rangle = \langle a_0, \ldots, a_k, \langle a_{k+1}, b\rangle\rangle = \langle a_0, \ldots, a_k, a_{k+1}, b\rangle$ na mocy (11.3). □

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:

$$p_0 = x_0, \quad p_1 = x_0x_1 + 1, \quad q_0 = 1, \quad q_1 = x_1 \quad (11.5)$$

$$\begin{cases} p_{n+1} = p_n x_{n+1} + p_{n-1} & \text{dla } n = 1, 2, \ldots \\ q_{n+1} = q_n x_{n+1} + q_{n-1} & \text{dla } n = 1, 2, \ldots \end{cases} \quad (11.6)$$

Stwierdzenie 11.4. *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 (11.6), 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 11.5. *Dla każdego naturalnego n zachodzi wzór:*

$$p_{n-1} \cdot q_n - q_{n-1} \cdot p_n = (-1)^n. \tag{11.7}$$

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 (11.7) zachodzi dla pewnego naturalnego n. Wtedy z (11.6),

$$p_n \cdot q_{n+1} - q_n \cdot p_{n+1} =$$

$$= p_n \cdot (q_n x_{n+1} + q_{n-1}) - q_n \cdot (p_n x_{n+1} + p_{n-1}) =$$

$$= p_n q_n x_{n+1} + p_n q_{n-1} - q_n p_n x_{n+1} - q_n p_{n-1} = -(p_{n-1} \cdot q_n - q_{n-1} \cdot p_n) =$$

$$= (-1) \cdot (-1)^n = (-1)^{n+1},$$

czyli wtedy wzór (11.7) zachodzi dla liczby $n + 1$. Zatem na mocy zasady indukcji matematycznej mamy tezę. □

Twierdzenie 11.6. *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*

$$\langle a_0, a_1, \ldots, a_n \rangle = \frac{p_n(a_0, a_1, \ldots, a_n)}{q_n(a_0, a_1, \ldots, a_n)}. \tag{11.8}$$

Dowód. Zastosujemy indukcję względem $n \in \mathbb{N}_0$. Ponieważ $\frac{p_0(a_0)}{q_0(a_0)} = \frac{a_0}{1} = a_0 = \langle a_0 \rangle$ oraz $\frac{p_1(a_0,a_1)}{q_1(a_0,a_1)} = \frac{a_0 a_1 + 1}{a_1} = a_0 + \frac{1}{a_1} = \langle a_0, a_1 \rangle$, więc

wzór (11.8) zachodzi dla $n = 0$ i dla $n = 1$. Niech teraz wzór (11.8) zachodzi dla pewnej liczby naturalnej n 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 (11.3),

$$\langle a_0, a_1, \ldots, a_n, a_{n+1}\rangle = \left\langle a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right\rangle.$$

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 (11.6),

$$p_n\left(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right) =$$

$$= p_{n-1}(a_0, \ldots, a_{n-1})\left(a_n + \frac{1}{a_{n+1}}\right) + p_{n-2}(a_0, \ldots, a_{n-2}),$$

więc na mocy (11.6),

$$p_n\left(a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right) =$$

$$= p_{n-1}(a_0, \ldots, a_{n-1})a_n + p_{n-2}(a_0, \ldots, a_{n-2}) +$$

$$+ \frac{1}{a_{n+1}} p_{n-1}(a_0, \ldots, a_{n-1}) =$$

$$= p_n(a_0, \ldots, a_n) + \frac{1}{a_{n+1}} p_{n-1}(a_0, \ldots, a_{n-1}) =$$

$$= \frac{1}{a_{n+1}}\left(p_n(a_0, \ldots, a_n)a_{n+1} + p_{n-1}(a_0, \ldots, a_{n-1})\right) =$$

$$= \frac{1}{a_{n+1}} p_{n+1}\left(a_0, \ldots, a_n, a_{n+1}\right).$$

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 (11.8) zachodzi dla liczby $n+1$. Kończy to więc nasz dowód. □

Twierdzenie 11.7. *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 (11.5), a z (11.6) wynika od razu (ii). Z (11.7) uzyskujemy podpunkt (iii). Natomiast (iv) jest konsekwencją twierdzenia 11.6. (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 $k \in \mathbb{N}_0$: $\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{P_k Q_{k+1} - Q_k P_{k+1}}{Q_k Q_{k+1}} = \frac{(-1)^{k+1}}{Q_k Q_{k+1}}$. 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), $R_k - R_{k+2} = \frac{(-1)^{k+1}}{Q_k Q_{k+1}} + \frac{(-1)^{k+2}}{Q_{k+1} Q_{k+2}}$. Zatem $R_k - R_{k+2} = (-1)^{k+1} \cdot \frac{Q_{k+2} - Q_k}{Q_k Q_{k+1} Q_{k+2}}$. 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 $\lim\limits_{n \to \infty} R_n = \alpha$. $\square$

11.2 Skończone ułamki łańcuchowe

Definicja 11.8. 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 $n > 0$.

Przykład 11.9. 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 11.7 i ze stwierdzenia 11.4 otrzymujemy od razu następujące

Twierdzenie 11.10. *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) $P_0 = a_0$, $P_1 = a_0a_1 + 1$, $Q_0 = 1$ oraz $Q_1 = a_1$,

(iii) $P_{k+1} = P_ka_{k+1} + P_{k-1}$ i $Q_{k+1} = Q_ka_{k+1} + Q_{k-1}$ 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 11.11. Zastosujemy twierdzenie 11.10 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 11.2 uzyskujemy od razu następujący

Lemat 11.12. *Część całkowita dodolnego skończonego ułamka łańcuchowego* $\langle a_0, \ldots, a_n\rangle$ *jest równa* a_0. □

Twierdzenie 11.13. *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 11.12, $a_0 = b_0$. 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 11.12, $a_0 = b_0$. Ponieważ $n > 0$, więc z pierwszej części dowodu $m > 0$. Stąd na mocy (11.1), $a_0 + \frac{1}{\langle a_1, \ldots, a_{n+1}\rangle} = a_0 + \frac{1}{\langle b_1, \ldots, b_m\rangle}$. 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 11.14. *Każda liczba wymierna jest równa dokładnie jednemu skończonemu ułamkowi łańcuchowemu. Dokładniej, jeśli* $a \in \mathbb{Z}$ *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 11.13. 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 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 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 (11.1), $\frac{a}{b} = \langle q_0, q_1, \ldots, q_n, q_{n+1} \rangle$. □

Wniosek 11.15. *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 11.14 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 (11.3), $q = \langle c_0, c_1, \ldots, c_p - 1, 1 \rangle$. Ponadto, $p \in \mathbb{N}$, więc p i $p + 1$ jako kolejne liczby naturalne są różnej parzystości, co kończy dowód. □

Przykład 11.16. Zapiszemy $\frac{41}{18}$ w postaci skończonego ułamka łańcuchowego. W tym celu wyznaczamy najpierw kolejne dzielenia z resztą w algorytmie Euklidesa obliczania NWD$(41, 18)$:

$$\begin{aligned} 41 &= 2 \cdot 18 + 5 \\ 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned} \quad . \tag{11.9}$$

Zatem na mocy twierdzenia 11.14, $\frac{41}{18} = \langle 2, 3, 1, 1, 2 \rangle$. Ponadto mamy, że $18 = 0 \cdot 41 + 18$, więc stąd $\frac{18}{41} = \langle 0, 2, 3, 1, 1, 2 \rangle$.

Zauważmy, że twierdzenie 11.10 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 11.17. Twierdzenie 11.10 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$(84281, 86147)$:

$$\begin{aligned} 84281 &= 0 \cdot 86147 + 84281 \\ 86147 &= 1 \cdot 84281 + 1866 \\ 84281 &= 45 \cdot 1866 + 311 \\ 1866 &= 6 \cdot 311 \end{aligned} \quad . \tag{11.10}$$

Zatem na mocy twierdzenia 11.14, $\frac{84281}{86147} = \langle 0, 1, 45, 6 \rangle$. Budujemy tabelkę:

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 11.14 ułamek $\frac{271}{277}$ jest nieskracalny.

11.3 Nieskończone ułamki łańcuchowe

Z twierdzenia 11.7 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 11.18. Niech $(a_n)_{n=0}^{\infty}$ będzie ciągiem liczb całkowitych takim, że $a_k \geqslant 1$ dla wszystkich $k \in \mathbb{N}$. Granicę ciagu

$$(\langle a_0, a_1, \ldots, a_n\rangle)_{n=0}^{\infty}$$

nazywamy **nieskończonym ułamkiem łańcuchowym** i oznaczamy symbolem $\langle a_0, a_1, a_2, \ldots\rangle$.

Z twierdzenia 11.7 i ze stwierdzenia 11.4 otrzymujemy od razu następujące

Twierdzenie 11.19. *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) $P_{k+1} = P_ka_{k+1} + P_{k-1}$ i $Q_{k+1} = Q_ka_{k+1} + Q_{k-1}$ 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 11.20. *Niech $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$ będzie dowolnym nieskończonym ułamkiem łańcuchowym. Wtedy przy oznaczeniach twierdzenia 11.19:*

(i) $\lfloor\alpha\rfloor = a_0$,

(ii) $|\alpha - R_n| < \frac{1}{Q_nQ_{n+1}}$ dla każdego $n \in \mathbb{N}$,

(iii) α jest liczbą niewymierną.

Dowód. Na mocy twierdzenia 11.19, $a_0 = R_0 < \alpha < R_1 = a_0 + \frac{1}{a_1} \leqslant$ $\leqslant a_0 + 1$, 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

$$|\alpha - R_n| < |R_n - R_{n+1}| = \frac{1}{Q_nQ_{n+1}}.$$

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 11.19 (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 11.19 (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 11.19. Wobec tego liczba α jest niewymierna. □

Z twierdzeń 11.10 i 11.20 uzyskujemy od razu następujący

Wniosek 11.21. *Żaden nieskończony ułamek łańcuchowy nie jest równy żadnemu skończonemu ułamkowi łańcuchowemu.*

Stwierdzenie 11.22. *Dla każdego nieskończonego ułamka łańcuchowego $\langle a_0, a_1, a_2, \ldots\rangle$ i dla dowolnego $n \in \mathbb{N}_0$ zachodzi wzór:*

$$\langle a_0, a_1, a_2, \ldots\rangle = \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, a_{n+2}, \ldots\rangle\rangle. \tag{11.11}$$

Dowód. Weźmy dowolne $m \in \mathbb{N}$. Wtedy na mocy wzoru (11.2),

$$\langle a_0, a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+m}\rangle = \langle a_0, a_1, \ldots, a_n, \langle a_{n+1}, \ldots, a_{n+m}\rangle\rangle.$$

Z twierdzenia 11.19 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 11.3 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 11.23. *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 łańcucowe $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$ i $\beta = \langle b_0, b_1, b_2, \ldots\rangle$ są równe. Wtedy $\lfloor\alpha\rfloor = \lfloor\beta\rfloor$, więc z twierdzenia 11.20 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 11.22 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 11.20 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 11.7 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 11.7, $(-1)^i\delta = (-1)^i\gamma$, 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 $i \in \mathbb{N}_0$. □

11.4 Rozwijanie liczby niewymiernej na ułamek łańcuchowy

Niech x będzie dowolną rzeczywistą liczbą niewymierną. Wtedy $\lfloor x\rfloor \leqslant x < \lfloor x\rfloor + 1$ 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 (11.2), $x = \langle\lfloor x\rfloor, \lfloor x_1\rfloor, x_2\rangle$, 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:

$$x_k > 1 \ \text{ i } \ x_{k+1} = \frac{1}{x_k - \lfloor x_k \rfloor} \quad \text{dla każdego } \ k \in \mathbb{N}, \tag{11.12}$$

przy czym na mocy (11.2) i prostej indukcji:

$$x = \langle \lfloor x \rfloor, \lfloor x_1 \rfloor, \ldots, \lfloor x_n \rfloor, x_{n+1} \rangle \quad \text{dla każdego } \ n \in \mathbb{N}_0. \tag{11.13}$$

W szczególności

$$a_0 = \lfloor x \rfloor \in \mathbb{Z} \quad \text{oraz } \ a_n = \lfloor x_n \rfloor \in \mathbb{N} \ \text{ dla każdego } \ n \in \mathbb{N}. \tag{11.14}$$

Udowodnimy, że

$$x = \langle a_0, a_1, a_2, \ldots \rangle. \tag{11.15}$$

Niech $n \in \mathbb{N}$. Wtedy z (11.13) i (11.14) mamy, że $x = \langle a_0, \ldots, a_n, x_{n+1} \rangle$. Zatem na mocy twierdzenia 11.7 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 11.7 (*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 11.7. 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 11.23 wynika od razu następujące

Twierdzenie 11.24. *Każda rzeczywista liczba niewymierna jest dokładnie jednym nieskończonym ułamkiem łańcuchowym.*

Następujące stwierdzenie ułatwia obliczanie części całkowitej liczby rzeczywistej.

Stwierdzenie 11.25. *Dla dowolnych $k \in \mathbb{Z}$, $n \in \mathbb{N}$ i $x \in \mathbb{R}$:*
(i) $\lfloor x+k \rfloor = \lfloor x \rfloor + k$,
(ii) $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$.

Dowód. (i). Ponieważ $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$, więc $\lfloor x \rfloor + k \leqslant x + k < \lfloor x \rfloor + k + 1$. Ponadto $\lfloor x \rfloor, k \in \mathbb{Z}$, więc $\lfloor x \rfloor + k \in \mathbb{Z}$. Zatem z definicji części całkowitej, $\lfloor x+k \rfloor = \lfloor x \rfloor + k$.

(ii). Z twierdzenia o dzieleniu z resztą mamy, że $\lfloor x \rfloor = qn + r$ dla pewnych $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, n-1\}$. Ponadto z definicji części całkowitej $x = \lfloor x \rfloor + s$ dla pewnego $s \in \mathbb{R}$ takiego, że $0 \leqslant s < 1$. Stąd $q \leqslant \frac{\lfloor x \rfloor}{n} = q + \frac{r}{n} < q + \frac{n}{n} = q + 1$, czyli $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = q$. Ponadto

$$q \leqslant \frac{x}{n} = \frac{qn + r + s}{n} = q + \frac{r+s}{n} < q + \frac{(n-1)+1}{n} = q + 1,$$

więc $\left\lfloor \frac{x}{n} \right\rfloor = q$. Zatem $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$. □

Przykład 11.26. 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 11.25, $a_1 = \lfloor x_1 \rfloor = \left\lfloor \frac{4+4}{5} \right\rfloor = 1$. 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 11.25, $a_2 = \left\lfloor \frac{4+1}{4} \right\rfloor = 1$. 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 11.25, $a_3 = \left\lfloor \frac{4+3}{3} \right\rfloor = 2$. 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 11.25, $a_4 = \left\lfloor \frac{4+3}{4} \right\rfloor = 1$. 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 11.25, $a_5 = \left\lfloor \frac{4+1}{5} \right\rfloor = 1$. 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 11.25, $a_6 = 4+4 = 8$. 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 11.27. *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 11.14 wynika, że α jest skończonym ułamkiem łańcuchowym, czyli $\alpha = \langle a_0, a_1, \ldots, a_m \rangle$. Na mocy twierdzenia 11.10 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 11.15 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

$$\frac{a}{b} = \langle c_0, c_1, \ldots, c_m \rangle \text{ oraz } (-1)^m = \operatorname{sgn}\left(\alpha - \frac{a}{b}\right). \tag{11.16}$$

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 (11.16) 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

$$0 < (-1)^m(\alpha Q_m' - P_m') < \frac{1}{2Q_m'}. \tag{11.17}$$

Niech

$$\omega = \frac{P'_{m-1} - \alpha Q'_{m-1}}{\alpha Q'_m - P'_m}. \tag{11.18}$$

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

$$\alpha = \frac{\omega P'_m + P'_{m-1}}{\omega Q'_m + Q'_{m-1}}. \tag{11.19}$$

Z (11.18) i (11.17) 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 11.7, więc $\omega > 1$, skąd $\lfloor \omega \rfloor > 1$. Zatem na mocy twierdzenia 11.6 i wzoru (11.19) 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 (11.18), $\omega \in \mathbb{Q}$ i na mocy twierdzenia 11.14 i lematu 11.12, $\omega = \langle c_{m+1}, c_{m+2}, \ldots, c_{m+n} \rangle$ dla pewnych liczb naturalnych $n, c_{m+1}, c_{m+2}, \ldots, c_{m+n}$, przy czym $c_{m+n} > 1$. Stąd i z (11.2) uzyskujemy, że $\alpha = \langle c_0, c_1, \ldots, c_m, c_{m+1}, \ldots, c_{m+n} \rangle$, więc na mocy twierdzenia 11.14, $P'_i = P_i$ 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 (11.19), $\omega \notin \mathbb{Q}$ i z twierdzeń 11.24 i 11.20 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 (11.11) uzyskujemy, że $\alpha = \langle c_0, c_1, \ldots, c_m, c_{m+1}, c_{m+2}, \ldots \rangle$. Zatem na mocy twierdzenia 11.19 otrzymujemy, że $P'_i = P_i$ oraz $Q'_i = Q_i$ dla $i = 0, 1, \ldots, m$, czyli $a = P_m$ i $b = Q_m$. □

Zadanie 11.28. Przedstaw w postaci ułamka łańcuchowego następujące liczby rzeczywiste:

(a) $\frac{1+\sqrt{5}}{2}$, (b) $\frac{1+\sqrt{5}}{3}$, (c) $\frac{2+\sqrt{5}}{4}$.

Zadanie 11.29. Niech ciągi $(P_n)_{n=0}^{\infty}$ i $(Q_n)_{n=0}^{\infty}$ będą wyznaczone przez rozwinięcie liczby niewymiernej α na ułamek łańcuchowy. Udowodnij, 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 $n \in \mathbb{N}$. Wyprowadź stąd, że $|\alpha - \frac{P_n}{Q_n}| < \frac{1}{2Q_n^2}$ dla nieskończenie wielu $n \in \mathbb{N}$.

Zadanie 11.30. 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. Udowodnij, że jeżeli $x, y \in \mathbb{N}$ i $x^2 - Dy^2 = \pm 2$, to $x = P_m$ i $y = Q_m$ dla pewnego $m \in \mathbb{N}_0$.

Rozdział 12

Niewymierności kwadratowe

12.1 Określenie niewymierności kwadratowych

Niech D będzie liczbą naturalną, która nie jest kwadratem liczby naturalnej. Wówczas dodatnia liczba rzeczywista $\sqrt{D}$ jest niewymierna na mocy wniosku 1.31. 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:

$$a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D} \iff [a_1 = a_2 \text{ i } b_1 = b_2]. \tag{12.1}$$

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:

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}. \tag{12.2}$$

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 (12.1) 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:

$$a + b\sqrt{D} \mapsto \overline{a + b\sqrt{D}} = a - b\sqrt{D} \tag{12.3}$$

i nazywanej przez nas **sprzęganiem** w ciele $\mathbb{Q}(\sqrt{D})$. Własności tej funkcji grupuje następujące stwierdzenie.

Stwierdzenie 12.1. *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 (12.1), $b_1 = -b_1$, 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 (12.1) i (12.3).

(iv). Ze wzoru (12.3), $\overline{(\overline{\alpha})} = \overline{a_1 - b_1\sqrt{D}} = a_1 - (-b_1)\sqrt{D} = \alpha$.

(v). Ze wzoru (12.3) 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 12.1 można wyprowadzić następujący

Wniosek 12.2. *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 12.3. Niewymiernością kwadratową nazywamy każdą liczbę niewymierną należącą do ciała postaci $\mathbb{Q}(\sqrt{D})$, gdzie D jest liczbą naturalną nie będącą kwadratem liczby 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 12.4. *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 12.5. *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 12.2 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 12.6. *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 (12.1), $b+y = 0$, 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 (12.1), $(x-a)b = 0$. 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 (11.13) mamy, że dla każdego $k \in \mathbb{N}$:

$$\alpha = \langle a_0, a_1, \ldots, a_{k-1}, \alpha_k \rangle. \tag{12.4}$$

Na mocy stwierdzenia 12.5 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

$$A_1 = f(a_0),\ B_1 = 2a_0A + B,\ C_1 = A, \tag{12.5}$$

przy czym $B_1^2 - 4A_1C_1 = B^2 - 4AC$. Udowodnimy, że przy tych oznaczeniach zachodzi też następujący

Lemat 12.7. *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 11.19;
$n_4 = (P_kQ_{k-1} + Q_kP_{k-1})^2 - 4P_kQ_kP_{k-1}Q_{k-1} = (P_{k-1}Q_k - Q_{k-1}P_k)^2 =$
$= ((-1)^k)^2 = 1$, na mocy twierdzenia 11.19 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 (12.4) i (11.8), $\alpha = \frac{P_k\alpha_{k+1}+P_{k-1}}{Q_k\alpha_{k+1}+Q_{k-1}}$, 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 $A_k\alpha_{k+1}^2 + B_k\alpha_{k+1} + C_k = 0$. □

12.2 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, tzn. 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:

$$\langle a_0, a_1, a_2, \ldots\rangle = \langle a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+k-1}}\rangle. \tag{12.6}$$

Z twierdzenia 11.23 otrzymujemy od razu następujące

Stwierdzenie 12.8. *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 12.9. *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 11.23 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 12.8 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 12.8, 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 12.10. Dla $a \in \mathbb{N}$ obliczymy wartość ułamka łańcuchowego $\alpha = \langle \overline{a}\rangle = \langle a, a, a, \ldots\rangle$. Ze stwierdzenia 11.22 mamy, że $\alpha = \langle a, \alpha\rangle$, natomiast z twierdzenia 11.20 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:

$$\langle a, a, a, \ldots\rangle = \frac{a + \sqrt{a^2+4}}{2}, \tag{12.7}$$

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 12.11. Dla $a,b\in\mathbb{N}$ obliczymy wartość ułamka łańcuchowego $\alpha=\langle\overline{a,b}\rangle$. Ze stwierdzenia 11.22 mamy, że $\alpha=\langle a,b,\alpha\rangle$, natomiast z twierdzenia 11.20 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:

$$\langle a,b,a,b,a,b,\ldots\rangle=\frac{ab+\sqrt{a^2b^2+4ab}}{2b},\tag{12.8}$$

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 12.12. Uogólnijmy przykład 12.11 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 11.20 liczba α jest niewymierna i $\lfloor\alpha\rfloor=a_0\in\mathbb{N}$, skąd wynika, że $\alpha>1$. Ze stwierdzenia 11.22 mamy, że $\alpha=\langle a_0,a_1,\ldots,a_k,\alpha\rangle$. Zatem na mocy wzoru (11.8), $\alpha=\frac{P_k\alpha+P_{k-1}}{Q_k\alpha+Q_{k-1}}$. Stąd $Q_k\alpha^2+(Q_{k-1}-P_k)\alpha-P_{k-1}=0$ i na mocy stwierdzenia 12.5, 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:

$$\langle \overline{a_0, a_1, \ldots, a_k} \rangle = \frac{P_k - Q_{k-1} + \sqrt{(Q_{k-1} - P_k)^2 + 4Q_kP_{k-1}}}{2Q_k}, \quad (12.9)$$

z którego wynika, że $\alpha = \langle \overline{a_0, a_1, \ldots, a_k} \rangle$ jest niewymiernością kwadratową. Ponadto, jak pokazaliśmy, $\alpha > 1$ oraz

$$\overline{\alpha} = \frac{P_k - Q_{k-1} - \sqrt{(Q_{k-1} - P_k)^2 + 4Q_kP_{k-1}}}{2Q_k} < 0.$$

Ze stwierdzenia 12.1 wynika, że α i $\overline{\alpha}$ są pierwiastkami trójmianu kwadratowego $f(x) = Q_kx^2 + (Q_{k-1} - P_k)x - P_{k-1}$. Dodatkowo $f(0) = -P_{k-1} < 0$ i $f(-1) = (Q_k - Q_{k-1}) + (P_k - P_{k-1}) > 0$, bo z twierdzenia 11.19 wynika, że $Q_k - Q_{k-1} \geqslant 0$ oraz $P_1 = a_0a_1 + 1 > a_0 = P_0$ 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 12.13. (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 12.10 i 12.12, 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 11.19 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 11.19 liczba α jest niewymierna. Zatem α jest niewymiernością kwadratową.

$\Leftarrow$. Ze stwierdzenia 12.5 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 12.1 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 11.19, więc istnieje $n_0 \in \mathbb{N}$ 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 11.19 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 12.7, 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 11.19 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 12.8 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 12.14. (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 12.10 i 12.12.

$\Leftarrow$. Niech α będzie niewymiernością kwadratową taką, że $\alpha > 1$ i $-1 < \overline{\alpha} < 0$. Z twierdzenia 12.13 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 11.20, $a_0 = \lfloor\alpha\rfloor \geqslant 1$, 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

$$\alpha_n > 1 \quad \text{dla każdego} \quad n \in \mathbb{N}_0. \tag{12.10}$$

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 12.1, $\overline{\alpha_n} = a_n + \frac{1}{\overline{\alpha_{n+1}}}$, 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

$$-1 < \overline{\alpha_n} < 0 \quad \text{dla każdego} \quad n \in \mathbb{N}_0. \tag{12.11}$$

Ponieważ $\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$ dla $n \in \mathbb{N}$, więc ze stwierdzenia 12.1 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 (12.11),

$$-\frac{1}{\overline{\alpha_n}} = a_{n-1} - \overline{\alpha_{n-1}} \quad \text{oraz} \quad \left\lfloor -\frac{1}{\overline{\alpha_n}} \right\rfloor = a_{n-1} \quad \text{dla} \quad n \in \mathbb{N}. \tag{12.12}$$

Załóżmy, że $s \geqslant 1$. Wtedy z (12.12) 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 12.8, że $\alpha = \langle \overline{a_0, a_1, \ldots, a_{r-1}} \rangle$.

Dalej, $\alpha_0 = \alpha_r$, więc z (12.12), $\frac{1}{-\overline{\alpha_0}} = a_{r-1} - \overline{\alpha_{r-1}}$, 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 (12.12), $-\overline{\alpha_{r-k}} = a_{r-(k+1)} - \overline{\alpha_{r-(k+1)}} = \left\langle a_{r-(k+1)}, \frac{1}{-\overline{\alpha_{r-(k+1)}}} \right\rangle$. Stąd na mocy stwierdzenia 11.22,

$$\frac{1}{-\overline{\alpha_0}} = \left\langle a_{r-1}, a_{r-2}, \ldots, a_{r-k}, a_{r-(k+1)}, \frac{1}{-\overline{\alpha_{r-(k+1)}}} \right\rangle.$$

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 12.15. *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. □

Zadanie 12.16. Dla jakich $x, y \in \mathbb{Z}$ liczba $x + y\sqrt{5}$ ma czysto okresowe rozwinięcie na nieskończony ułamek łańcuchowy?

Zadanie 12.17. Wyznacz wszystkie $a, b \in \mathbb{N}$ takie, że $\frac{a+\sqrt{5}}{b}$ ma czysto okresowe rozwinięcie na nieskończony ułamek łańcuchowy.

12.3 Rozwijanie $\sqrt{D}$ na ułamek łańcuchowy

Twierdzenie 12.18. *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 12.14 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 11.20, $a_0 + \sqrt{D} = \langle\overline{2a_0, a_1, \ldots, a_{k-1}}\rangle$ 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 11.23,

$$(a_1, a_2, \ldots, a_{k-1}) = (a_{k-1}, \ldots, a_2, a_1),$$

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 12.7, 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 12.9, α_{n+1} ma rozwinięcie czysto okresowe na ułamek łańcuchowy, więc na mocy stwierdzenia 12.15 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 11.19 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 $n \in \mathbb{N}$:

$$\alpha_n = \frac{b_n + \sqrt{D}}{c_n}, \quad \text{gdzie } b_n, c_n \in \mathbb{N}, \tag{12.13}$$

przy czym

$$P_{n-1}^2 - DQ_{n-1}^2 = c_n \quad \text{dla parzystych } n \in \mathbb{N} \tag{12.14}$$

oraz

$$P_{n-1}^2 - DQ_{n-1}^2 = -c_n \quad \text{dla nieparzystych } n \in \mathbb{N}. \tag{12.15}$$

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 11.25, 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 12.9, $n = km$ 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 (12.13) mamy, że, $c_{kn} = 1$. Jeśli liczba kn jest parzysta, to z (12.14), $P_{kn-1}^2 - DQ_{kn-1}^2 = 1$, a jeśli liczba kn jest nieparzysta, to z (12.15), $P_{kn-1}^2 - DQ_{kn-1}^2 = -1$. Wobec tego $P_{kn-1}^2 - DQ_{kn-1}^2 = (-1)^{kn}$.

Dowód naszego twierdzenia jest zatem zakończony. □

Z dowodu twierdzenia 12.18 i ze stwierdzenia 11.25 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 11.25, $a_1 = \lfloor \alpha_1 \rfloor = \left\lfloor \frac{b_1 + a_0}{c_1} \right\rfloor$. Ponadto dla $i \in \mathbb{N}$ ze wzoru (12.13) 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 11.25, $a_{i+1} = \left\lfloor \frac{b_{i+1}+a_0}{c_{i+1}} \right\rfloor$.

Przykład 12.19. 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:

$$\sqrt{61} = \langle 7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14} \rangle.$$

Zadanie 12.20. Stosując algorytm podany w tym rozdziale wyznacz rozwinięcie liczby $\sqrt{71}$ na ułamek łańcuchowy.

Zadanie 12.21. Dla jakich liczb naturalnych k istnieją $a, D \in \mathbb{N}$ takie, że $\sqrt{D} = \langle a, \overline{\underbrace{1, \ldots, 1}_{k-1}, 2a} \rangle$?

Zadanie 12.22. Udowodnij, że dla każdej liczby naturalnej k istnieją $a, D \in \mathbb{N}$ takie, że $a \geqslant 3$ i $\sqrt{D} = \langle a, \overline{\underbrace{2, \ldots, 2}_{k-1}, 2a} \rangle$.

12.4 Zastosowania do równań $x^2 - Dy^2 = C$

Lemat 12.23. *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 11.27, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}_0$. □

Twierdzenie 12.24. *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 12.18 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 12.18, $P_{km-1}^2 - DQ_{km-1}^2 = 1$ 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 12.23, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}$. Stąd $P_n^2 - DQ_n^2 = 1$, więc na mocy (12.14) i (12.15), $c_{n+1} = 1$ i $n + 1$ jest parzyste, ale z dowodu twierdzenia 12.18, $k \mid n + 1$, 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 12.18 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 12.23, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}$. Stąd $P_n^2 - DQ_n^2 = 1$, więc na mocy (12.14) i (12.15), $c_{n+1} = 1$ i $n + 1$ jest parzyste, ale z dowodu twierdzenia 12.18, $k \mid n + 1$, 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 12.25. *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 12.18 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 12.23, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}$. Stąd $P_n^2 - DQ_n^2 = -1$, więc na mocy (12.14) i (12.15), $c_{n+1} = 1$ i $n+1$ jest nieparzyste. Ponadto z dowodu twierdzenia 12.18, $k \mid n+1$, 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 12.18, $P_{k(2m-1)-1}^2 - DQ_{k(2m-1)-1}^2 = -1$. 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 7.16 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 12.24, $P_{2k-1} = P_{k-1}^2 + DQ_{k-1}^2$ i $Q_{2k-1} = 2P_{k-1}Q_{k-1}$. □

Przykład 12.26. Zilustrujmy twierdzenia 12.24 i 12.25 dla liczby $D = 61$. Z przykładu 12.19 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 12.24, 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 12.24. Mianowicie z twierdzenia 7.9 uzyskujemy, że $x_{n+1} = 1766319049x_n + 61 \cdot 226153980y_n$ oraz $y_{n+1} = 226153980x_n + {}$ $+1766319049y_n$ dla $n \in \mathbb{N}_0$.

Przykład 12.27. Uzasadnimy, że dla naturalnych $k \geqslant 3$ równanie $x^2 - (k^2 - 4)y^2 = -1$ posiada rozwiązanie w liczbach naturalnych x i y wtedy i tylko wtedy, gdy $k = 3$. Dla $k = 3$ równanie to przybiera postać: $x^2 - 5y^2 = -1$ i oczywiście posiada rozwiązanie w liczbach naturalnych: $(2, 1)$.

Niech dalej $k > 3$ i przypuśćmy, że istnieją $x, y \in \mathbb{N}$ takie, że $x^2 - {}$ $+(k^2-4)y^2 = -1$. Jeśli k jest parzyste, to $(k^2-4)y^2 \equiv 0 \pmod 4$, więc $x^2 \equiv 3 \pmod 4$, co prowadzi do sprzeczności, gdyż $x^2 \equiv 0 \pmod 4$

lub $x^2 \equiv 1 \pmod 4$ dla każdego $x \in \mathbb{Z}$. Wobec tego k jest nieparzyste i $k > 3$. Zatem $k = 2s+3$ dla pewnego $s \in \mathbb{N}$. Przedstawimy teraz $\sqrt{D}$ dla $D = (2s+3)^2 - 4 = 4s^2 + 12s + 5$ w postaci ułamka łańcuchowego stosując algorytm podany wyżej. Ponieważ $(2s+2)^2 < D < (2s+3)^2$, więc $a_0 = 2s+2$. Wobec tego:

(0) $b_0 = 0$, $c_0 = 1$ i $a_0 = 2s+2$.

Stosując (II) do $i = 0$ uzyskujemy, że $b_1 = (2s+2)\cdot 1 - 0 = 2s+2$, $c_1 = \frac{4s^2+12s+5-4s^2-8s-4}{1} = 4s+1$, $a_1 = \lfloor \frac{2s+2+2s+2}{4s+1} \rfloor = \lfloor \frac{4s+4}{4s+1} \rfloor = 1$, czyli:

(1) $b_1 = 2s+2$, $c_1 = 4s+12$ i $a_1 = 1$.

Podobnie dalej, $b_2 = 1\cdot(4s+1) - (2s+2) = 2s-1$, $c_2 = \frac{4s^2+12s+5-4s^2+4s-1}{4s+1} = \frac{16s+4}{4s+1} = 4$, $a_2 = \lfloor \frac{2s-1+2s+2}{4} \rfloor = \lfloor \frac{4s+1}{4} \rfloor = s$, czyli:

(2) $b_2 = 2s-1$, $c_2 = 4$ i $a_2 = s$.

Dalej, $b_3 = s\cdot 4 - (2s-1) = 2s+1$, $c_3 = \frac{4s^2+12s+5-4s^2-4s-1}{4} = \frac{8s+4}{4} = 2s+1$, $a_3 = \lfloor \frac{2s+1+2s+2}{2s+1} \rfloor = \lfloor \frac{4s+3}{2s+1} \rfloor = 2$, czyli:

(3) $b_3 = 2s+1$, $c_3 = 2s+1$ i $a_3 = 2$.

Dalej, $b_4 = 2\cdot(2s+1) - (2s+1) = 2s+1$, $c_4 = \frac{4s^2+12s+5-4s^2-4s-1}{2s+1} = \frac{8s+4}{2s+1} = 4$ i $a_4 = \lfloor \frac{2s+1+2s+2}{4} \rfloor = \lfloor \frac{4s+3}{4} \rfloor = s$, czyli:

(4) $b_4 = 2s+1$, $c_4 = 4$ i $a_4 = s$.

Dalej, $b_5 = s\cdot 4 - (2s+1) = 2s-1$, $c_5 = \frac{4s^2+12s+5-4s^2+4s-1}{4} = \frac{16s+4}{4} = 4s+1$ i $a_5 = \lfloor \frac{2s-1+2s+2}{4s+1} \rfloor = 1$, czyli:

(5) $b_5 = 2s-1$, $c_5 = 4s+1$ i $a_5 = 1$.

Dalej, $b_6 = 1\cdot(4s+1) - (2s-1) = 2s+2$, $c_6 = \frac{4s^2+12s+5-4s^2-8s-4}{4s+1} = \frac{4s+1}{4s+1} = 1$, $a_6 = \lfloor \frac{2s+2+2s+2}{1} \rfloor = 4s+4$, czyli:

(6) $b_6 = 2s+2$, $c_6 = 1$, $a_6 = 4s+4 = 2a_0$.

Wobec tego:

$$\sqrt{4s^2+12s+5} = \langle 2s+2, \overline{1, s, 2, s, 1, 4s+4}\rangle.$$

Stąd długość najkrótszego okresu przedstawienia liczby $\sqrt{k^2-4}$ w postaci ułamka łańcuchowego wynosi 6, a więc jest liczbą parzystą. Zatem na mocy twierdzenia 12.25 mamy sprzeczność.

Przykład 12.28. Pokażemy zastosowanie udowodnionych twierdzeń i zaprezentowanych metod do opisania wszystkich rozwiązań

w liczbach naturalnych równania

$$x^2 - 61y^2 = -3. \tag{12.16}$$

Załóżmy, że $x, y \in \mathbb{N}$ i $x^2 - 61y^2 = -3$. Wtedy $x^2 = 49y^2 + (12y^2 - 3) > 49y^2$, skąd $x > 7y$. Ponadto $3 = |x^2 - 61y^2| = (x + \sqrt{61}y)|x - y\sqrt{61}|$, więc $|\sqrt{61} - \frac{x}{y}| = \frac{1}{y}|x - \sqrt{61}y| = \frac{1}{y} \cdot \frac{3}{x+y\sqrt{61}}$. Dodatkowo $\sqrt{61} > 7$, więc $x + y\sqrt{61} > 7y + 7y = 14y$. Wobec tego $|\sqrt{61} - \frac{x}{y}| < \frac{1}{y} \cdot \frac{3}{14y} = \frac{3}{14y^2} < \frac{1}{2y^2}$, czyli $|\sqrt{61} - \frac{x}{y}| < \frac{1}{2y^2}$. Z (12.16) wynika, że $\mathrm{NWD}(x, y) \mid 3$. Stąd $\mathrm{NWD}(x, y) = 1$ lub $\mathrm{NWD}(x, y) = 3$. Jednak w drugim przypadku $3 \mid x$ i $3 \mid y$, skąd $9 \mid x^2 - 61y^2 = -3$, co prowadzi do sprzeczności. Zatem $\mathrm{NWD}(x, y) = 1$ i na mocy twierdzenia 11.27, $x = P_n$ i $y = Q_n$ dla pewnego $n \in \mathbb{N}_0$, gdzie ciągi $(P_n)_{n=0}^{\infty}$ i $(Q_n)_{n=0}^{\infty}$ są wyznaczone z rozkładu liczby $\sqrt{61}$ na ułamek łańcuchowy. Ponadto $P_0 = 7$ i $Q_0 = 1$, więc $n \in \mathbb{N}$. Ponieważ $P_n^2 - 61Q_n^2 = -3 < 0$, więc liczba n musi być parzysta i na mocy (12.14) i (12.15), $P_n^2 - 61Q_n^2 = -c_{n+1}$, czyli $c_{n+1} = 3$. Przy oznaczeniach dowodu twierdzenia 12.18 oraz z przykładu 12.19 oznacza to, że $\alpha_{n+1} = \alpha_2$ lub $\alpha_{n+1} = \alpha_9$. Z czystej okresowości ułamka łańcuchowego α_1 i tego, że najmniejszy okres ma długość 11 wynika, że $n+1 = 11m+2$ lub $n+1 = 11m+9$ dla pewnego $m \in \mathbb{N}_0$. Dalej, liczba $n+1$ jest nieparzysta, więc w pierwszym przypadku $n+1 = 11(2s+1)+2$ dla pewnego $s \in \mathbb{N}_0$, a w drugim, $n + 1 = 11 \cdot 2s + 9$ dla pewnego $s \in \mathbb{N}_0$. Zatem $n = 22s + 12$ lub $n = 22s + 8$ dla pewnego $s \in \mathbb{N}_0$. Stąd $x = P_{22s+12}$ i $y = Q_{22s+12}$ albo $x = P_{22s+8}$ i $y = Q_{22s+8}$ dla pewnego $s \in \mathbb{N}_0$.

Na odwrót, jeśli $x = P_{22s+12}$ i $y = Q_{22s+12}$ albo $x = P_{22s+8}$ i $y = Q_{22s+8}$ dla pewnego $s \in \mathbb{N}_0$, to $x, y \in \mathbb{N}$ oraz $x = P_{n+1}$ i $y = Q_{n+1}$, gdzie n jest parzyste i $n+1 = 11(2s+1)+2$ lub $n+1 = 11 \cdot 2s+9$. Zatem na mocy (12.14) i (12.15), $x^2 - Dy^2 = -c_{n+1}$. Ponadto wtedy $\alpha_{n+1} = \alpha_2$ lub $\alpha_{n+1} = \alpha_9$, więc z (12.13), $c_{n+1} = c_2 = 3$ lub $c_{n+1} = c_9 = 3$, czyli w obu przypadkach $x^2 - Dy^2 = -3$.

Uzyskaliśmy zatem, że wszystkimi rozwiązaniami w liczbach naturalnych równania (12.16) są $x = P_{22s+12}$ i $y = Q_{22s+12}$ oraz $x = P_{22s+8}$ i $y = Q_{22s+8}$ dla każdego $s \in \mathbb{N}_0$. Ponieważ $Q_1 < Q_2 < \ldots$, więc na mocy przykładu 12.26 minimalnym rozwiązaniem jest

para $(P_8, Q_8) = (5639, 722)$. Oczywiście następnym rozwiązaniem jest (P_{12}, Q_{12}), którego obliczenie pozostawimy Czytelnikowi.

Część IV

Elementy teorii pierścieni

Rozdział 13

Dziedziny całkowitości

13.1 Arytmetyka dziedzin całkowitości

Dziedziną całkowitości nazywamy taki podzbiór P pewnego ciała $(K, +, \cdot, 0, 1)$, że $1 \in P$ oraz $a - b, a \cdot b \in P$ dla dowolnych $a, b \in P$. Zauważmy, że wtedy $0 = 1 - 1 \in P$ oraz $-b = 0 - b \in P$ dla każdego $b \in P$. Ponadto dla $a, b \in P$: $a + b = a - (-b) \in P$, bo $-b \in P$. W języku algebraicznym oznacza to, że $(P, +, \cdot, 0, 1)$ jest przemiennym pierścieniem z jedynką i $0 \neq 1$ w P oraz $a \cdot b \neq 0$ dla dowolnych niezerowych $a, b \in P$. W takich pierścieniach P można uprawiać arytmetykę zbliżoną do arytmetyki liczb całkowitych. W dalszej części tej książki przez słowo pierścień będziemy rozumieli dziedzinę całkowitości. Czytelnika zainteresowanego teorią pierścieni odsyłamy do pozycji [8] oraz [4] i [5].

Niech P będzie dziedziną całkowitości. Mówimy, że element $a \in P$ jest **odwracalny** w P, jeżeli $a \cdot b = 1$ dla pewnego $b \in P$. Zauważmy, że element b jest wyznaczony jednoznacznie przez a, bo jeśli $c \in P$ i $a \cdot c = 1$, to $a \cdot b = a \cdot c$, skąd $b = c$, gdyż $a \neq 0$. Z tego powodu element b nazywamy **odwrotnym** do a i oznaczamy przez a^{-1}. Zatem $a \cdot a^{-1} = 1$, skąd $a^{-1} \cdot a = 1$, więc a^{-1} jest elementem odwracalnym w P oraz mamy wzór: $(a^{-1})^{-1} = a$. Zbiór wszystkich elementów odwracalnych pierścienia P będziemy oznaczali przez P^*. Ponieważ $1 \cdot 1 = 1$, więc $1 \in P^*$. Jeżeli $a, b \in P^*$, to $a \cdot x = 1$ i $b \cdot y = 1$ dla pewnych $x, y \in P$.

Stąd $(a\cdot b)\cdot(x\cdot y)=(a\cdot x)\cdot(b\cdot y)=1\cdot 1=1$, czyli $a\cdot b\in P^*$. W języku algebraicznym wypowiadamy to tak: $(P^*,\cdot,1)$ jest grupą abelową dla dowolnej dziedziny całkowitości $(P,+,\cdot,0,1)$.

Definicja 13.1. Niech P będzie dziedziną całkowitości i $a,b\in P$. Mówimy, że a **dzieli** b (w pierścieniu P) i piszemy $a\mid b$, jeżeli $b=a\cdot t$ dla pewnego $t\in P$. Jeżeli a nie dzieli b, to piszemy $a\nmid b$. Jeżeli $a\mid b$ i $b\mid a$, to mówimy, że elementy a i b są stowarzyszone i piszemy $a\sim b$.

Stwierdzenie 13.2. *Dla dowolnych elementów a,b,c dziedziny całkowitości P:*

(i) jeżeli $a\mid b$ i $b\mid c$, to $a\mid c$,

(ii) jeżeli $a\mid b$ i $a\mid c$, to $a\mid b\pm c$,

(iii) jeżeli $a\mid b$, to $a\cdot c\mid b\cdot c$,

(iv) jeżeli $c\neq 0$, to $a\cdot c\mid b\cdot c$ wtedy i tylko wtedy, gdy $a\mid b$,

(v) $a\sim b$ wtedy i tylko wtedy, gdy $b=u\cdot a$ dla pewnego $u\in P^*$.

Dowód. (i). Z założenia, $b=t\cdot a$ i $c=s\cdot b$ dla pewnych $t,s\in P$. Stąd $c=(s\cdot t)\cdot a$, więc $a\mid c$, bo $s\cdot t\in P$.

(ii). Z założenia $b=t\cdot a$ i $c=s\cdot a$ dla pewnych $s,t\in P$. Zatem $b\pm c=(t\pm s)\cdot a$, czyli $a\mid b\pm c$, bo $t\pm s\in P$.

(iii). Z założenia $b=t\cdot a$ dla pewnego $t\in P$. Stąd $b\cdot c=t\cdot(a\cdot c)$, czyli $a\cdot c\mid b\cdot c$.

(iv). Wobec (iii) wystarczy wykazać jedynie implikację $\Leftarrow$. W tym celu z założenia mamy, że $b\cdot c=t\cdot(a\cdot c)$ dla pewnego $t\in P$. Stąd $(b-t\cdot a)\cdot c=0$, a ponieważ P jest dziedziną całkowitości i $c\neq 0$, to $b-t\cdot a=0$, czyli $b=t\cdot a$ i $a\mid b$.

(v). Załóżmy, że $b=u\cdot a$ dla pewnego $u\in P^*$. Wtedy $a\mid b$ i $u\cdot v=1$ dla pewnego $v\in P$. Zatem $a=1\cdot a=u\cdot v\cdot a=v\cdot b$, skąd $b\mid a$ i wobec tego $a\sim b$. Na odwrót, załóżmy, że $a\sim b$. Wtedy $a\mid b$ i $b\mid a$. Zatem $b=t\cdot a$ i $a=s\cdot b$ dla pewnych $s,t\in P$. Jeśli $a=0$, to $b=t\cdot 0=0$ i $b=1\cdot a$, więc wystarczy przyjąć $u=1$. Jeżeli zaś $a\neq 0$, to $a=(s\cdot t)\cdot a$, skąd $a\cdot(1-s\cdot t)=0$. Ponieważ P jest dziedziną całkowitości i $a\neq 0$, więc $1-s\cdot t=0$, czyli $s\cdot t=1$ i wystarczy przyjąć $u=t$. □

Definicja 13.3. Niech P będzie dziedziną całkowitości i $a,b,c\in P$. Mówimy, że a **przystaje do** b **modulo** c (w pierścieniu P) i piszemy $a\equiv b\pmod c$, jeżeli $c\mid a-b$ w pierścieniu P.

Stwierdzenie 13.4. *Niech P będzie dziedziną całkowitości i $c \in P$. Wówczas dla dowolnych $x, y, z \in P$:*

(i) $x \equiv x \pmod{c}$,

(ii) jeżeli $x \equiv y \pmod{c}$, *to* $y \equiv x \pmod{c}$,

(iii) jeżeli $x \equiv y \pmod{c}$ *i* $y \equiv z \pmod{c}$, *to* $x \equiv z \pmod{c}$.

Dowód. Ponieważ $x - x = 0 = 0 \cdot c$, więc $x \equiv x \pmod{c}$. Niech $x \equiv y \pmod{c}$. Wtedy $c \mid x - y$, czyli $x - y = t \cdot c$ dla pewnego $t \in P$, skąd $y - x = (-t) \cdot c$, a zatem $c \mid y - x$ i $y \equiv x \pmod{c}$.

Załóżmy, że $x \equiv y \pmod{c}$ oraz $y \equiv z \pmod{c}$. Wtedy $c \mid x - y$ i $c \mid y - z$, więc ze stwierdzenia 13.2 otrzymujemy, że $c \mid (x-y)+(y-z)$, czyli $c \mid x - z$, skąd $x \equiv z \pmod{c}$. □

Stwierdzenie 13.5. *Niech P będzie dziedziną całkowitości, niech $n \in \mathbb{N}$ i niech $a, b, c, d, a_1, \ldots, a_n, b_1, \ldots, b_n \in P$. Wtedy:*

(i) jeżeli $a \equiv b \pmod{c}$, *to*

$$a \cdot d \equiv b \cdot d \pmod{c} \text{ oraz } a \cdot d \equiv b \cdot d \pmod{c \cdot d},$$

(ii) jeżeli $a \cdot d \equiv b \cdot d \pmod{c \cdot d}$ *i* $d \neq 0$, *to* $a \equiv b \pmod{c}$,

(iii) jeżeli $a_i \equiv b_i \pmod{c}$ *dla* $i = 1, \ldots, n$, *to*

$$a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n \pmod{c},$$

(iv) jeżeli $a_i \equiv b_i \pmod{c}$ *dla* $i = 1, \ldots, n$, *to*

$$a_1 \cdot \ldots \cdot a_n \equiv b_1 \cdot \ldots \cdot b_n \pmod{c},$$

(v) jeżeli $a \equiv b \pmod{c}$, *to* $a^n \equiv b^n \pmod{c}$.

Dowód. (i). Załóżmy, że $a \equiv b \pmod{c}$. Wtedy $c \mid a - b$, więc ze stwierdzenia 13.2 dostajemy, że $c \mid (a - b) \cdot d$, czyli $c \mid a \cdot d - b \cdot d$, a zatem $a \cdot d \equiv b \cdot d \pmod{c}$. Ponadto, ze stwierdzenia 13.2 mamy, że $c \cdot d \mid (a - b) \cdot d$, czyli $c \cdot d \mid a \cdot d - b \cdot d$, a zatem $a \cdot d \equiv b \cdot d \pmod{c \cdot d}$.

(ii). Załóżmy, że $a \cdot d \equiv b \cdot d \pmod{c \cdot d}$ i $d \neq 0$. Wtedy $c \cdot d \mid a \cdot d - b \cdot d$, więc ze stwierdzenia 13.2: $c \mid a - b$, czyli $a \equiv b \pmod{c}$.

(iii). Z założenia, dla każdego $i = 1, \ldots, n$ istnieje $t_i \in P$ takie, że $a_i - b_i = t_i \cdot c$. Stąd $(a_1 + \ldots + a_n) - (b_1 + \ldots + b_n) = (t_1 + \ldots + b_n) \cdot c$, czyli $a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n \pmod{c}$.

(iv). Zastosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista. Jeśli $a_i \equiv b_i \pmod{c}$ dla $i = 1, 2$, to $c \mid a_i - b_i$, więc $a_i - b_i = t_i \cdot c$ dla pewnego $t_i \in P$. Zatem $a_1 \cdot a_2 - b_1 \cdot b_2 = (b_1 + t_1 \cdot c) \cdot (b_2 + t_2 \cdot c) - b_1 \cdot b_2 = = (b_1 \cdot t_2 + t_1 \cdot b_2 + t_1 \cdot t_2 \cdot c) \cdot c$, skąd $c \mid a_1 \cdot a_2 - b_1 \cdot b_2$, czyli $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{c}$. Zatem teza zachodzi także dla $n = 2$.

Przypuśćmy, że teza zachodzi dla pewnego naturalnego n i weźmy dowolne $a_i, b_i \in P$ takie, że $a_i \equiv b_i \pmod{c}$ dla $i = 1, \ldots, n+1$. Wtedy z założenia indukcyjnego $a_1 \cdot \ldots \cdot a_n \equiv b_1 \cdot \ldots \cdot b_n \pmod{c}$. Ponadto $a_{n+1} \equiv b_{n+1} \pmod{c}$, więc z kroku dla $n = 2$, $(a_1 \cdot \ldots \cdot a_n) \cdot a_{n+1} \equiv \equiv (b_1 \cdot \ldots \cdot b_n) \cdot b_{n+1} \pmod{c}$, czyli teza zachodzi dla liczby $n + 1$.

(v). Wystarczy w (iv) podstawić $a = a_1 = \ldots = a_n$ i $b = b_1 = \ldots = = b_n$. □

Przykład 13.6. Niech D będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej. Jeżeli $D > 0$, to przez $\sqrt{D}$ będziemy rozumieli dodatnią liczbę rzeczywistą, której kwadrat jest równy D. Jeżeli zaś $D < 0$, to przez $\sqrt{D}$ będziemy rozumieli $\sqrt{-D} \cdot i$, gdzie $\sqrt{-D}$ jest dodatnią liczbą rzeczywistą, której kwadrat jest równy $-D$, a i jest jednostką urojoną; zatem w tym przypadku także $(\sqrt{D})^2 = D$. Jeżeli $D < 0$ oraz $a_1, a_2, b_1, b_2 \in \mathbb{Q}$ i $a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D}$, to $a_1 + b_1\sqrt{-D}i = a_2 + b_2\sqrt{-D}i$, więc $a_1 = a_2$ i $b_1\sqrt{-D} = b_2\sqrt{-D}$, skąd $b_1 = b_2$. Stąd i na mocy (12.1) dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{Q}$ mamy, że

$$a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D} \iff [a_1 = a_2 \text{ i } b_1 = b_2]. \tag{13.1}$$

Z rozdziału 12 wiemy, że w przypadku, gdy $D > 0$

$$\mathbb{Q}(\sqrt{D}) = \{x + y\sqrt{D} : x, y \in \mathbb{Q}\}$$

jest podciałem ciała $\mathbb{R}$, a więc jest ciałem. Analogicznie dowodzimy, że $\mathbb{Q}(\sqrt{D})$ jest podciałem ciała $\mathbb{C}$, gdy $D < 0$. Ponadto, analogicznie jak w dowodzie stwierdzenia 12.1 pokazujemy, że funkcja $\alpha \mapsto \overline{\alpha}$, gdzie $\overline{x + y\sqrt{D}} = x - y\sqrt{D}$ dla $x, y \in \mathbb{Q}$ spełnia podpunkty $(i) - (vi)$ stwierdzenia 12.1.

Niech

$$\mathbb{Z}[\sqrt{D}] = \{x + y\sqrt{D} : x, y \in \mathbb{Z}\}.$$

Oczywiście $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{Q}(\sqrt{D})$, $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{D}]$ oraz $\alpha - \beta \in \mathbb{Z}[\sqrt{D}]$ dla dowolnych $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$. Ponadto $\alpha = a_1 + b_1\sqrt{D}$ i $\beta = a_2 + b_2\sqrt{D}$, więc $\alpha \cdot \beta = (a_1a_2 + Db_1b_2) + (a_1b_2 + b_1a_2)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Wobec tego $\mathbb{Z}[\sqrt{D}]$ jest dziedziną całkowitości oraz $\overline{\alpha} \in \mathbb{Z}[\sqrt{D}]$ dla każdego $\alpha \in \mathbb{Z}[\sqrt{D}]$.

Zauważmy, że dla $x, y \in \mathbb{Q}$ zachodzi wzór:

$$(x + y\sqrt{D}) \cdot \overline{(x + y\sqrt{D})} = x^2 - Dy^2, \tag{13.2}$$

z którego wynika, że $\alpha \cdot \overline{\alpha} \in \mathbb{Q}$ dla $\alpha \in \mathbb{Q}(\sqrt{D})$ i $\alpha \cdot \overline{\alpha} \in \mathbb{Z}$ dla każdego $\alpha \in \mathbb{Z}[\sqrt{D}]$.

Zauważmy, że dla dowolnych $k, a, b \in \mathbb{Z}$:

$$k \mid a + b\sqrt{D} \iff [k \mid a \text{ oraz } k \mid b \text{ w pierścieniu } \mathbb{Z}]. \tag{13.3}$$

Rzeczywiście, jeśli $k \mid a+b\sqrt{D}$, to istnieją $x, y \in \mathbb{Z}$ takie, że $a+b\sqrt{D} = k(x+y\sqrt{D})$, skąd na mocy (13.1), $a = kx$ i $b = ky$. Na odwrót, jeśli $k \mid a$ i $k \mid b$ w pierścieniu $\mathbb{Z}$, to $a = kx$ i $b = ky$ dla pewnych $x, y \in \mathbb{Z}$, więc $a + b\sqrt{D} = k(x + y\sqrt{D})$, skąd $k \mid a + b\sqrt{D}$.

Duże znaczenie ma też funkcja $N = N_D \colon \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ dana wzorem

$$N(\alpha) = \alpha \cdot \overline{\alpha}.$$

Zauważmy, że dla $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$: $N(\alpha\cdot\beta) = (\alpha\cdot\beta)\cdot\overline{(\alpha \cdot \beta)} = \alpha\cdot\beta\cdot\overline{\alpha}\cdot\overline{\beta} = (\alpha \cdot \overline{\alpha}) \cdot (\beta \cdot \overline{\beta}) = N(\alpha) \cdot N(\beta)$, czyli:

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \quad \text{dla dowolnych } \alpha, \beta \in \mathbb{Q}(\sqrt{D}). \tag{13.4}$$

Jeśli $\beta \neq 0$, to $\alpha = \beta \cdot \frac{\alpha}{\beta}$ i ze wzoru (13.4) uzyskujemy:

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}. \tag{13.5}$$

Dodatkowo, $N(a) = a^2$ dla $a \in \mathbb{Q}$ i w szczególności $N(1) = 1$. Pokażemy teraz, że zachodzi jeszcze jedna ważna własność funkcji N:

$$\text{jeżeli } \alpha \mid \beta \text{ w pierścieniu } \mathbb{Z}[\sqrt{D}], \text{ to } N(\alpha) \mid N(\beta) \text{ w pierścieniu } \mathbb{Z}. \tag{13.6}$$

Rzeczywiście, jeśli $\alpha \mid \beta$ w pierścieniu $\mathbb{Z}[\sqrt{D}]$, to $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$ i istnieje $\gamma \in \mathbb{Z}[\sqrt{D}]$ takie, że $\beta = \gamma \cdot \alpha$. Zatem z (13.4), $N(\beta) = N(\gamma) \cdot N(\alpha)$. Ponadto $N(\alpha), N(\beta), N(\gamma) \in \mathbb{Z}$, więc $N(\alpha) \mid N(\beta)$ w pierścieniu $\mathbb{Z}$.

Funkcja N ma związek z elementami odwracalnymi pierścienia $\mathbb{Z}[\sqrt{D}]$. Zachodzą bowiem następujące wzory:

$$(\mathbb{Z}[\sqrt{D}])^* = \{\alpha \in \mathbb{Z}[\sqrt{D}] : N(\alpha) = \pm 1\}, \tag{13.7}$$

$$(\mathbb{Z}[\sqrt{D}])^* = \{x + y\sqrt{D} : x, y \in \mathbb{Z} \text{ i } x^2 - Dy^2 = \pm 1\}. \tag{13.8}$$

Rzeczywiście, niech $\alpha = x + y\sqrt{D}$, gdzie $x, y \in \mathbb{Z}$. Jeśli $x^2 - Dy^2 = \pm 1$, to $\alpha \cdot \overline{\alpha} = \pm 1$, skąd $\alpha \cdot \overline{\alpha} = 1$ lub $\alpha \cdot (-\overline{\alpha}) = 1$, a więc $\alpha \in (\mathbb{Z}[\sqrt{D}])^*$. Na odwrót, załóżmy, że $\alpha \in (\mathbb{Z}[\sqrt{D}])^*$. Wtedy $\alpha \cdot \beta = 1$ dla pewnego $\beta \in \in \mathbb{Z}[\sqrt{D}]$, więc na mocy (13.4), $N(\alpha) \cdot N(\beta) = 1$. Ponadto liczby $N(\alpha)$ i $N(\beta)$ są całkowite, więc $N(\alpha) = \pm 1$.

Ze wzoru (13.8) uzyskujemy od razu następujący wzór:

$$(\mathbb{Z}[\sqrt{D}])^* = \{1, -1\} \quad \text{dla każdego } D < -1. \tag{13.9}$$

Dla $D = -1$ pierścień $\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[i]$ jest nazywany **pierścieniem liczb całkowitych Gaussa**. Ze wzoru (13.8) na mocy przykładu 4.32 uzyskujemy się wzór:

$$(\mathbb{Z}[i])^* = \{1, -1, i, -i\}. \tag{13.10}$$

Przykład 13.7. Niech D będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej taką, że $D \equiv 1 \pmod 4$. Oznaczmy

$$\omega = \omega_D = \frac{1 + \sqrt{D}}{2}.$$

Wtedy $2\omega - 1 = \sqrt{D}$, skąd $4\omega^2 - 4\omega + 1 = D$, czyli

$$\omega^2 = \omega + \frac{D-1}{4}, \tag{13.11}$$

przy czym $\frac{D-1}{4} \in \mathbb{Z}$, bo $D \equiv 1 \pmod 4$. Wynika stąd, że zbiór $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ jest pierścieniem. Ponadto zbiór $\{1, \omega\}$ jest

liniowo niezależny nad ciałem $\mathbb{Q}$. Dla $x, y \in \mathbb{Z}$ mamy, że $x + y\sqrt{D} = (x - y) + 2y\frac{1+\sqrt{D}}{2}$, więc $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Zauważmy, że

$$\overline{\omega} = 1 - \omega \in \mathbb{Z}[\omega], \tag{13.12}$$

bo $\overline{\omega} = \frac{1-\sqrt{D}}{2} = 1 - \frac{1+\sqrt{D}}{2} = 1 - \omega \in \mathbb{Z}[\omega]$. Wynika stąd, że $\overline{\alpha} \in \mathbb{Z}[\omega]$ dla wszystkich $\alpha \in \mathbb{Z}[\omega]$. Ponadto,

$$N(a+b\omega) = a^2 + ab - b^2 \cdot \frac{D-1}{4} \in \mathbb{Z} \text{ dla dowolnych } a, b \in \mathbb{Z}, \tag{13.13}$$

gdyż $N(\alpha) = (a + \frac{b}{2})^2 - D(\frac{b}{2})^2 = a^2 + ab + \frac{b^2}{4} - \frac{b^2 D}{4} = a^2 + ab - b^2 \cdot \frac{D-1}{4}$, skąd $N(\alpha) \in \mathbb{Z}$. Stąd, podobnie jak w przykładzie 13.6 pokazuje się, że w tym przypadku zachodzą wzory:

$$(\mathbb{Z}[\omega])^* = \{\alpha \in \mathbb{Z}[\omega] : N(\alpha) = \pm 1\}, \tag{13.14}$$

$$(\mathbb{Z}[\omega])^* = \{a + b\omega : a^2 + ab - b^2\frac{D-1}{4} = \pm 1\}. \tag{13.15}$$

Pierścień $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ nazywany jest **pierścieniem Eisensteina**. Ze wzoru (13.15) na mocy przykładu 4.33 wynika, że grupa $(\mathbb{Z}[\frac{1+\sqrt{-3}}{2}])^*$ ma dokładnie sześć elementów i zachodzi wzór:

$$\left(\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)^* = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}. \tag{13.16}$$

Natomiast dla $D < -3$ i $D \equiv 1 \pmod 4$ zachodzi wzór:

$$\left(\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]\right)^* = \{1, -1\}. \tag{13.17}$$

13.2 Dziedziny z jednoznacznością rozkładu

Definicja 13.8. Niech P będzie dziedziną całkowitości i $a \in P$. Mówimy, że a jest **elementem nierozkładalnym** pierścienia P, jeżeli $a \neq 0$, $a \notin P^*$ i dla dowolnych $x, y \in P$ takich, że $a = x \cdot y$ jest $x \in P^*$ lub $y \in P^*$.

Definicja 13.9. Niech P będzie dziedziną całkowitości i $a \in P$. Mówimy, że a jest **elementem pierwszym** pierścienia P, jeżeli $a \neq 0$, $a \notin P^*$ i dla dowolnych $x, y \in P$ takich, że $a \mid x \cdot y$ mamy, że $a \mid x$ lub $a \mid y$ w pierścieniu P.

Przez prostą indukcje dowodzi się, że jeżeli a jest elementem pierwszym dziedziny całkowitości P, to iloczyn skończonej liczby elementów pierścienia P jest podzielny przez a wtedy i tylko wtedy, gdy pewien z tych czynników jest podzielny przez a.

Stwierdzenie 13.10. *Każdy element pierwszy dziedziny całkowitości P jest elementem nierozkładalnym w P.*

Dowód. Niech a będzie elementem pierwszym dziedziny całkowitości P. Wtedy $a \neq 0$ i $a \notin P^*$. Weźmy dowolne $x, y \in P$ takie, że $a = x \cdot y$. Wtedy $a \mid x \cdot y$, więc $a \mid x$ lub $a \mid y$. W pierwszym przypadku $x = a \cdot t$ dla pewnego $t \in P$, więc $a = x \cdot y = at \cdot y$, skąd $a \cdot (1 - t \cdot y) = 0$. Ponadto P jest dziedziną całkowitości i $a \neq 0$, więc $1 - ty = 0$, skąd $1 = ty$, czyli $y \in P^*$. W drugim przypadku, $y = s \cdot a$ dla pewnego $s \in P$, skąd $a = x \cdot y = x \cdot sa$, więc $a \cdot (1 - xs) = 0$. Zatem $1 = x \cdot s$, skąd $x \in P^*$. Wobec tego a jest elementem nierozkładalnym w P. □

Przykład 13.11. Nie zawsze element nierozkładalny jest elementem pierwszym. Pokażemy, że dla liczb całkowitych $D < -2$ w pierścieniu $\mathbb{Z}[\sqrt{D}]$ liczba 2 jest elementem nierozkładalnym, ale nie jest elementem pierwszym. Oczywiście $2 \neq 0$ i ze wzoru (13.8), $2 \notin (\mathbb{Z}[\sqrt{D}])^*$. Załóżmy, ze istnieje $\alpha \in \mathbb{Z}[\sqrt{D}]$ takie, że $N(\alpha) = 2$. Wtedy $\alpha = x + y\sqrt{D}$ dla pewnych $x, y \in \mathbb{Z}$, więc $x^2 - Dy^2 = 2$, ale $-D > 2$, więc dla $y \neq 0$, $2 = x^2 - Dy^2 \geqslant -Dy^2 \geqslant -D > 2$, co prowadzi do sprzeczności. Ponadto dla $y = 0$, $x^2 = 2$, co też jest niemożliwe. Weźmy teraz dowolne $\beta, \gamma \in \mathbb{Z}[\sqrt{D}]$ takie, że $2 = \beta \cdot \gamma$. Wtedy na mocy (13.4), $4 = N(\beta) \cdot N(\gamma)$, ale $N(\beta), N(\gamma) \in \mathbb{N}_0$ i jak pokazaliśmy, $N(\beta), N(\gamma) \neq 2$, więc $N(\beta) = 1$ lub $N(\gamma) = 1$. Stąd na mocy (13.7), $\beta \in (\mathbb{Z}[\sqrt{D}])^*$ lub $\gamma \in (\mathbb{Z}[\sqrt{D}])^*$. Zatem 2 jest elementem nierozkładalnym w $\mathbb{Z}[\sqrt{D}]$.

Elementy pierścienia $\mathbb{Z}[\sqrt{D}]$ które są podzielne przez 2 są postaci $2(a + b\sqrt{D}) = 2a + 2b\sqrt{D}$ dla $a, b \in \mathbb{Z}$. Stąd $2 \nmid 1 + \sqrt{D}$, $2 \nmid 1 - \sqrt{D}$

oraz $2 \nmid \sqrt{D}$. Jeśli liczba D jest parzysta, to $2 \mid D$ w pierścieniu $\mathbb{Z}$, skąd $2 \mid D$ w pierścieniu $\mathbb{Z}[\sqrt{D}]$ oraz $D = \sqrt{D} \cdot \sqrt{D}$, więc wtedy 2 nie jest elementem pierwszym pierścienia $\mathbb{Z}[\sqrt{D}]$. Jeżeli zaś liczba D jest nieparzysta, to $2 \mid 1 - D$ w pierścieniu $\mathbb{Z}$, skąd $2 \mid 1 - D$ w pierścieniu $\mathbb{Z}[\sqrt{D}]$ oraz $1 - D = (1 + \sqrt{D}) \cdot (1 - \sqrt{D})$, więc także w tym przypadku 2 nie jest elementem pierwszym pierścienia $\mathbb{Z}[\sqrt{D}]$.

Przykład 13.12. Niech D będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej i niech $p \in \mathbb{P}$. Załóżmy, że $\alpha \in \mathbb{Z}[\sqrt{D}]$ i $N(\alpha) = \pm p$. Wtedy $\alpha \neq 0$ i na mocy (13.9), $\alpha \notin (\mathbb{Z}[\sqrt{D}])^*$. Ponadto $\alpha = a + b\sqrt{D}$ dla pewnych $a, b \in \mathbb{Z}$. Stąd $a^2 - Db^2 = \pm p$, więc $p \nmid b$, bo inaczej $p \mid b$ i $p \mid a$, skąd $p^2 \mid \pm p$, co jest niemożliwe. Weźmy dowolne $x, y \in \mathbb{Z}$. Ponieważ $p \nmid b$, więc na mocy lematu 2.9 istnieje $k \in \mathbb{Z}_p$ takie, że $bk \equiv bx - ay \pmod{p}$. Stąd $b(x - k) \equiv ay \pmod{p}$, więc $ab(x - k) \equiv a^2 y \pmod{p}$, ale $a^2 = Db^2 \pm p$, więc $ab(x - k) \equiv Db^2 y \pmod{p}$, skąd $a(x - k) \equiv Dby \pmod{p}$, bo $p \nmid b$. Ponadto $\frac{(x-k)+y\sqrt{D}}{a+b\sqrt{D}} = \frac{((x-k)+y\sqrt{D})(a-b\sqrt{D})}{a^2-Db^2} = \frac{(x-k)a-byD}{\pm p} + \frac{ay-b(x-k)}{\pm p}\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Stąd uzyskujemy, że $x + y\sqrt{D} \equiv k \pmod{\alpha}$ w pierścieniu $\mathbb{Z}[\sqrt{D}]$.

Weźmy dowolne $\beta, \gamma \in \mathbb{Z}[\sqrt{D}]$ takie, że $\alpha \mid \beta \cdot \gamma$. Wtedy istnieją $k, l \in \mathbb{Z}_p$ takie, że $\beta \equiv k \pmod{\alpha}$ i $\gamma \equiv l \pmod{\alpha}$. Zatem $\beta \cdot \gamma \equiv kl \pmod{\alpha}$, ale $\beta \cdot \gamma \equiv 0 \pmod{\alpha}$, więc stąd $\alpha \mid kl$ i na mocy (13.6), $N(\alpha) \mid N(k) \cdot N(l)$, czyli $p^2 \mid kl$. Stąd $p \mid k$ lub $p \mid l$, ale $\alpha \mid p$, więc $\alpha \mid k$ lub $\alpha \mid l$, skąd $\alpha \mid \beta$ lub $\alpha \mid \gamma$.

Wobec tego α jest elementem pierwszym w pierścieniu $\mathbb{Z}[\sqrt{D}]$ i na mocy stwierdzenia 13.10, α jest elementem nierozkładalnym tego pierścienia.

Podobnie pokazujemy, że jeśli dodatkowo $D \equiv 1 \pmod{4}$ i $p \in \mathbb{P}$ oraz $N(\alpha) = \pm p$ dla pewnego $\alpha \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, to α jest elementem pierwszym w pierścieniu $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ i na mocy stwierdzenia 13.10, α jest elementem nierozkładalnym tego pierścienia.

Definicja 13.13. Niech P będzie dziedziną całkowitości i $a \in P$. Mówimy, że a ma **rozkład jednoznaczny** w pierścieniu P, jeżeli $a = p_1 \cdot \ldots \cdot p_n$ dla pewnych elementów nierozkładalnych $p_1, \ldots, p_n$ pierścienia P oraz jeżeli $a = q_1 \cdot \ldots \cdot q_m$ dla pewnych elementów nie-

rozkładalnych $q_1, \ldots, q_m$ pierścienia P, to $m = n$ i po ewentualnej permutacji indeksów mamy, że $q_i \sim p_i$ dla każdego $i = 1, \ldots, n$.

Definicja 13.14. Mówimy, że dziedzina całkowitości P jest **dziedziną z jednoznacznością rozkładu**, jeżeli każdy jej niezerowy i nieodwracalny element ma rozkład jednoznaczny.

Twierdzenie 13.15. *W dziedzinie z jednoznacznością rozkładu pojęcia elementu nierozkładalnego i elementu pierwszego pokrywają się.*

Dowód. Niech P będzie dziedziną z jednoznacznością rozkładu i niech $a \in P$. Jeżeli a jest elementem pierwszym w P, to na mocy stwierdzenia 13.10, a jest elementem nierozkładalnym w P. Na odwrót, przypuśćmy, że a jest elementem nierozkładalnym w P i weźmy dowolne $x, y \in P$ takie, że $a \mid x \cdot y$. Należy pokazać, że wtedy $a \mid x$ lub $a \mid y$. Ponieważ $0 = 0 \cdot a$, więc $a \mid 0$, czyli można dalej zakładać, że $x \neq 0$ i $y \neq 0$. Dalej, $x \cdot y = t \cdot a$ dla pewnego $t \in P$. Jeśli $x \in P^*$, to $y = (tx^{-1}) \cdot a$, skąd $a \mid y$. Podobnie, jeśli $y \in P^*$, to $a \mid x$. Możemy zatem dalej zakładać, że $x \notin P^*$ i $y \notin P^*$. Stąd $t \neq 0$. Jeśli $t \in P^*$, to $(t^{-1}x) \cdot y = a$, więc z nierozkładalności a, $t^{-1}x \in P^*$ lub $y \in P^*$, skąd $a \mid y$ lub $a \mid x$. Niech dalej $t \notin P^*$. Zatem $x, y, t \neq 0$ i $x, y, t \notin P^*$. Ponadto P jest dziedziną z jednoznacznością rozkładu, więc istnieją elementy nierozkładalne $p_1, \ldots, p_k, q_1, \ldots, p_l, r_1, \ldots, r_n$ takie, że $x = p_1 \cdot \ldots \cdot p_k$, $y = q_1 \cdot \ldots \cdot q_l$ i $t = r_1 \cdot \ldots \cdot r_n$. Ponadto $x \cdot y = t \cdot a$, więc $p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_l = r_1 \cdot \ldots \cdot r_n \cdot a = ta$ i z jednoznaczności rozkładu elementu ta oraz z nierozkładalności elementu a wynika, że $a \sim p_i$ dla pewnego $i = 1, \ldots, k$ lub $a \sim q_j$ dla pewnego $j = 1, \ldots, l$. Stąd $a \mid x$ lub $a \mid y$. □

Twierdzenie 13.16. *Dla dziedziny całkowitości P następujące warunki są równoważne:*

(i) P jest dziedziną z jednoznacznością rozkładu,

(ii) każdy element $a \in P$ nierozkładalny w P jest elementem pierwszym w P i każdy niezerowy element nieodwracalny pierścienia P jest iloczynem skończonej liczby elementów nierozkładalnych w P.

Dowód. Na mocy twierdzenia 13.15 wystarczy udowodnić implikację $(ii) \Rightarrow (i)$. Sprowadza się to do wykazania, że jeżeli

$$p_1, \ldots, p_m, q_1, \ldots, q_n$$

są elementami nierozkładalnymi w P takimi, że $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$, to $m = n$ i po ewentualnej permutacji elementów $p_1, \ldots, p_m$ mamy, że $p_i \sim q_i$ dla każdego $i = 1, \ldots, m$.

Zastosujemy indukcję ze względu na m (przy dowolnym $n \in \mathbb{N}$). Dla $m = 1$ z nierozkładalności elementów $p_1, q_1, \ldots, q_n$ wynika, że $n = 1$ (bo inaczej $q_i \in P^*$ dla pewnego $i = 1, \ldots, n$, co jest niemożliwe), więc $p_1 = q_1$, czyli $p_1 \sim q_1$.

Przypuśćmy, że teza zachodzi dla pewnej liczby naturalnej m i niech $p_1, \ldots, p_{m+1}, q_1, \ldots, q_n$ będą elementami pierwszymi w P takimi, że $p_1 \cdot \ldots \cdot p_{m+1} = q_1 \cdot \ldots \cdot q_n$. Na mocy pierwszej części dowodu $n > 1$. Ponadto wtedy $p_{m+1} \mid q_1 \cdot \ldots \cdot q_n$ i na mocy założenia p_{m+1} jest elementem pierwszym, więc $p_{m+1} \mid q_i$ dla pewnego $i = 1, \ldots, n$. Bez zmniejszania ogólności możemy zakładać, że $p_{m+1} \mid q_n$. Dodatkowo p_{m+1} i q_n są elementami nierozkładalnymi, więc $q_n \sim p_{m+1}$ i na mocy stwierdzenia 13.2, $p_{m+1} = uq_n$ dla pewnego $u \in P^*$. Po skróceniu przez q_n uzyskujemy, że $(up_1) \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_{n-1}$. Ponadto $up_1 \sim p_1$, czyli up_1 jest elementem nierozkładalnym w P, więc na mocy założenia indukcyjnego $m = n - 1$ i po ewentualnej zmianie kolejności czynników nierozkładalnych $up_1 \sim q_1, p_2 \sim q_2, \ldots, p_m \sim q_m$. Wobec tego $m + 1 = n$ i $p_i \sim q_i$ dla każdego $i = 1, \ldots, m, m + 1$. □

Twierdzenie 13.17. *Niech D będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej. Pierścień $\mathbb{Z}[\sqrt{D}]$ jest dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy, gdy każdy jego element nierozkładalny jest elementem pierwszym.*

Dowód. Na mocy twierdzenia 13.16 wystarczy pokazać, że każdy niezerowy i nieodwracalny element $\alpha \in \mathbb{Z}[\sqrt{D}]$ jest iloczynem skończonej liczby elementów nierozkładalnych tego pierścienia. Z przykładu 13.6 wynika, że $|N_D(\alpha)| \in \mathbb{N} \setminus \{1\}$. Gdyby zatem nasza teza była fałszywa, to na mocy zasady minimum istniałoby $\alpha \in \mathbb{Z}[\sqrt{D}]$ takie, że $|N_D(\alpha)| > 1$ i α nie jest iloczynem skończonej liczby elemen-

tów nierozkładalnych pierścienia $\mathbb{Z}[\sqrt{D}]$, przy czym $|N_D(\alpha)|$ jest najmniejsze. Stąd w szczególności α nie jest elementem nierozkładalnym w $\mathbb{Z}[\sqrt{D}]$. Ponadto $\alpha \neq 0$ i α nie jest odwracalne w $\mathbb{Z}[\sqrt{D}]$, więc $\alpha = \beta \cdot \gamma$ dla pewnych niezerowych elementów $\beta, \gamma \in \mathbb{Z}[\omega_D]$, które nie są odwracalne w $\mathbb{Z}[\omega_D]$. Stąd $|N_D(\alpha)| = |N_D(\beta)| \cdot |N_D(\gamma)|$, a ponieważ $|N_D(\beta)|, |N_D(\gamma)| \in \mathbb{N}$ i na mocy przykładu 13.6, $|N_D(\beta)|, |N_D(\gamma)| > 1$, więc $|N_D(\beta)|, |N_D(\gamma)| < |N_D(\alpha)|$. Zatem z minimalności $|N_D(\alpha)|$ istnieją elementy nierozkładalne $p_1, \ldots, p_n, q_1, \ldots, q_m$ pierścienia $\mathbb{Z}[\sqrt{D}]$ takie, że $\beta = p_1 \cdot \ldots \cdot p_n$ i $\gamma = q_1 \cdot \ldots \cdot q_m$. Stąd $\alpha = p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m$, czyli α jest iloczynem skończonej liczby elementów nierozkładalnych w $\mathbb{Z}[\sqrt{D}]$, sprzeczność. □

Przykład 13.18. Niech $D < -2$ będzie liczbą całkowitą. Wtedy z twierdzenia 13.17 i z przykładu 13.11 wynika, że pierścień $\mathbb{Z}[\sqrt{D}]$ nie jest z jednoznacznością rozkładu (chociaż oczywiście jest dziedziną całkowitości).

Używając przykładu 13.7 można analogicznie jak w przypadku twierdzenia 13.17 udowodnić następujące

Twierdzenie 13.19. *Niech D będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej i taką, że $D \equiv 1 \pmod 4$. Pierścień $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ jest dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy, gdy każdy jego element nierozkładalny jest elementem pierwszym.*

Elementy $a_1, \ldots, a_n$ dziedziny z jednoznacznością rozkładu P nazywamy **względnie pierwszymi**, jeżeli każdy ich wspólny dzielnik jest elementem odwracalnym w P. Na mocy twierdzenia 13.15 jest to równoważne temu, że nie istnieje element pierwszy w P będący wspólnym dzielnikiem elementów $a_1, \ldots, a_n$.

Następujące twierdzenie, odgrywa fundamentalną rolę w rozwiązywaniu wielu równań diofantycznych:

Twierdzenie 13.20. *Niech a, b, c będą elementami dziedziny z jednoznacznością rozkładu P. Jeżeli elementy a i b są względnie pierwsze oraz $a \cdot b \sim c^n$ dla pewnego naturalnego n, to istnieją $c_1, c_2 \in P$ takie, że $a \sim c_1^n$ i $b \sim c_2^n$.*

Dowód. Jeżeli $a = 0$, to $b \neq 0$ i $b \mid a$ oraz oczywiście $b \mid b$, więc $b \in P^*$, bo elementy a i b są względnie pierwsze. Zatem wtedy $b \sim 1$, skąd $a \sim 0^n$ i $b \sim 1^n$. Analogicznie dla $b = 0$ wystarczy wziąć $c_1 = 1$ i $c_2 = 0$. Niech dalej $a \neq 0$ i $b \neq 0$. Jeżeli $a \in P^*$, to $b \sim ab$, więc $b \sim c^n$ i $a \sim 1^n$. Jeżeli $b \in P^*$, to podobnie $a \sim c^n$ i $b \sim 1^n$. Możemy zatem zakładać, że $a \notin P^*$ i $b \notin P^*$ oraz $a \neq 0$ i $b \neq 0$. Ponieważ P jest dziedziną z jednoznacznością rozkładu oraz elementy a i b są względnie pierwsze, więc istnieją parami niestowarzyszone elementy pierwsze $p_1, \ldots, p_s, q_1, \ldots, q_r$ oraz istnieją liczby naturalne $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r$ takie, że $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ i $b = q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}$. Zatem $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r} \sim c^n$. Stąd $c \neq 0$, $c \notin P^*$ i jeśli element pierwszy p dzieli c, to $p \sim p_i$ dla pewnego $i = 1, \ldots, s$ lub $p \sim q_j$ dla pewnego $j = 1, \ldots, r$. Wobec tego $c = up_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s} \cdot q_1^{\delta_1} \cdot \ldots \cdot q_r^{\delta_r}$ dla pewnego $u \in P^*$ oraz dla pewnych liczb naturalnych $\gamma_1, \ldots, \gamma_s, \delta_1, \ldots, \delta_r$. Zatem $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r} = (up_1)^{n\gamma_1} \cdot \ldots \cdot p_s^{n\gamma_s} \cdot q_1^{n\delta_1} \cdot \ldots \cdot q_r^{n\delta_r}$, skąd z jednoznaczności rozkładu w pierścieniu P, $\alpha_i = n\gamma_i$ dla $i = 1, \ldots, s$ oraz $\beta_j = n\delta_j$ dla $j = 1, \ldots, r$. Zatem $a \sim c_1^n$ dla $c_1 = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$ oraz $b \sim c_2^n$ dla $c_2 = q_1^{\delta_1} \cdot \ldots \cdot q_r^{\delta_r}$. □

13.3 Przykłady dziedzin z jednoznacznością rozkładu

Ideałem pierścienia P nazywamy taki niepusty podzbiór $I \subseteq P$, że $i - j \in I$ oraz $a \cdot i \in I$ dla dowolnych $i, j \in I$ oraz dla każdego $a \in P$. Dla każdego $a \in P$ zbiór

$$(a) = aP = \{a \cdot x : x \in P\}$$

jest ideałem pierścienia P. Nazywamy go **ideałem głównym generowanym przez** a. Dziedzinę całkowitości, w której każdy ideał jest główny nazywamy **dziedziną ideałów głównych**.

Twierdzenie 13.21. *Każda dziedzina ideałów głównych P jest dziedziną z jednoznacznością rozkładu.*

Dowód. Niech $a \in P$ będzie elementem nierozkładalnym. Weźmy dowolne $x, y \in P$ takie, że $a \mid xy$ i przypuśćmy, że $a \nmid x$. Zauważmy, że $(a, x) = \{au + xv : u, v \in P\}$ jest ideałem pierścienia P ostro zawierającymi ideał (a), bo $x \in (a, x) \setminus (a)$, gdyż $a \nmid x$. Dodatkowo każdy ideał pierścienia P jest główny, więc $(a, x) = (p)$ dla pewnego $p \in P$. Stąd $a = pr$ dla pewnego $r \in P$. Jeśli $r \in P^*$, to $p = ar^{-1}$ i $x = pt$ dla pewnego $t \in P$, więc $x = a(s^{-1}t)$, skąd $a \mid x$, wbrew założeniu. Zatem $r \notin P^*$ i z nierozkładalności elementu a mamy, że $p \in P^*$. Stąd $1 = pp^{-1} \in (a, x)$, czyli $1 = au + xv$ dla pewnych $u, v \in P$. Zatem $y = auy + xyv$, skąd $a \mid y$, bo $a \mid xy$ i $a \mid auy$. Wobec tego a jest elementem pierwszym w P.

Na mocy twierdzenia 13.16 wystarczy wykazać, że każdy niezerowy i nieodwracalny element pierścienia P jest iloczynem skończonej liczby elementów nierozkładalnych w P. Przypuśćmy, że tak nie jest. Wtedy istnieje niezerowy element c nieodwracalny w P, który nie jest iloczynem skończonej liczby elementów nierozkładalnych w P. W szczególności c nie jest elementem nierozkładalnym w P. Zatem $c = c_1 \cdot d_1$ dla pewnych niezerowych elementów nieodwracalnych pierścienia P, przy czym można zakładać, że c_1 nie jest iloczynem skończonej liczby elementów nierozkładalnych w P. Zauważmy, że ideał (c) jest ostro zawarty w ideale (c_1), bo $c = c_1 d_1$ i $c_1 \notin (a)$, gdyż inaczej $c_1 = cu$ dla pewnego $u \in P$, skąd $c_1 = c_1 d_1 u$, a zatem $1 = d_1 u$, skąd $d_1 \in P^*$, wbrew założeniu. Analogicznie, istnieje niezerowy element nieodwracalny c_2 taki, że ideał (c_1) jest ostro zawarty w ideale (c_2). Kontynuując ten proces widzimy, że możemy skonstruować ciąg elementów $c, c_1, c_2, \ldots$ pierścienia P taki, że $(c) \subset (c_1) \subset (c_2) \subset \ldots$. Standardowe sprawdzenie pokazuje, że $I = (c) \cup (c_1) \cup (c_2) \cup \ldots$ jest ideałem pierścienia P. Zatem $I = (b)$ dla pewnego $b \in P$. Wtedy $b \in I$, więc $b \in (c_k)$ dla pewnego $k \in \mathbb{N}$, więc $I = (b) \subseteq (c_k) \subseteq (c_{k+1}) \subseteq I$, skąd $(c_k) = (c_{k+1})$ i mamy sprzeczność. □

Ważną podklasą dziedzin ideałów głównych są tak zwane **pierścienie euklidesowe**. Oto ich określenie:

Definicja 13.22. Powiemy, że dziedzina całkowitości P jest **pierścieniem euklidesowym**, jeżeli istnieje funkcja $N \colon P \to \mathbb{N}_0$ zwana

normą i taka, że:

I. dla każdego $a \in P$: $N(a) = 0$ wtedy i tylko wtedy, gdy $a = 0$,

II. $N(a \cdot b) = N(a) \cdot N(b)$ dla dowolnych $a, b \in P$,

III. dla każdego niezerowego $a \in P$ i dla dowolnego $b \in P$ istnieją $q, r \in P$ takie, że $b = q \cdot a + r$ i $N(r) < N(a)$.

Stwierdzenie 13.23. *Niech P będzie pierścieniem euklidesowym z normą N. Wówczas $N(1) = 1$ i dla każdego $a \in P$: a jest elementem odwracalnym pierścienia P wtedy i tylko wtedy, gdy $N(a) = 1$.*

Dowód. Ponieważ dla każdego $x \in P$ mamy, że $x = 1 \cdot x$, więc na mocy II, $N(x) = N(1) \cdot N(x)$. Ponadto $P \neq \{0\}$, więc istnieje niezerowe $x \in P$ i wtedy z I, $N(x) \neq 0$, więc po skróceniu $N(1) = 1$.

Weźmy dowolne $a \in P$. Jeśli $a \in P^*$, to $a \cdot b = 1$ dla pewnego $b \in P$, ale $N(1) = 1$, więc na mocy II, $N(a) \cdot N(b) = 1$, skąd $N(a), N(b) \in \mathbb{N}$ i wobec tego $N(a) = 1$. Na odwrót, załóżmy, że $N(a) = 1$. Wtedy na mocy I, $a \neq 0$. Zatem z III, $1 = q \cdot a + r$ dla pewnych $q, r \in P$ takich, że $N(r) < N(a)$. Ponadto $N(r) \in \mathbb{N}_0$ i $N(a) = 1$, więc $N(r) = 0$, skąd $r = 0$ na mocy I. Zatem $1 = q \cdot a$ i $a \in P^*$. □

Twierdzenie 13.24. *Każdy pierścień euklidesowy jest dziedziną ideałów głównych. W szczególności każdy pierścień euklidesowy jest dziedziną z jednoznacznością rozkładu.*

Dowód. Niech P będzie pierścieniem euklidesowym z normą N. Niech I będzie dowolnym ideałem pierścienia P. Jeśli $I = \{0\}$, to $I = (0)$. Niech dalej $I \neq \{0\}$. Wtedy na mocy I dla każdego $a \in I \setminus \{0\}$ mamy, że $N(a) \in \mathbb{N}$. Z zasady minimum w zbiorze $\{N(a) : a \in I \setminus \{0\}\}$ istnieje element najmniejszy $N(a)$. Oczywiście $(a) \subseteq I$. Weźmy dowolne $b \in I$. Wtedy z III istnieją $q, r \in P$ takie, że $b = q \cdot a + r$ i $N(r) < N(a)$. Stąd $q \cdot a \in I$ oraz $r = b - q \cdot a \in I$. Z wyboru a wynika, że $r = 0$. Zatem $b = q \cdot a \in (a)$, czyli $I \subseteq (a)$ i ostatecznie $I = (a)$. Stąd na mocy twierdzenia 13.21 P jest dziedziną z jednoznacznością rozkładu. □

Z twierdzenia o dzieleniu z resztą wynika, że pierścień $\mathbb{Z}$ jest pierścieniem euklidesowym, którego normą jest wartość bezwzględna.

Przykład 13.25. Niech $\omega_D = \sqrt{D}$ dla $D = -2, -1, 2, 3$ i $\omega_{-3} = \frac{1+\sqrt{-3}}{2}$. Pokażemy, że $\mathbb{Z}[\omega_D]$ dla $D = -3, -2, -1, 2, 3$ jest pierścieniem euklidesowym z normą N daną wzorem $N(\alpha) = |N_D(\alpha)|$ dla $\alpha \in \mathbb{Z}[\omega_D]$. Rzeczywiście, warunki I oraz II były pokazane w przykładach 13.6 i 13.7. Pozostaje więc wykazać, że zachodzi warunek III. W tym celu weźmy dowolne $\alpha, \beta \in \mathbb{Z}[\omega_D]$, $\beta \neq 0$. Wtedy α, β należą do ciała $\mathbb{Q}(\sqrt{D})$, więc istnieją liczby wymierne u, v takie, że $\frac{\alpha}{\beta} = u + v\sqrt{D}$. Stąd istnieją $x, y \in \mathbb{Q}$ takie, że $\frac{\alpha}{\beta} = x + y\omega_D$. Niech x_0 będzie liczbą całkowitą najbliższą liczby x i niech y_0 będzie liczbą całkowitą najbliższą liczby y. Wtedy $|x - x_0| \leqslant \frac{1}{2}$ i $|y - y_0| \leqslant \frac{1}{2}$. Określamy $\gamma = x_0 + y_0\omega_D$ i $\rho = \alpha - \gamma \cdot \beta$. Wtedy $\gamma, \rho \in \mathbb{Z}[\omega_D]$, $\alpha = \gamma \cdot \beta + \rho$ oraz $\rho = \alpha - \gamma \cdot \beta = \frac{\alpha}{\beta} \cdot \beta - \gamma \cdot \beta = \beta \cdot (\frac{\alpha}{\beta} - \gamma) = \beta \cdot ((x + y\omega_D) - (x_0 + y_0\omega_D)) = \beta \cdot ((x - x_0) + (y - y_0)\omega_D)$. Stąd na mocy przykładów 13.6 i 13.7, $N(\rho) = N(\beta) \cdot N((x - x_0) + (y - y_0)\omega_D) = N(\beta) \cdot N((x - x_0) + (y - y_0)\omega_D)$. Wystarczy zatem wykazać, że dla dowolnych liczb wymiernych p, q takich, że $|p|, |q| \leqslant \frac{1}{2}$ zachodzi nierówność:

$$N(p + q\omega_D) < 1. \tag{13.18}$$

Jeżeli $D = -2, -1, 2$, to $N(p + q\omega_D) = |p^2 - Dq^2| \leqslant p^2 + |D|q^2 \leqslant \leqslant \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1$. Natomiast dla $D = 3$:

$$N(p + q\omega_D) = |p^2 - Dq^2| = |p^2 - 3q^2| =$$

$$= \begin{cases} p^2 - 3q^2 \leqslant \frac{1}{4} & \text{gdy } p^2 - 3q^2 \geqslant 0 \\ 3q^2 - p^2 \leqslant \frac{3}{4} & \text{gdy } p^2 - 3q^2 < 0 \end{cases}.$$

Zatem także $N(p + q\omega_D) < 1$.

W końcu, dla $D = -3$ jest $D \equiv 1 \pmod 4$, więc z przykładu 13.7, $N(p + q\omega_D) = |p^2 + pq + q^2| \leqslant |p|^2 + |p| \cdot |q| + |q|^2 \leqslant 3 \cdot \frac{1}{4} < 1$.

Przykład 13.26. Niech $D \in \{-7, -11\}$. Udowodnimy, że pierścień $\mathbb{Z}[\omega_D]$, gdzie $\omega_D = \frac{1+\sqrt{D}}{2}$, jest pierścieniem euklidesowym z normą N taką, że $N(\alpha) = N_D(\alpha)$ dla $\alpha \in \mathbb{Z}[\omega_D]$. Rzeczywiście, warunki I oraz II były pokazane w przykładzie 13.7. Pozostaje więc wykazać, że zachodzi warunek III. W tym celu weźmy dowolne $\alpha, \beta \in \mathbb{Z}[\omega_D]$, $\beta \neq 0$. Wtedy

α, β należą do ciała $\mathbb{Q}(\sqrt{D})$, więc istnieją liczby wymierne x, y takie, że $\frac{\alpha}{\beta} = x + y\sqrt{D}$. Niech y_0 będzie liczbą całkowitą najbliższą liczby y. Wtedy $|y - y_0| \leqslant \frac{1}{2}$. Dalej, niech x_0 będzie liczbą całkowitą najbliższą liczby $x + \frac{y-y_0}{2}$. Wtedy $|x - x_0 + \frac{y-y_0}{2}| \leqslant \frac{1}{2}$. Oznaczmy $\gamma = x_0 + y_0\omega_D$. Wtedy $\gamma \in \mathbb{Z}[\omega_D]$ i $\rho = \beta - \gamma \cdot \alpha \in \mathbb{Z}[\omega_D]$ oraz $\beta = \gamma \cdot \alpha + \rho$, więc wystarczy pokazać, że $N_D(\rho) < N_D(\alpha)$. Ponadto $\beta = \frac{\beta}{\alpha} \cdot \alpha = (x + y\omega_D) \cdot \alpha$, więc $\rho = ((x - x_0) + (y - y_0)\omega_D) \cdot \alpha$, skąd $N_D(\rho) = N_D((x - x_0) + +(y - y_0)\omega_D) \cdot N_D(\alpha)$. Wystarczy zatem wykazać, że $N_D((x - x_0) + +(y - y_0)\omega_D) < 1$. Z przykładu 13.7 oraz z nierówności $|y - y_0| \leqslant \frac{1}{2}$ i $|x - x_0 + \frac{y-y_0}{2}| \leqslant \frac{1}{2}$ oraz z założenia, że $D \in \{-7, -11\}$ wynika, że $N_D((x-x_0)+(y-y_0)\omega_D) = ((x-x_0)+\frac{y-y_0}{2})^2+\frac{|D|}{4}(y-y_0)^2 \leqslant \frac{1}{4}+\frac{11}{4}\cdot\frac{1}{4} = = \frac{15}{16} < 1$.

Jeżeli D jest bezkwadratową liczbą naturalną, to rozszerzenie $K = = Q(\sqrt{-D})$ nazywamy **urojonym ciałem kwadratowym**. Element $a \in K$ nazywamy algebraiczną liczbą całkowitą, jeżeli jest on pierwiastkiem pewnego unormowanego wielomianu o współczynnikach całkowitych. Dobrze wiadomo, że zbiór wszystkich algebraicznych liczb całkowitych pierścienia K tworzy pierścień nazywany **pierścieniem liczb algebraicznych całkowitych** i oznaczany przez $\mathcal{O}_K$. Dowód tego faktu można znaleźć w dowolnym podręczniku Algebraicznej Teorii Liczb, na przykład w [27]. Pierścień ten ma szereg interesujących własności, które były i są intensywnie badane przez wielu matematyków.

I tak, na przykład dla niektórych wartości D pierścień $\mathcal{O}_K$ jest dziedziną ideałów głównych. Gauss znalazł 9 takich wartości D, i podejrzewał, że innych nie ma. Dopiero w połowie XX wieku okazało się, że miał rację. Mówi o tym następujące twierdzenie.

Twierdzenie 13.27. [Stark–Heegner] *Jeżeli D jest bezkwadratową liczbą naturalną, to pierścień $\mathcal{O}_K$ jest dziedziną ideałów głównych wtedy i tylko wtedy, gdy:*

$$D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Liczby występujące w poprzednim twierdzeniu nazywamy **liczbami Heegnera**. Pierwszy dowód twierdzenia 13.27 podał Heegener

w 1952, ale jego rozumowanie zawierało lukę, którą w 1967 uzupełnił Stark. O historii twierdzenia Starka-Heegnera, innych jego dowodach, a także o związkach z różnymi działami matematyki można przeczytać w przeglądowym artykule [17]. Znajduje się tam także bogata kolekcja referencji do omawianego tematu.

Część V

Zastosowania pierścieni w teorii równań diofantycznych

Rozdział 14

Pierścień liczb całkowitych Gaussa

14.1 Klasyfikacja elementów pierwszych

Z przykładu 13.25 wiemy, że $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ jest pierścieniem euklidesowym z normą N daną wzorem $N(x+yi) = x^2+y^2$ dla $x, y \in \mathbb{Z}$. Wobec tego na mocy twierdzeń 13.15 i 13.24 w pierścieniu $\mathbb{Z}[i]$ pojęcia elementu pierwszego i elementu nierozkładalnego pokrywają się.

Ze wzoru (13.10) wiemy, że $(\mathbb{Z}[i])^* = \{1, -1, i, -i\}$. Zatem na mocy stwierdzenia 13.2 dla dowolnego niezerowego $\alpha \in \mathbb{Z}[i]$ istnieją dokładnie cztery liczby całkowite Gaussa stowarzyszone z α i są nimi: $\alpha, -\alpha, i \cdot \alpha, -i \cdot \alpha$.

Stwierdzenie 14.1. *Dla każdej liczby całkowitej Gaussa $\alpha \neq 0$ istnieje dokładnie jedna stowarzyszona z α liczba całkowita Gaussa $a + bi$ taka, że $a \in \mathbb{N}$ i $b \in \mathbb{N}_0$.*

Dowód. Niech $\alpha \in \mathbb{Z}[i] \setminus \{0\}$. Wtedy $\alpha = x + yi$ dla pewnych $x, y \in \mathbb{Z}$, przy czym $x \neq 0$ lub $y \neq 0$. Jeśli $x = 0$ i $y > 0$, to $\alpha \cdot (-i) = y$, więc $\alpha \sim y$. Jeśli $x = 0$ i $y < 0$, to $\alpha \cdot i = -y$, skąd $\alpha \sim -y$. Niech dalej $x \neq 0$. Jeśli $y = 0$ i $x > 0$, to $\alpha \sim x$, a jeśli $y = 0$ i $x < 0$, to $\alpha \sim -x$.

Niech dalej $x \neq 0$ i $y \neq 0$. Jeśli $x, y > 0$, to wystarczy obrać $a = x$ i $b = y$. Jeśli $x > 0$ i $y < 0$, to $\alpha \cdot i = (-y) + xi$, więc $a = -y$ i $b = x$.

Jeśli $x < 0$ i $y < 0$, to $\alpha \cdot (-1) = (-x) + (-y)i$, więc $a = -x$ i $b = -y$. W końcu, jeśli $x < 0$ i $y > 0$, to $\alpha \cdot (-i) = y + (-x)i$, więc $a = y$ i $b = -x$.

Niech teraz $a, c \in \mathbb{N}$ i $b, d \in \mathbb{N}_0$ będą takie, że $a+bi \sim c+di$. Wtedy $c + di \in \{a + bi, -a - bi, -b + ai, b - ai\}$, skąd $c + di = a + bi$. □

Wniosek 14.2. *Liczby całkowite Gaussa $a + bi$ oraz $a - bi$, gdzie $a, b \in \mathbb{N}$ są stowarzyszone wtedy i tylko wtedy, gdy $a = b$.*

Dowód. Ponieważ $(a - bi) \cdot i = b + ai$, więc $a - bi \sim b + ai$. Zatem $a+bi \sim a-bi \iff a+bi \sim b+ai$ i na mocy stwierdzenia 14.1 mamy tezę. □

Stwierdzenie 14.3. *Jeżeli n jest liczbą naturalną nieparzystą, to każdy element odwracalny pierścienia $\mathbb{Z}[i]$ jest n-tą potęgą pewnego elementu odwracalnego w $\mathbb{Z}[i]$.*

Dowód. Ponieważ liczba n jest nieparzysta, więc $-1 = (-1)^n$ i oczywiście $1 = 1^n$. Dalej, $i^2 = -1$, więc $i^3 = -i$ oraz $i^4 = 1$. Stąd $i^{4k} = 1$ dla każdego $k \in \mathbb{N}_0$. Dodatkowo $n = 4k + 1$ lub $n = 4k + 3$, więc w pierwszym przypadku $i = i^n$ oraz $-i = (-i)^n$, a w drugim $i = (-i)^n$ oraz $-i = i^n$. Ponadto $(\mathbb{Z}[i])^* = \{1, -1, i, -i\}$. Zatem teza została udowodniona. □

Uwaga 14.4. Pokażemy teraz zastosowanie pierścienia $\mathbb{Z}[i]$ do udowodnienia twierdzenia Fermata o dwóch kwadratach. Niech p będzie dowolną liczbą pierwszą postaci $4k + 1$. Na mocy twierdzenia 7.25 istnieje $c \in \mathbb{N}$ takie, że $p \mid c^2 + 1$. Ponadto $c^2 + 1 = (c + i)(c - i)$, więc $p \mid (c+i)(c-i)$ w pierścieniu $\mathbb{Z}[i]$. Dalej, na mocy (13.3), $p \nmid c+i$ oraz $p \nmid c - i$. Ponadto $p \neq 0$ i p nie jest elementem odwracalnym w $\mathbb{Z}[i]$. Z twierdzeń 13.15 i 13.24 wynika, że $p = \alpha \cdot \beta$ dla pewnych niezerowych elementów nieodwracalnych α i β pierścienia $\mathbb{Z}[i]$. Zatem na mocy stwierdzenia 13.23, $N(\alpha), N(\beta) \neq 1$ i $p^2 = N(\alpha) \cdot N(\beta)$. Stąd $N(\alpha) = p$. Dodatkowo $\alpha = x+yi$ dla pewnych $x, y \in \mathbb{Z}$, więc $x^2+y^2 = p$. Z pierwszości liczby p wynika, że $x, y \neq 0$, więc $|x|, |y| \in \mathbb{N}$ i $p = |x|^2 + |y|^2$.

Stwierdzenie 14.5. *Dla każdej liczby pierwszej p postaci $4k + 1$ istnieje dokładnie jedna para (a, b) liczb naturalnych taka, że $a > b$ i $p = a^2 + b^2$.*

Dowód. Istnienie takiej pary wynika z nieparzystości p oraz z twierdzenia Fermata o dwóch kwadratach. Załóżmy, że (c, d) jest parą liczb naturalnych taką, że $c^2 + d^2 = p$ oraz $c > d$. Wtedy w pierścieniu euklidesowym $\mathbb{Z}[i]$ elementy $a+bi$, $a-bi$, $c+di$ oraz $c-di$ mają normę p, więc na mocy przykładu 13.12 i twierdzenia 13.15 są one elementami pierwszymi pierścienia $\mathbb{Z}[i]$. Ponadto $p = (a + bi)(a - bi) = (c + di)(c - di)$, więc $c+di \mid a+bi$ lub $c+di \mid a-bi$, skąd $c+di \sim a+bi$ lub $c+di \sim a-bi$. Dodatkowo $a-bi = (b+ai)\cdot(-i)$, więc $c+di \sim a+bi$ lub $c+di \sim b+ai$ i na mocy stwierdzenia 14.1, $c + di = a + bi$ lub $c + di = b + ai$, skąd $(c, d) = (a, b)$, gdyż $(c, d) \neq (b, a)$, bo $c > d$ i $a > b$. □

Twierdzenie 14.6. *Wszystkimi z dokładnością do stowarzyszenia elementami pierwszymi pierścienia $\mathbb{Z}[i]$ są: $1 + i$, liczby pierwsze q postaci $4k + 3$ i liczby zespolone postaci $a + bi$ oraz $a - bi$, gdzie $a > b$, $a, b \in \mathbb{N}$ i $a^2 + b^2$ jest liczbą pierwszą postaci $4k + 1$.*

Dowód. Jak wiemy w pierścieniu $\mathbb{Z}[i]$ elementy pierwsze pokrywają się z elementami nierozkładalnymi. Wystarczy zatem opisać elementy nierozkładalne tego pierścienia.

Ponieważ $N(1 + i) = 1^2 + 1^2 = 2 \in \mathbb{P}$ oraz dla $a, b \in \mathbb{N}$ takich, że $a > b$ i $a^2 + b^2 \in \mathbb{P}$ jest $N(a + bi) = N(a - bi) = a^2 + b^2$, więc na mocy przykładu 13.12, $1+i$, $a+bi$ oraz $a-bi$ są elementami nierozkładalnymi w $\mathbb{Z}[i]$ oraz na mocy stwierdzeń 14.1 i 14.2 żadne dwa z tych elementów nie są stowarzyszone. Niech q będzie liczbą pierwszą postaci $4k + 3$. Oczywiście $q \neq 0$ i $q \notin \{1, -1, i, -i\}$. Jeżeli $x, y \in \mathbb{Z}$ i $N(x+yi) = q$, to $x^2 + y^2 = q$, co przeczy stwierdzeniu 4.1. Zatem $q \neq N(\alpha)$ dla każdego $\alpha \in \mathbb{Z}[i]$. Weźmy dowolne $\alpha, \beta \in \mathbb{Z}[i]$ takie, że $q = \alpha \cdot \beta$. Wtedy $q^2 = N(\alpha) \cdot N(\beta)$, a ponieważ $N(\alpha), N(\beta) \in \mathbb{N}$ oraz $N(\alpha), N(\beta) \neq q$, więc $N(\alpha) = 1$ lub $N(\beta) = 1$, skąd na mocy przykładu 13.12, α lub β jest elementem odwracalnym w $\mathbb{Z}[i]$. Wobec tego q jest elementem nierozkładalnym w $\mathbb{Z}[i]$, przy czym na mocy (13.3), $q \nmid 1 + i$ oraz $q \nmid a + bi$ i $q \nmid a - bi$, gdy $a^2 + b^2$ jest liczbą pierwszą postaci $4k + 1$.

Niech teraz π będzie elementem nierozkładalnym w $\mathbb{Z}[i]$. Wtedy π jest elementem pierwszym w $\mathbb{Z}[i]$ i $N(\pi) > 1$ jest liczbą naturalną. Zatem $N(\pi) = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ dla pewnych liczb pierwszych $p_1, p_2, \ldots, p_s$. Ponadto $N(\pi) = \pi \cdot \overline{\pi}$, więc $\pi \mid p_1 \cdot p_2 \cdot \ldots \cdot p_s$ i z pierwszości elementu π,

$\pi \mid p_j$ dla pewnego $j = 1, \ldots, s$. Jeśli $p_j = 2$, to $\pi \mid 2i = (1+i)^2$, skąd $\pi \mid 1+i$, więc z pierwszej części dowodu $\pi \sim 1+i$. Jeżeli $p_j \equiv 3 \pmod 4$, to z pierwszej części dowodu $\pi \sim p_j$. Niech zatem $p_j \equiv 1 \pmod 4$. Wtedy na mocy stwierdzenia 14.5 istnieje dokładnie jedna para (a_j, b_j) liczb naturalnych taka, że $a_j > b_j$ oraz $p_j = a_j^2 + b_j^2 = (a_j + b_j i)(a_j - b_j i)$. Z pierwszości elementu π wynika, że $\pi \mid a_j + b_j i$ lub $\pi \mid a_j - b_j i$. Stąd i z pierwszej części dowodu $\pi \sim a_j + b_j i$ lub $\pi \sim a_j - b_j i$, co kończy dowód. □

Oznaczmy przez $\mathbb{G}$ (na cześć Gaussa) zbiór elementów pierwszych pierścienia $\mathbb{Z}[i]$ podany w twierdzeniu 14.6. Ponieważ $\mathbb{Z}[i]$ jest dziedziną z jednoznacznością rozkładu i $(\mathbb{Z}[i])^* = \{1, -1, i, -i\}$, więc uzyskujemy stąd następujące

Twierdzenie 14.7. *Każda niezerową liczbę całkowitą Gaussa taką, że $\alpha \neq 1, -1, i, -i$ można zapisać jednoznacznie w postaci*

$$\alpha = \varepsilon \cdot \pi_1^{k_1} \cdot \ldots \cdot \pi_s^{k_s},$$

gdzie $\varepsilon \in \{1, -1, i, -i\}$, $s, k_1, \ldots, k_s \in \mathbb{N}$ oraz $\pi_1, \ldots, \pi_s$ są różnymi elementami ze zbioru $\mathbb{G}$. □

Stwierdzenie 14.8. *Niech a i b będą liczbami naturalnymi takimi, że $p = a^2 + b^2 \in \mathbb{P}$. Wtedy dla dowolnych $x, y \in \mathbb{Z}$ równoważne są warunki:*

(i) $a + bi \mid x + yi$ w pierścieniu $\mathbb{Z}[i]$,

(ii) $ay \equiv bx \pmod p$.

Dowód. Zauważmy, że w ciele $\mathbb{Q}(i)$: $\frac{x+yi}{a+bi} = \frac{(x+yi)(a-bi)}{(a+bi)(a-bi)} = \frac{ax+by}{p} + \frac{ay-bx}{p} i$. Wobec tego $a + bi \mid x + yi$ w pierścieniu $\mathbb{Z}[i]$ wtedy i tylko wtedy, gdy $ax + by \equiv 0 \pmod p$ i $ay - bx \equiv 0 \pmod p$. Stąd mamy implikację $(i) \Rightarrow (ii)$.

Na odwrót, niech $ay \equiv bx \pmod p$. Wtedy $a^2 y \equiv abx \pmod p$, ale $a^2 \equiv -b^2 \pmod p$, więc $-b^2 y \equiv abx \pmod p$. Ponieważ $p \in \mathbb{P}$ i $a^2 + b^2 = p$, więc $p \nmid b$ i po skróceniu otrzymanej kongduencji przez b uzyskamy, że $ax \equiv -by \pmod p$, czyli $ax + by \equiv 0 \pmod p$. Stąd i z pierwszej części dowodu $a + bi \mid x + yi$ w pierścieniu $\mathbb{Z}[i]$. □

Stosując stwierdzenie 14.8 dla $a = b = 1$ uzyskujemy od razu następujące

Stwierdzenie 14.9. *Liczba całkowita Gaussa $a+bi$, gdzie $a, b \in \mathbb{Z}$ jest podzielna przez $1+i$ wtedy i tylko wtedy, gdy $a \equiv b \pmod 2$.*

Ponieważ $a-bi \sim (a-bi)\cdot i = b+ai$ dla $a, b \in \mathbb{N}$, więc ze stwierdzenia 14.8 uzyskujemy od razu następujące

Stwierdzenie 14.10. *Niech a i b będą liczbami naturalnymi takimi, że $p = a^2 + b^2 \in \mathbb{P}$. Wtedy dla dowolnych $x, y \in \mathbb{Z}$ równoważne są warunki:*

(i) $a - bi \mid x + yi$ w pierścieniu $\mathbb{Z}[i]$,

(ii) $by \equiv ax \pmod p$.

Zadanie 14.11. W pierścieniu liczb całkowitych Gaussa wyprowadź cechy podzielności przez liczby: $2 + i$, $2 - i$, $3 + 2i$ oraz $3 - 2i$.

Stwierdzenie 14.12. *Dla dowolnych liczb całkowitych a i b równoważne są warunki:*

(i) liczby a i b są względnie pierwsze i mają różną parzystość,

(ii) liczby całkowite Gaussa $a+bi$ oraz $a-bi$ są względnie pierwsze.

Dowód. $(i) \Rightarrow (ii)$. Przypuśćmy, że tak nie jest. Wtedy istnieje element pierwszy π pierścienia $\mathbb{Z}[i]$ taki, że $\pi \mid a+bi$ oraz $\pi \mid a-bi$. Stąd $\pi \mid 2a$ oraz $\pi \mid 2b$, bo $2a = (a + bi) + (a - bi)$ i $2bi = (a + bi) - (a - bi)$ oraz $i \in (\mathbb{Z}[i])^*$. Na mocy twierdzenia 1.11, $ak+bl = 1$ dla pewnych $k, l \in \mathbb{Z}$. Zatem $2 = 2ak + 2bl$, skąd $\pi \mid 2$, ale $2 \sim 2i = (1 + i)^2$, więc $\pi \mid 1 + i$. Z twierdzenia 14.6 mamy, że $\pi \sim 1 + i$. Zatem $1 + i \mid a + bi$, skąd na mocy stwierdzenia 14.9 uzyskujemy, że $a \equiv b \pmod 2$, co przeczy temu, że a i b są różnej parzystości. Wobec tego elementy $a + bi$ oraz $a - bi$ są względnie pierwsze w pierścieniu $\mathbb{Z}[i]$.

$(ii) \Rightarrow (i)$. Ponieważ $\mathrm{NWD}(a, b)$ dzieli $a + bi$ oraz $a - bi$, więc $d \in \{1, -1, i, -i\}$, skąd $\mathrm{NWD}(a, b) = 1$. Jeżeli liczby a i b są tej samej parzystości, to $a \equiv b \pmod 2$, skąd $a \equiv -b \pmod 2$ i na mocy stwierdzenia 14.9, $1+i \mid a+bi$ oraz $1+i \mid a-bi$, skąd $1+i \in \{1, -1, i, -i\}$, co prowadzi do sprzeczności. Zatem liczby a i b są różnej parzystości. $\square$

Przykład 14.13. Zilustrujemy teraz algorytm zapisywania liczb całkowitych Gaussa w postaci podanej w twierdzeniu 14.6 na przykładzie $\alpha = -126 + 306i$.

Najpierw obliczamy $\mathrm{NWD}(-126, 306) = 18$, więc $\alpha = 18(-7+17i)$. Następnie rozkładamy liczbę 18 naczynniki pierwsze: $18 = 2 \cdot 3^2$. Ponadto $2 = (1+i)^2 \cdot (-i)$ oraz $1+i$ i 3 są elementami pierwszymi pierścienia $\mathbb{Z}[i]$, więc $18 = (-i) \cdot (1+i)^2 \cdot 3^2$ jest rozkładem liczby 18 w postaci podanej w twierdzeniu 14.6. Liczby -7 i 17 są względnie pierwsze i $-7 \equiv 17 \pmod 2$, więc $1 + i \mid -7 + 17i$ na mocy stwierdzenia 14.9. Obliczamy $\frac{-7+17i}{1+i} = 5 + 12i$, skąd $\alpha = (-i) \cdot (1+i)^3 \cdot 3^2 \cdot (5+12i)$.

Teraz obliczamy $N(5 + 12i) = 5^2 + 12^2 = 169 = 13^2$. Ponieważ $13 = (3+2i)(3-2i)$, więc badamy przy pomocy stwierdzenia 14.8, czy $3 + 2i \mid 5 + 21i$: $3 \cdot 12 - 2 \cdot 5 = 2 \cdot 13$, więc $3 + 2i \mid 5 + 12i$. Obliczamy $\frac{5+12i}{3+2i} = 3+2i$. Stąd ostatecznie: $-126+306i = (-i)\cdot(1+i)^3\cdot 3^2\cdot(3+2i)^2$.

Zadanie 14.14. Przedstaw w postaci podanej w twierdzeniu 14.13 następujące liczby całkowite Gaussa: $7 + 17i$, $8 - 14i$, $-39 + 48i$.

Zadanie 14.15. W pierścieniu liczb całkowitych Gaussa wykonaj dzielenie z resztą elementu $\beta = 27 - 23i$ przez element $\alpha = 8 + 3i$.

Zadanie 14.16. Udowodnij, że $1+i \mid \alpha$ albo $1+i \mid \alpha-1$ dla każdej liczby całkowitej Gaussa α.

14.2 Sumy kwadratów dwóch liczb całkowitych

Stwierdzenie 14.17. *Jeżeli liczby naturalne $a_1, a_2, \ldots, a_n$ są sumami kwadratów dwóch liczb całkowitych, to ich iloczyn też jest sumą kwadratów dwóch liczb całkowitych.*

Dowód. Z założenia istnieją $x_k, y_k \in \mathbb{Z}$ takie, że $a_k = x_k^2 + y_k^2$ dla każdego $k = 1, 2, \ldots, n$. Jak wiemy, $\mathbb{Z}[i]$ jest pierścieniem euklidesowym z normą N daną wzorem $N(x+yi) = x^2+y^2$ dla $x, y \in \mathbb{Z}$. W $\mathbb{Z}[i]$ mamy, że $\alpha = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n \in \mathbb{Z}[i]$, gdzie $\alpha_k = x_k + y_k i$ dla $k = 1, 2, \ldots, n$. Zatem $\alpha = x + yi$ dla pewnych $x, y \in \mathbb{Z}$ oraz z (13.4) przez prostą

indukcję uzyskujemy, że $N(\alpha) = N(\alpha_1) \cdot N(\alpha_2) \cdot \ldots \cdot N(\alpha_n)$. Ponadto $N(\alpha_k) = x_k^2 + y_k^2 = a_k$ dla $k = 1, 2, \ldots, n$ oraz $N(\alpha) = x^2 + y^2$. Wobec tego $x^2 + y^2 = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, co kończy dowód. □

Twierdzenie 14.18. *Liczba naturalna n jest sumą kwadratów dwóch liczb całkowitych wtedy i tylko wtedy, gdy $n = 1$ lub $n > 1$ i w rozkładnie kanonicznym n nie występuje liczba pierwsza postaci $4k + 3$ w nieparzystym wykładniku.*

Dowód. Zauważmy, że $1 = 0^2 + 1^2$. Ponadto każda liczbę naturalną $n > 1$ można zapisać w postaci kanonicznej. Załóżmy, że w tym zapisie nie ma liczb pierwszych postaci $4k+3$ lub każda liczba pierwsza postaci $4k + 3$ występująca w tym zapisie ma wykładnik parzysty. Ponieważ dla $q, s \in \mathbb{N}$ jest $q^{2s} = 0^2 + (q^s)^2$, $2 = 1^2 + 1^2$ oraz z twierdzenia Fermata o dwóch kwadratach każda liczba pierwsza postaci $4k + 1$ jest sumą kwadratów dwóch liczb całkowitych, więc na mocy stwierdzenia 14.17 liczba n jest sumą kwadratów dwóch liczb całkowitych.

Gdyby implikacja odwrotna była fałszywa istniałyby: liczba pierwsza q postaci $4k + 3$ oraz liczby naturalne t, m i liczby całkowite x, y takie, że $q^{2t+1}m = x^2 + y^2$ oraz $q \nmid m$. Wtedy można zakładać, że t jest najmniejsze i na mocy stwierdzenia 2.15, $x = qx_1$ oraz $y = qy_1$ dla pewnych $x_1, y_1 \in \mathbb{Z}$, skąd po skróceniu przez q^2, $q^{2(t-1)+1}m = x_1^2 + y_1^2$ i mamy sprzeczność z minimalnością t. □

Twierdzenie 14.19. (Eulera). *Liczba naturalna n jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych wtedy i tylko wtedy, gdy $n = 1$ lub $n = 2$ lub $n > 2$ i w rozkładnie kanonicznym n nie występuje żadna liczba pierwsza postaci $4k + 3$, zaś wykładnik liczby 2 jest nie większy niż 1.*

W szczególności, każdy naturalny dzielnik liczby będącej sumą kwadratów dwóch względnie pierwszych liczb całkowitych także jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych.

Dowód. Zauważmy, że $1 = 0^2 + 1^2$ i $2 = 1^2 + 1^2$ oraz $\mathrm{NWD}(0, 1) = \mathrm{NWD}(1, 1) = 1$. Niech teraz $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ dla pewnych liczb pierwszych $p_1, p_2, \ldots, p_s$ postaci $4k+1$. Z twierdzenia Fermata o dwóch kwadratach dla każdego $k = 1, 2, \ldots, s$ istnieją liczby naturalne a_k, b_k

takie, że $a_k > b_k$ oraz $p_k = a_k^2 + b_k^2$. Stąd z pierwszości p_k mamy, że $\mathrm{NWD}(a_k, b_k) = 1$ dla $k = 1, 2, \ldots, s$. Istnieją $x, y \in \mathbb{Z}$ takie, że $x + yi = (a_1 + b_1 i) \cdot (a_2 + b_2 i) \cdot \ldots \cdot (a_s + b_s i)$ w pierścieniu liczb całkowitych Gaussa. Ze wzoru (13.4) przez prostą indukcję uzyskujemy, że $N(x + yi) = N(a_1 + b_1 i) \cdot N(a_2 + b_2 i) \cdot \ldots \cdot N(a_s + b_s i)$, skąd $x^2 + y^2 = (a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2) \cdot \ldots \cdot (a_s^2 + b_s^2) = p_1 \cdot p_2 \cdot \ldots \cdot p_s$, a więc $n = x^2 + y^2$. Jeśli $\mathrm{NWD}(x, y) > 1$, to istnieje liczba pierwsza p taka, że $p \mid x$ i $p \mid y$, skąd $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Wobec tego $p \mid p_k$, skąd $p = p_k$ dla pewnego $k = 1, 2, \ldots, s$. Ponadto $p = (a_k + b_k i)(a_k - b_k i)$, więc w pierścieniu $\mathbb{Z}[i]$, $a_k - b_k i \mid (a_1 + b_1 i) \cdot (a_2 + b_2 i) \cdot \ldots \cdot (a_s + b_s i)$. Na mocy przykładu 14.6, $a_k - b_k i$ oraz $a_1 + b_1 i, a_2 + b_2 i, \ldots, a_s + b_s i$ są elementami pierwszymi w $\mathbb{Z}[i]$, więc $a_k - b_k i \sim a_j + b_j i$ dla pewnego $j = 1, 2, \ldots, s$ i otrzymujemy sprzeczność z twierdzeniem 14.6. Wobec tego liczby całkowite x i y są względnie pierwsze. Ponadto n jest liczbą nieparzystą jako iloczyn liczb nieparzystych, więc liczby x i y są różnej parzystości, skąd 2 nie dzieli $x - y$. Jeśli liczby $x - y$ i $x + y$ nie są względnie pierwsze, to istnieje liczba pierwsza q taka, że $q \mid x + y$ i $q \mid x - y$. Stąd $q \neq 2$ oraz $q \mid (x + y) + (x - y)$ i $q \mid (x + y) - (x - y)$, czyli $q \mid 2x$ i $q \mid 2y$. Zatem $q \mid x$ i $q \mid y$, co prowadzi do sprzeczności. Wobec tego liczby $x + y$ i $x - y$ są wzgędnie pierwsze. Ponadto $(x + y)^2 + (x - y)^2 = x^2 + 2xy + y^2 + x^2 - 2xy + y^2 = 2(x^2 + y^2) = 2n$, co oznacza, że liczba $2n$ też jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych.

Na odwrót, załóżmy, że liczba naturalna $n > 2$ jest sumą kwadratów dwóch względnie pierwszych liczb całkowitych x i y. Jeśli istnieje liczba pierwsza q postaci $4k + 3$ dzieląca n, to ze stwierdzenia 2.15, $q \mid x$ i $q \mid y$, co przeczy temu, że $\mathrm{NWD}(x, y) = 1$. Wobec tego w rozkładzie kanonicznym liczby n nie występuje żadna liczba pierwsza postaci $4k + 3$. Załóżmy, że $4 \mid n$. Wtedy $4 \mid x^2 + y^2$, więc $x^2 + y^2$ jest liczbą parzystą i liczby x i y nie moga być obie jednocześnie liczbami parzystymi (bo są one względnie pierwsze). Stąd liczby x i y są nieparzyste, a zatem $x^2 \equiv 1 \pmod 4$ i $y^2 \equiv 1 \pmod 4$, skąd $x^2 + y^2 \equiv 2 \pmod 4$, co przeczy temu, że $4 \mid x^2 + y^2$. Wobec tego 4 nie dzieli n, a zatem liczba 2 wchodzi w rozkład liczby n na czynniki pierwsze z wykładnikiem nie większym niż 1.

Ostatnia część naszego twierdzenia wynika od razu z pierwszej czę-

ści naszego dowodu, gdyż dzielniki naturalne liczb n opisanych w treści twierdzenia są takiej samej postaci jak n. □

W twierdzeniu 14.18 podano warunki konieczne i dostateczne na to, aby dla ustalonej liczby naturalnej n równanie diofantyczne:

$$x^2 + y^2 = n \tag{14.1}$$

miało rozwiązanie. W związku z tym powstaje naturalne pytanie o liczbę wszystkich rozwiązań tego równania, czyli o liczbę elementów zbioru $R(n) = \{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 = n\}$. Weźmy dowolne $(x, y) \in R(n)$. Wtedy $x + yi \in \mathbb{Z}[i]$ oraz $(x + yi)(x - yi) = n$. Zatem $\alpha = x + yi$ jest dzielnikiem liczby n takim, że $\overline{\alpha} = x - yi$ jest dzielnikiem dopełniającym dla α. Na odwrót, niech $\alpha \in \mathbb{Z}[i]$ będzie dzielnikiem liczby n takim, że $\alpha \cdot \overline{\alpha} = n$. Wtedy $\alpha = x + yi$ dla pewnych $x, y \in \mathbb{Z}$ oraz $\overline{\alpha} = x - yi$, więc $n = (x + yi)(x - yi) = x^2 + y^2$, skąd $(x, y) \in R(n)$. Wobec tego zbiór $R(n)$ jest wyznaczony przez takie dzielniki α liczby n w pierścieniu $\mathbb{Z}[i]$, że $\alpha \cdot \overline{\alpha} = n$ i liczba elementów zbioru $R(n)$ jest równa liczbie wszystkich takich dzielników α liczby n.

Na mocy twierdzenia 14.18 istnieją różne liczby pierwsze $p_1, \ldots, p_s$ postaci $4k + 1$ oraz różne liczby pierwsze $q_1, \ldots, q_r$ postaci $4k + 3$ i nieujemne liczby całkowite $k, k_1, \ldots, k_s, l_1, \ldots, l_r$ takie, że

$$n = 2^k \cdot p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} \cdot q_1^{2l_1} \cdot \ldots \cdot q_r^{2l_r}.$$

Ponadto, na mocy twierdzenia 14.7 dla każdego $j = 1, \ldots, s$ istnieją liczby naturalne a_j i b_j takie, że $a_j > b_j$ oraz $a_j^2 + b_j^2 = p_j$. Niech $\pi_j = a_j + b_j i$ dla $j = 1, \ldots, s$. Wtedy $p_j = \pi_j \cdot \overline{\pi_j}$. Ponadto $2 \sim (1+i)^2$, więc w pierścieniu $\mathbb{Z}[i]$:

$$n \sim (1 + i)^{2k} \cdot \pi_1^{k_1} \cdot \ldots \cdot \pi_s^{k_s} \cdot \overline{\pi_1}^{k_1} \cdot \ldots \cdot \overline{\pi_s}^{k_s} \cdot q_1^{2l_1} \cdot \ldots \cdot q_r^{2l_r}.$$

Stąd na mocy twierdzenia 14.7 dzielnik α liczby n spełnia warunek:

$$\alpha \sim (1 + i)^K \cdot \pi_1^{K_1} \cdot \ldots \cdot \pi_s^{K_s} \cdot \overline{\pi_1}^{M_1} \cdot \ldots \cdot \overline{\pi_s}^{M_s} \cdot q_1^{L_1} \cdot \ldots \cdot q_r^{L_r},$$

gdzie nieujemne wykładniki spełniają nierówności: $K \leqslant 2k$, $K_j \leqslant k_j$ oraz $M_j \leqslant k_j$ dla $j = 1, \ldots, s$, $L_j \leqslant 2l_j$ dla $j = 1, \ldots, r$.

Wobec tego z własności sprzęgania liczb zespolonych i tego, że $1-i \sim 1+i$:

$$\overline{\alpha} \sim (1+i)^K \cdot \overline{\pi_1}^{K_1} \cdot \ldots \cdot \overline{\pi_s}^{K_s} \cdot \pi_1^{M_1} \cdot \ldots \cdot \pi_s^{M_s} \cdot q_1^{L_1} \cdot \ldots \cdot q_r^{L_r}.$$

Stąd

$$\alpha \cdot \overline{\alpha} \sim (1+i)^{2K} \cdot \pi_1^{K_1+M_1} \cdot \ldots \cdot \pi_s^{K_s+M_s} \cdot \overline{\pi_1}^{K_1+M_1} \cdot \ldots \cdot \overline{\pi_s}^{K_s+M_s} \cdot q_1^{2L_1} \cdot \ldots \cdot q_r^{2L_r}.$$

Ponadto $\alpha \cdot \overline{\alpha} \sim n$, więc na mocy twierdzenia 14.7: $2K = 2k$, $K_j + M_j = k_j$ dla $j = 1, \ldots, s$ oraz $2L_j = 2l_j$ dla $j = 1, \ldots, r$. Stąd $K = k$ i dla $j = 1, \ldots, s$: $K_j \leqslant k_j$ i $M_j = k_j - K_j$ oraz $L_j = l_j$ dla $j = 1, \ldots, r$.

Wobec tego ostatecznie otrzymujemy, że

$$\alpha = \varepsilon \cdot (1+i)^k \cdot \pi_1^{K_1} \cdot \ldots \cdot \pi_s^{K_s} \cdot \overline{\pi_1}^{k_1-K_1} \cdot \ldots \cdot \overline{\pi_s}^{k_s-K_s} \cdot q_1^{l_1} \cdot \ldots \cdot q_r^{l_r}, \quad (14.2)$$

gdzie $\varepsilon \in \{1, -1, i, -i\}$ oraz $0 \leqslant K_j \leqslant k_j$ dla $j = 1, \ldots, s$.

Ponadto, $\varepsilon \cdot \overline{\varepsilon} = 1$ dla każdego $\varepsilon \in \{1, -1, i, -i\}$, więc z własności sprzęgania liczb zespolonych dla takiego α mamy, że $\alpha \cdot \overline{\alpha} = n$.

Zatem na mocy twierdzenia 14.7 uzyskujemy z tych rozważań, że $|R(n)| = 4 \cdot (k_1+1) \cdot \ldots \cdot (k_s+1)$ oraz dzięki wzorowi (14.2) możemy wypisać wszystkie elementy zbioru $R(n)$. W szczególności udowodniliśmy następujące twierdzenie Gaussa:

Twierdzenie 14.20. *Niech n będzie liczbą naturalną taką, że $n = 1$ lub $n > 1$ i w rozkładnie kanonicznym n nie występuje liczba pierwsza postaci $4k+3$ w nieparzystym wykładniku. Jeżeli liczba n nie posiada dzielnika pierwszego postaci $4k+1$, to równanie diofantyczne* (14.1) *posiada dokładnie cztery rozwiązania, a jeżeli liczba n posiada dokładnie $s \in \mathbb{N}$ różnych dzielników pierwszych postaci $4k+1$ wchodzących w jej rozkład kanoniczny z wykładnikami $k_1, \ldots, k_s$, to liczba rozwiązań równania diofantycznego* (14.1) *jest równa $4 \cdot (k_1+1) \cdot \ldots \cdot (k_s+1)$.*

Przykład 14.21. Stosując podaną wyżej metodę wyznaczymy wszystkie rozwiązania równania diofantycznego $x^2 + y^2 = 4050$. Ponieważ $4050 = 2 \cdot 5^2 \cdot 3^2$, więc na mocy twierdzenia 14.20 to równanie

posiada dokładnie $4 \cdot (2+1) = 12$ rozwiązań w liczbach całkowitych. Wzór (14.2) przybiera zatem postać:

$$\alpha = \varepsilon \cdot (1+i) \cdot (2+i)^k \cdot (2-i)^{2-k} \cdot 3^2$$

dla $\varepsilon \in \{1, -1, i, -i\}$ oraz $k = 0, 1, 2$. Dla $k = 0$ uzyskamy, że $\alpha \in \{63 - 9i, -63 + 9i, 9 + 63i, -9 - 63i\}$. Dla $k = 1$ mamy, że $\alpha \in \{45 + 45i, -45 - 45i, -45 + 45i, 45 - 45i\}$. Natomiast dla $k = 2$: $\alpha \in \{-9 + 63i, 9 - 63i, -63 - 9i, 63 + 9i\}$. Wobec tego wszystkimi rozwiązaniami równania diofantycznego $x^2 + y^2 = 4050$ są: $(63, -9)$, $(-63, 9)$, $(9, 63)$, $(-9, -63)$, $(45, 45)$, $(-45, -45)$, $(-45, 45)$, $(45, -45)$, $(-9, 63)$, $(9, -63)$, $(-63, -9)$ i $(63, 9)$.

Zadanie 14.22. Wyznacz wszystkie rozwiązania równania diofantycznego $x^2 + y^2 = 19890$.

14.3 Twierdzenie Lebesgue'a

Przedstawimy teraz dowód twierdzenia Lebesgue'a oparty na udowodnionych przez nas wcześniej własnościach pierścienia euklidesowego $\mathbb{Z}[i]$. Rozpoczynamy od wykazania następującego lematu.

Lemat 14.23. *Jeżeli liczby naturalne x i y oraz nieparzyste $n > 1$ spełniają równanie*

$$y^2 + 1 = x^n, \tag{14.3}$$

to istnieje parzysta liczba naturalna c taka, że

$$\sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k} c^{2k} = 1. \tag{14.4}$$

Dowód. Jeżeli y jest liczbą nieparzystą, to x musi być liczbą parzystą, skąd $4 \mid x^n$, bo $n > 1$. Zatem $4 \mid y^2 + 1$, ale $y^2 \equiv 1 \pmod 4$, więc mamy sprzeczność. Zatem y jest parzyste, zaś x jest nieparzyste. Dla uproszczenia notacji w dalszych rozważaniach oznaczmy $t = \frac{n-1}{2}$. Wtedy $n = 2t+1$ i $t \in \mathbb{N}$, bo $n > 1$ i n jest liczbą naturalną nieparzystą.

W pierścieniu $\mathbb{Z}[i]$, który na mocy przykładu 13.25 jest pierścieniem euklidesowym, mamy, że $(y+i)\cdot(y-i) = y^m$. Elementy $y+i$, $y-i$ na mocy stwierdzenia 14.12 są względnie pierwsze. Z twierdzenia 13.20 istnieje $\alpha \in \mathbb{Z}[i]$ takie, że $y+i \sim \alpha^n$. Na mocy stwierdzenia 14.3 każdy element odwracalny pierścienia $\mathbb{Z}[i]$ jest n-tą potęgą pewnego elementu odwracalnego. Stąd $y+i = (a+bi)^n$ dla pewnych $a, b \in \mathbb{Z}$. Zatem $|y+i| = |a+bi|^n$, czyli $y^2+1 = (a^2+b^2)^n$. Ze wzoru Newtona

$$(a+bi)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k i^k =$$
$$= \sum_{k=0}^{t} (-1)^k \binom{n}{2k} a^{n-2k} b^{2k} + i \cdot \sum_{k=0}^{t} (-1)^k \binom{n}{2k+1} a^{2(t-k)} b^{2k+1},$$

skąd $1 = b \cdot \sum_{k=0}^{t} (-1)^k \binom{n}{2k+1} a^{2(t-k)} b^{2k}$, więc $b \mid 1$ w pierścieniu $\mathbb{Z}$, czyli $b = \pm 1$, skąd $y^2+1 = (a^2+1)^n$, więc a jest parzyste i uzyskujemy, że $\sum_{k=0}^{t} (-1)^k \binom{n}{2k+1} a^{2(t-k)} = \pm 1$, więc

$$\sum_{j=0}^{t} (-1)^{t-j} \binom{n}{2j} a^{2j} = \pm 1.$$

Zatem $\sum_{j=0}^{t} (-1)^j \binom{n}{2j} a^{2j} = \pm 1$. Jeśli $a = 0$, to $y^2+1 = 1$, skąd $y = 0$ i mamy sprzeczność. Zatem $a \neq 0$, więc $c = |a| \in \mathbb{N}$ i $a^{2j} = c^{2j}$ dla $j = 0, 1, \ldots, t$. Ponadto liczba c jest parzysta, więc $\sum_{j=0}^{t} (-1)^j \binom{n}{2j} c^{2j} = 1 + 4l$ dla pewnego $l \in \mathbb{Z}$. Stąd $1 + 4l = \pm 1$, więc ostatecznie $\sum_{k=0}^{t} (-1)^k \binom{n}{2k} c^{2k} = 1$. □

Twierdzenie 14.24. (Lebesgue'a). *Jeżeli $m, n \in \mathbb{N}$ i m jest parzyste oraz $n > 1$, to równanie $x^n - y^m = 1$ nie posiada rozwiązania w liczbach naturalnych.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieją $a, b, m, n \in \mathbb{N}$ takie, że $a^n - b^m = 1$ oraz $n > 1$ i $m = 2k$ dla pewnego $k \in \mathbb{N}$. Jeśli n jest parzyste, to $n = 2l$ dla pewnego $l \in \mathbb{N}$ i wtedy $(a^l - b^k)(a^l + b^k) = 1$, skąd $1 < a + b \leqslant a^l + b^k = 1$ i mamy sprzeczność. Wobec tego n jest liczbą nieparzystą oraz $(b^k)^2 + 1 = a^n$. W takim razie istnieją $x, y, t \in \mathbb{N}$ takie, że $y^2 + 1 = x^{2t+1}$. Oznaczmy $n = 2t + 1$. Zatem z lematu 14.23 istnieje parzysta liczba naturalna c taka, że $\sum_{k=0}^{t} (-1)^k \binom{n}{2k} c^{2k} = 1$. Stąd $1 + (-1)^{\frac{n(n-1)}{2}} c^2 + \sum_{k=2}^{t} (-1)^k \binom{n}{2k} c^{2k} = 1$, czyli

$$\frac{n(n-1)}{2} = \sum_{k=2}^{t} (-1)^k \binom{n}{2k} c^{2k-2}. \tag{14.5}$$

Niech s będzie największą nieujemną liczbą całkowitą taką, że 2^s dzieli $\frac{n(n-1)}{2}$. Wtedy $\frac{n(n-1)}{2} = 2^s l$ dla pewnej liczby nieparzystej l. Łatwo sprawdzić, że dla $k = 2, 3, \ldots, t$ zachodzi tożsamość

$$\binom{n}{2k} c^{2k-2} = \frac{n(n-1)}{2} \cdot \binom{n-2}{2k-2} \cdot \frac{c^{2k-2}}{k(2k-1)}. \tag{14.6}$$

Dla $k \geqslant 2$ mamy, że $2^{2k-2} > k$, skąd 2^{2k-2} nie dzieli liczby $k(2k-1)$. Ponadto c jest parzyste, więc dla $k \geqslant 2$, $2^{2k-2} \mid c^{2k-2}$. Wynika stąd, że istnieją względnie pierwsze liczby naturalne b, d takie, że $\frac{c^{2k-2}}{k(2k-1)} = \frac{2b}{d}$ oraz d jest liczbą nieparzystą. Stąd uzyskujemy, że

$$\binom{n}{2k} c^{2k-2} = 2^{s+1} l \binom{n-2}{2k-2} \cdot \frac{b}{d}.$$

Zatem $2^{s+1} \mid d \cdot \binom{n}{2k} c^{2k-2}$, skąd wobec nieparzystości d, $2^{s+1} \mid \binom{n}{2k} c^{2k-2}$ dla $k = 2, \ldots, t$. Zatem ze wzoru (14.5), $2^{s+1} \mid \frac{n(n-1)}{2}$ i mamy sprzeczność. □

Zadanie 14.25. Wyznacz wszystkie rozwiązania w liczbach całkowitych równania $x^2 + 4 = y^5$.

Zadanie 14.26. Niech $p > 3$ będzie liczbą pierwszą. Udowodnij, że istnieją liczby całkowite x i y spełniające równanie $x^2 + 4 = y^p$ wtedy i tylko wtedy, gdy istnieją liczby całkowite a i b takie, że $x + 2i = (a + bi)^p$.

Zadanie 14.27. Niech p będzie liczbą pierwszą postaci $4k + 1$. Udowodnij, że istnieją liczby całkowite x i y spełniające równanie $x^2 + 4 = y^p$ wtedy i tylko wtedy, gdy istnieje liczba całkowita a taka, że $x + 2i = (a + 2i)^p$.

Zadanie 14.28. Niech $p > 3$ będzie liczbą pierwszą taką, że $p \equiv 3 \pmod 4$. Udowodnij, że istnieją liczby całkowite x i y spełniające równanie $x^2 + 4 = y^p$ wtedy i tylko wtedy, gdy istnieje liczba całkowita a taka, że $x + 2i = (a - 2i)^p$.

Zadanie 14.29. Wyznacz wszystkie rozwiązania w liczbach całkowitych równania $x^2 + 9 = y^7$.

Rozdział 15

Zastosowania pierścienia $\mathbb{Z}[\sqrt{-2}]$

15.1 Klasyfikacja elementów pierwszych

Z przykładu 13.25 wiemy, że $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$ jest pierścieniem euklidesowym z normą N daną wzorem $N(x + y\sqrt{-2}) = x^2 + 2y^2$ dla $x, y \in \mathbb{Z}$. Wobec tego na mocy twierdzeń 13.15 i 13.24 w pierścieniu $\mathbb{Z}[\sqrt{-2}]$ pojęcia elementu pierwszego i elementu nierozkładalnego pokrywają się.

Ze wzoru (13.9) wiemy, że $(\mathbb{Z}[\sqrt{-2}])^* = \{1, -1\}$. Zatem na mocy stwierdzenia 13.2 dla dowolnego niezerowego $\alpha \in \mathbb{Z}[\sqrt{-2}]$ istnieją dokładnie dwa elementy stowarzyszone z α: $\alpha, -\alpha$.

15.2 Podstawowe spostrzeżenia o równaniu $x^2 + 2 = y^n$

Tytułowe równanie dla $n = 3$ o niewiadomych $x, y \in \mathbb{Z}$ było rozważane przez Fermata, który uważał, że posiada ono dokładnie dwa rozwiązania: $x = \pm 5$ i $y = 3$. Pierwszy pełny dowód tej hipotezy podał Euler w drugim tomie swojej *Algebry*. Następnie w roku 1923, T. Nagell przedstawił niekompletny dowód następującego twierdzenia:

Twierdzenie 15.1. *Dla naturalnych $n > 3$ równanie $x^2 + 2 = y^n$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Pierwszy pełny dowód tego twierdzenia przedstawił W. Ljunggren w 1943 roku. Następnie T. Nagell w 1954 roku podał inny dowód, który podobnie jak dowód W. Ljunggrena, nie był elementarny i bazował na rezultatach K. Mahlera dotyczących binarnych form kwadratowych. W związku z tym równanie:

$$x^2 + 2 = y^n, \tag{15.1}$$

nazywane jest w literaturze **równaniem Nagella**, a twierdzenie 15.1 nazywane jest **twierdzeniem Nagella**.

W 2000 roku B. Sury podjął próbę przedstawienia pierwszego elementarnego dowodu twierdzenia Nagella. Jednak jego rozumowanie zawiera błąd merytoryczny, który nie został zauważony przez recenzentów. Mianowicie w końcówce jego rozumowania rozpatrywany jest element $\beta = 1 + \sqrt{-2}$ pierścienia $\mathbb{Z}[\sqrt{-2}]$ i autor stwierdza, że dla naturalnych a i b na mocy rozwinięcia dwumianowego Newtona, $\beta^{2^a b} = = 1 + 2^a b\beta + 2^{a+1}\mu$ dla pewnego $\mu \in \mathbb{Z}[\sqrt{-2}]$. Następujący lemat pokazuje jednak, że tak nie jest.

Lemat 15.2. *Jeśli $\beta = 1 + \sqrt{-2}$, to $\beta^2 = -3 + 2\beta$, $\beta^3 = -6 + \beta$ i dla dowolnych $a, b \in \mathbb{N}$, gdzie $a \geqslant 2$ w pierścieniu $\mathbb{Z}[\sqrt{-2}]$ zachodzi wzór:*

$$\beta^{2^a b} = (1 + 2^a b) + 2^a b\beta + 2^{a+1}\mu \text{ dla pewnego } \mu \in \mathbb{Z}[\sqrt{-2}]. \tag{15.2}$$

Dowód. Zauważmy, że $\beta^2 = (1 + \sqrt{-2})^2 = 1 + 2\sqrt{-2} + (-2) = -3 + +2(1 + \sqrt{-2}) = -3 + 2\beta$. Stąd $\beta^3 = \beta(-3 + 2\beta) = -3\beta + 2\beta^2 = = -3\beta + 2(-3 + 2\beta) = -6 + \beta$. Zatem $\beta^4 = \beta(-6 + \beta) = = -6\beta + \beta^2 = -6\beta + (-3 + 2\beta) = -3 - 4\beta \equiv (1 + 2^2) + 2^2\beta \pmod{2^3}$. Załóżmy, że $\beta^{2^a} \equiv (1 + 2^a) + 2^a\beta \pmod{2^{a+1}}$ dla pewnego naturalnego $a \geqslant 2$. Wtedy $\beta^{2^a} = (1 + 2^a) + 2^a\beta + 2^{a+1}\mu$ dla pewnego $\mu \in \mathbb{Z}[\sqrt{-2}]$. Stąd $\beta^{2^{a+1}} = ((1 + 2^a) + 2^a\beta + 2^{a+1}\mu)^2 = = (1+2^a)^2 + 2^{2a}\beta^2 + 2^{2a+2}\mu^2 + 2^{a+1}(1+2^a)\beta + 2^{a+2}(1+2^a)\mu + 2^{2a+1}\beta\mu$. Ponadto $a \geqslant 2$, więc $2a+1 \geqslant a+3$ i $\beta^{2^{a+1}} \equiv (1+2^a)^2 + 2^{2a}\beta^2 + 2^{a+1}\beta =$

$= 1+2^{a+1}+2^{2a}+2^{2a}(-3+2\beta)+2^{a+1}\beta \equiv 1+2^{a+1}+2^{2a}-3\cdot 2^{2a}+2^{a+1}\beta =$
$= 1+2^{a+1}-2^{2a+1}+2^{a+1}\beta \equiv (1+2^{a+1})+2^{a+1}\beta \pmod{2^{a+2}}$. Zatem przez indukcję pokazaliśmy, że $\beta^{2^a} \equiv (1+2^a)+2^a\beta \pmod{2^{a+1}}$ dla każdego naturalnego $a \geqslant 2$.

Niech teraz $a, b \in \mathbb{N}$ i $a \geqslant 2$. Wtedy z pierwszej części dowodu $\beta^{2^a} =$
$= 1+2^a(1+\beta)+2^{a+1}\mu$ dla pewnego $\mu \in \mathbb{Z}[\sqrt{-2}]$. Stąd dwukrotnie na mocy wzoru dwumianowego Newtona $\beta^{2^a b} = (1+2^a(1+\beta)+2^{a+1}\mu)^b \equiv$
$\equiv (1+2^a(1+\beta))^b \equiv 1+b\cdot 2^a(1+\beta) \equiv (1+2^a b)+2^a b\beta \pmod{2^{a+1}}$, co kończy dowód. □

W tym rozdziale podamy elementarny dowód twierdzenia Nagella bazujący na własnościach pierścienia $\mathbb{Z}[\sqrt{-2}]$ oraz na twierdzeniu 7.20, w którym występuje pierścień $\mathbb{Z}[\sqrt{a^2+2}]$ dla pewnego $a \in \mathbb{N}$. Nasze rozważania rozpoczniemy od następujących uwag.

Uwaga 15.3. Łatwo zauważyć, że równanie (15.1) nie posiada rozwiązania w liczbach całkowitych x i y w przypadku, gdy n jest parzyste. Rzeczywiście, gdyby było inaczej, to dla pewnych $a, b \in \mathbb{Z}$ mielibyśmy $a^2+2=b^2$, skąd liczby a i b byłyby tej samej parzystości. Zatem liczby $b-a$ i $b+a$ byłyby parzyste, ale wtedy $2=(b-a)(b+a)$, więc $4 \mid 2$, co prowadzi do sprzeczności.

Uwaga 15.4. Jeśli $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$ i $x^2+2=y^n$, gdzie $n \geqslant 3$, to x i y są nieparzyste. Rzeczywiście, liczby x i y są tej samej parzystości. Gdyby były one obie parzyste, to $4 \mid x^2$ i $4 \mid y^n$, gdyż $n \geqslant 2$, skąd $4 \mid y^n - x^2$, czyli $4 \mid 2$, co prowadzi do sprzeczności.

Uwaga 15.5. Jeśli $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$ i $x^2+2=y^n$, gdzie $n \geqslant 3$, to elementy $x+\sqrt{-2}$ i $x-\sqrt{-2}$ pierścienia $\mathbb{Z}[\sqrt{-2}]$ są względnie pierwsze. Rzeczywiście, z przykładu 13.25 pierścień $\mathbb{Z}[\sqrt{-2}]$ jest euklidesowy z normą N, gdzie $N(a+b\sqrt{-2}) = a^2+2b^2$ dla $a, b \in \mathbb{Z}$. Wobec tego ten pierścień jest dziedziną z jednoznacznością rozkładu. Zatem jeśli elementy $x+\sqrt{-2}$ i $x-\sqrt{-2}$ nie są względnie pierwsze, to posiadają wspólny dzielnik α będący elementem pierwszym pierścienia $\mathbb{Z}[\sqrt{-2}]$. Wtedy α dzieli różnicę tych elementów, czyli element $2\sqrt{-2} = -(\sqrt{-2})^3$. Zatem $\alpha \mid \sqrt{-2}$, skąd $\alpha \mid 2$, bo $2 = (-\sqrt{-2})\cdot\sqrt{-2}$.

Ponadto $\alpha \mid x+\sqrt{-2}$, więc $\alpha \mid x$. Dalej, na mocy uwagi 15.4, $x = 2k+1$ dla pewnego $k \in \mathbb{Z}$ i $\alpha \mid 2$, a zatem $\alpha \mid 1$, co prowadzi do sprzeczności.

Uwaga 15.6. Niech $x, y \in \mathbb{Z}$, $x^2 + 2 = y^n$ i niech $n \in \mathbb{N}$, $n \geqslant 3$. Wówczas istnieją $a, b \in \mathbb{Z}$ takie, że

$$x + \sqrt{-2} = (a + b\sqrt{-2})^n. \tag{15.3}$$

Rzeczywiście, w pierścieniu $\mathbb{Z}[\sqrt{-2}]$ mamy, że $(x + \sqrt{-2})(x - \sqrt{-2}) = y^n$ i na mocy uwagi 15.5 elementy $x + \sqrt{-2}$ i $x - \sqrt{-2}$ dziedziny z jednoznacznością rozkładu $\mathbb{Z}[\sqrt{-2}]$ są względnie pierwsze, więc na mocy twierdzenia 13.20, $x+\sqrt{-2} = u\beta^n$ dla pewnego $\beta \in \mathbb{Z}[\sqrt{-2}]$ oraz dla pewnego $u \in (\mathbb{Z}[\sqrt{-2}])^*$. Ze wzoru (13.9), $(\mathbb{Z}[\sqrt{-2}])^* = \{1, -1\}$. Ponadto z uwagi 15.3 liczba n jest nieparzysta, więc $u = u^n$ i stąd $x + \sqrt{-2} = (u\beta)^n$. Zatem $x + \sqrt{-2} = (a + b\sqrt{-2})^n$ dla pewnych $a, b \in \mathbb{Z}$.

Na odwrót, załóżmy, że $x, a, b \in \mathbb{Z}$ i $n \in \{3, 4, \ldots\}$ spełniają równanie (15.3). Wtedy $N(x + \sqrt{-2}) = N((a + b\sqrt{-2})^n)$, skąd $x^2 + 2 = (a^2+2b^2)^n$. Zatem wtedy równanie (15.1) posiada rozwiązanie x oraz $y = a^2 + 2b^2$ w liczbach całkowitych.

Uwaga 15.7. Niech $x \in \mathbb{Z}$ i niech $n \in \mathbb{N}$, $n \geqslant 3$. Pokażemy, że $x^2 + 2 = y^n$ dla pewnego $y \in \mathbb{Z}$ wtedy i tylko wtedy, gdy istnieje nieparzysta liczba całkowita a taka, że

$$x + \sqrt{-2} = (a + \sqrt{-2})^n. \tag{15.4}$$

Jeśli $x + \sqrt{-2} = (a + \sqrt{-2})^n$ dla pewnego nieparzystego $a \in \mathbb{Z}$, to na mocy uwagi 15.6, $x^2 + 2 = (a^2 + 2)^n$ i wystarczy przyjąć $y = a^2 + 2$.

Na odwrót, załóżmy, że $x^2 + 2 = y^n$ dla pewnego $y \in \mathbb{Z}$. Wtedy z uwagi 15.6, $x + \sqrt{-2} = (a + b\sqrt{-2})^n$ dla pewnych $a, b \in \mathbb{Z}$. Ponadto z uwagi 15.3 liczba n jest nieparzysta i z uwagi 15.6, $x^2 + 2 = (a^2 + 2b^2)^n$, co implikuje, że $y = a^2 + 2b^2$. Dodatkowo na mocy uwagi 15.4 liczba y jest nieparzysta, a zatem liczba a też jest nieparzysta. Ze wzoru dwumianowego Newtona uzyskujemy, że

$$(a + b\sqrt{-2})^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k (\sqrt{-2})^k =$$

$$= \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} a^{n-2j} b^{2j} + \sqrt{-2} \cdot \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1} b^{2j+1}.$$

Wobec tego

$$x = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} a^{n-2j} b^{2j} \tag{15.5}$$

oraz

$$1 = b \cdot \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1} b^{2j}. \tag{15.6}$$

Z ostatniego wzoru $b \mid 1$, więc $b = \pm 1$, czyli $b^2 = 1$. Mnożąc obie strony wzoru (15.6) przez b uzyskujemy zatem, że

$$b = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1}.$$

Stąd $b \equiv na^{n-1} - 2\binom{n}{3} a^{n-3} \pmod 4$. Liczby n i a są nieparzyste, więc $a^{n-1} \equiv 1 \pmod 4$ i $a^{n-3} \equiv 1 \pmod 4$. Zatem $b \equiv n - 2\binom{n}{3} \pmod 4$ i $3b \equiv 3n - n(n-1)(n-2) = 3n - (n^2 - n)(n-2) \pmod 4$. Z nieparzystości n wynika, że $n^2 \equiv 1 \pmod 4$. Wobec tego $3b \equiv 3n - +(1-n)(n-2) \pmod 4$. Ponadto $3n - (1-n)(n-2) = 3n - n + +2 + n^2 - 2n = n^2 + 2 \equiv 1 + 2 \equiv 3 \pmod 4$, więc $3b \equiv 3 \pmod 4$, ale $\mathrm{NWD}(3, 4) = 1$, więc stąd $b \equiv 1 \pmod 4$. Ponadto $b = \pm 1$, więc ostatecznie $b = 1$ i $x + \sqrt{-2} = (a + \sqrt{-2})^n$.

Dodatkowo na mocy wzorów (15.5) i (15.6) uzyskujemy, że

$$x = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} a^{n-2j} \tag{15.7}$$

oraz

$$1 = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1}. \tag{15.8}$$

Na odwrót, niech liczba całkowita a spełnia równanie (15.8). Wtedy a jest nieparzyste i x dane wzorem (15.7) jest liczbą całkowitą. Z wcześniejszych naszych wyliczeń przy $b = 1$ uzyskujemy, że $x + \sqrt{-2} =$

$= (a+\sqrt{-2})^n$, a zatem $x^2+2 = (a^2+2)^n$. Stąd $y = a^2+2 \in \mathbb{Z}$ oraz $x^2+2 = y^n$.

W ten sposób wykazaliśmy, że równanie (15.1) posiada rozwiązanie w liczbach całkowitych x i y wtedy i tylko wtedy, gdy istnieje liczba całkowita a spełniająca równość (15.8).

Stosując uwagę 15.7 do $n = 3$ uzyskujemy równanie: $1 = 3a^2 - +2$, skąd $a = \pm 1$ oraz $x = \pm 5$ i $y = 3$. Wobec tego udowodniliśmy następujące twierdzenie Eulera:

Twierdzenie 15.8. *Wszystkimi rozwiązaniami równania* $x^2+2 = = y^3$ *w liczbach całkowitych są* $x = \pm 5$ *i* $y = 3$.

15.3 Dowód twierdzenia Nagella

Udowodnimy teraz bardzo ważny lemat odkryty przez B. Sury w [39].

Lemat 15.9. *Jeżeli dla liczby naturalnej* $n > 3$ *równanie* (15.1) *posiada rozwiązanie w liczbach całkowitych* x *i* y, *to* $n \equiv 3 \pmod 4$.

Dowód. Z uwagi 15.7 wynika, że n jest nieparzyste i istnieje nieparzysta liczba naturalna a taka, że $y = a^2+2$ oraz

$$1 = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1}. \tag{15.9}$$

Załóżmy, że $n \not\equiv 3 \pmod 4$. Wtedy $n \equiv 1 \pmod 4$. Zatem istnieje największa liczba naturalna t taka, że $2^t \mid n-1$, ale $4 \mid n-1$, więc $t \geqslant 2$ oraz $2^{t+1} \nmid n-1$. Stąd $n-1 = 2^t(2S+1)$ dla pewnego $S \in \mathbb{N}_0$, a zatem $n \equiv 1+2^t \pmod{2^{t+1}}$. Weźmy dowolne naturalne $k \geqslant 3$ takie, że $2k+1 \leqslant n$. Wtedy $\frac{n(n-1)}{(2k+1)(2k)} \cdot \binom{n-2}{2k-1} = \frac{n(n-1)}{(2k+1)(2k)} \cdot \frac{(n-2)!}{(2k-1)!(n-2k-1)!} = = \frac{n!}{(2k+1)!(n-2k-1)!} = \binom{n}{2k+1}$. Zatem dla takich k mamy tożsamość:

$$2^k \binom{n}{2k+1} = \frac{2^k}{2k} \cdot (n-1) \cdot \frac{n}{2k+1} \cdot \binom{n-2}{2k-1}. \tag{15.10}$$

Istnieją $s \in \mathbb{N}_0$ i nieparzyste $u \in \mathbb{N}$ takie, że $k = 2^s u$. Jeśli $k \leqslant s+1$, to $2^k \mid 2k$, skąd $2^k \leqslant 2k$, czyli $2^{k-1} \leqslant k$. Dalej, $k \geqslant 3$, więc $k-1 \geqslant 2$ i z dwumianu Newtona, $2^{k-1} = (1+1)^{k-1} \geqslant 1 + (k-1) + \binom{k-1}{2} > k$, co prowadzi do sprzeczności. Zatem $k \geqslant s+2$, czyli $\frac{2^k}{2k} = \frac{2c}{2v-1}$ dla pewnych $c, v \in \mathbb{N}$. Ponadto, $n-1 = 2^t(2S+1)$ i liczby $2k+1$ oraz n są nieparzyste, więc na mocy (15.10) mamy, że

$$2^k \binom{n}{2k+1} \equiv 0 \pmod{2^{t+1}} \text{ dla wszystkich } k \geqslant 3,\ k \leqslant \frac{n-1}{2}. \tag{15.11}$$

Stąd i ze wzoru (15.9) wynika, że

$$\binom{n}{1} a^{n-1} - 2\binom{n}{3} a^{n-3} + 4\binom{n}{5} a^{n-5} \equiv 1 \pmod{2^{t+1}}. \tag{15.12}$$

Z twierdzenia Eulera otrzymujemy, że $a^{2^t} = a^{\varphi(2^{t+1})} \equiv 1 \pmod{2^{t+1}}$, skąd po uwzględnieniu, że $n-1 = 2^t(2S+1)$ uzyskujemy kongruencję: $a^{n-1} \equiv 1 \pmod{2^{t+1}}$. Ponadto $n \equiv 1 + 2^t \pmod{2^{t+1}}$, więc:

$$\binom{n}{1} a^{n-1} \equiv 1 + 2^t \pmod{2^{t+1}}. \tag{15.13}$$

Oznaczmy $D = 2\binom{n}{3} a^{n-3}$. Wtedy $D = \frac{n(n-1)(n-2)}{3} \cdot a^{n-3}$ i $n \equiv 1 + 2^t \pmod{2^{t+1}}$, więc $3D \equiv (1+2^t) \cdot 2^t \cdot (2^t - 1) \cdot a^{n-3} \equiv 3 \cdot 2^t \pmod{2^{t+1}}$, bo $2 \mid (1+2^t) \cdot (2^t - 1) \cdot a^{n-3} - 3$, gdyż liczba a jest nieparzysta. Ponadto $\mathrm{NWD}(3, 2^{t+1}) = 1$, więc $D \equiv 2^t \pmod{2^{t+1}}$. Wobec tego:

$$2\binom{n}{3} a^{n-3} \equiv 2^t \pmod{2^{t+1}}. \tag{15.14}$$

Oznaczmy $E = 4\binom{n}{5} a^{n-5}$. Wtedy $E = \frac{n(n-1)(n-2)(n-3)(n-4)}{2 \cdot 3 \cdot 5} a^{n-5}$ i $n = 1 + 2^t + 2^{t+1}S$, więc $15E = (1 + 2^t + 2^{t+1}S)(2^t + 2^{t+1}S)(2^t + 2^{t+1}S + 1)(2^{t-1} + 2^t S - 1)(2^t + 2^{t+1}S - 3) \cdot a^{n-5}$. Dodatkowo $t \geqslant 2$, więc liczba $(1+2^t+2^{t+1}S)(2^t+2^{t+1}S-1)(2^{t-1}+2^tS-1)(2^t+2^{t+1}S-3)a^{n-5} = 2g+1$ dla pewnego $g \in \mathbb{Z}$ i stąd $15E \equiv 2^t(2g+1) \equiv 2^t \equiv 15 \cdot 2^t \pmod{2^{t+1}}$.

Ponadto $\mathrm{NWD}(15, 2^{t+1}) = 1$, więc $E \equiv 2^t \pmod{2^{t+1}}$. Wobec tego

$$4\binom{n}{5}a^{n-5} \equiv 2^t \pmod{2^{t+1}}. \tag{15.15}$$

Z zależności (15.13)-(15.15) i (15.12) wynika, że $(1 + 2^t) - 2^t + 2^t \equiv$ $\equiv 1 \pmod{2^{t+1}}$, skąd $2^{t+1} \mid 2^t$ i mamy sprzeczność. Wobec tego $n \equiv 3 \pmod 4$. □

Lemat 15.10. *Niech $n > 3$ będzie liczbą naturalną. Jeżeli $x^2 + 2 =$ $= y^n$ dla pewnych $x, y \in \mathbb{Z}$, to $y = 3$.*

Dowód. Na mocy lematu 15.9, $n = 4m + 3$ dla pewnego $m \in \mathbb{N}_0$. Ponadto z uwagi 15.7, x jest nieparzyste oraz $y = a^2 + 2$ dla pewnej nieparzystej liczby naturalnej a spełniającej zależność (15.9). Wobec tego $1 \equiv (-2)^{\frac{n-1}{2}} \pmod a$. Dodatkowo $\frac{n-1}{2} = 2m + 1$, więc

$$2^{\frac{n-1}{2}} \equiv -1 \pmod a. \tag{15.16}$$

Ponadto x jest nieparzyste, więc możemy zakładać, że $x \in \mathbb{N}$ i równość $x^2 + 2 = y^n$ możemy zapisać w postaci $x^2 - (a^2 + 2)(y^{\frac{n-1}{2}})^2 = -2$. Z twierdzenia 7.20 uzyskujemy, że $y^{\frac{n-1}{2}} \equiv 1 \pmod a$. Jednak $y \equiv 2 \pmod a$, więc $2^{\frac{n-1}{2}} \equiv 1 \pmod a$. Stąd i z (15.16), $1 \equiv -1 \pmod a$, czyli $a \mid 2$, ale a jest nieparzyste, więc $a = 1$ i $y = 3$. □

Lemat 15.11. *Niech $n, t \in \mathbb{N}$, gdzie $n > 3$ i $t \geqslant 2$, będą takie, że $2^t \mid n - 3$ oraz $2^{t+1} \nmid n - 3$. Wtedy $\sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} \equiv 1 + 2^t \pmod{2^{t+1}}$.*

Dowód. Na mocy naszych założeń $n = 2^t b + 3$ dla pewnych $t, b \in \mathbb{N}$, gdzie $t \geqslant 2$ i $2 \nmid b$. W pierścieniu $\mathbb{Z}[\sqrt{-2}]$ dla $\beta = 1 + \sqrt{-2}$ z lematu 15.2 i z nieparzystości b mamy, że $\beta^{2^t b} \equiv (1+2^t b)+2^t b\beta \equiv (1+2^t)+2^t\beta \pmod{2^{t+1}}$. Ponadto $\beta^3 = \beta - 6$, więc stąd $\beta^n \equiv (\beta-6)((1+2^t)+2^t\beta) \equiv$ $\equiv (1+2^t)\beta+2^t\beta^2-6 \equiv (1+2^t)\beta+2^t(-3+2\beta)-6 \equiv (2^t-6)+(1+2^t)\beta \pmod{2^{t+1}}$. Zatem $\beta^n = (2^t - 6) + (1 + 2^t)\beta + 2^{t+1}\mu$ dla pewnego

$\mu \in \mathbb{Z}[\sqrt{-2}]$. Stąd $\overline{\beta}^n = (2^t - 6) + (1 + 2^t)\overline{\beta} + 2^{t+1}\overline{\mu}$. Wobec tego $\beta^n - \overline{\beta}^n = (1 + 2^t)(\beta - \overline{\beta}) + 2^{t+1}(\mu - \overline{\mu})$. Dodatkowo $\mu = u + v\sqrt{-2}$ dla pewnych $u, v \in \mathbb{Z}$ i $\beta - \overline{\beta} = 2\sqrt{-2}$, więc $\mu - \overline{\mu} = 2v\sqrt{-2}$. Stąd

$$\frac{\beta^n - \overline{\beta}^n}{2\sqrt{-2}} = 1 + 2^t + 2^{t+1}v. \tag{15.17}$$

Na mocy wzoru Newtona

$$\beta^n = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} + \sqrt{-2} \cdot \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1},$$

więc $\overline{\beta}^n = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} - \sqrt{-2} \cdot \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1}$. Zatem $\frac{\beta^n - \overline{\beta}^n}{2\sqrt{-2}} = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1}$ i na mocy (15.17) mamy tezę. □

Przejdźmy teraz do dowodu twierdzenia Nagella. Załóżmy, że dla pewnego naturalnego $n > 3$ istnieją liczby całkowite x i y takie, że $x^2 + 2 = y^n$. Z lematu 15.9 uzyskujemy, że $n \equiv 3 \pmod 4$, skąd wynika istnienie liczby naturalnej $t \geqslant 2$ takiej, że $2^t \mid n - 3$ i $2^{t+1} \nmid n - 3$. Z lematu 15.10 i jego dowodu otrzymujemy, że $y = 3$ i $\sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} = 1$. Stąd na mocy lematu 15.11 mamy, że $1 \equiv 1 + 2^t \pmod{2^{t+1}}$, a więc $2^{t+1} \mid 2^t$, co prowadzi do sprzeczności. Wobec tego równanie (15.1) dla naturalnych $n > 3$ nie posiada rozwiązania w liczbach całkowitych x i y. W ten sposób dowód twierdzenia Nagella został zakończony.

Zadanie 15.12. Udowodnij, że jedynym rozwiązaniem równania $x^3 = 2y^2 + 1$ w liczbach całkowitych x i y jest $x = 1$ i $y = 0$.

Rozdział 16

Zastosowania pierścienia Eisensteina

16.1 Podstawowe własności pierścienia Eisensteina

Z przykładu 13.25 wiemy, że pierścień Eisensteina $\mathbb{Z}[\omega]$, gdzie $\omega = \frac{1+\sqrt{-3}}{2}$, jest dziedziną z jednoznacznością rozkładu jako pierścień euklidesowy z normą N daną wzorem: $N(a+b\omega) = a^2+ab+b^2$ dla $a, b \in \mathbb{Z}$. Każdy element tego pierścienia można jednoznacznie zapisać w postaci $a+b\omega$ dla pewnych $a, b \in \mathbb{Z}$. Ze wzorów (13.8) i (13.9) mamy od razu, że

$$\omega^2 = \omega - 1, \quad \omega^3 = -1 \quad \text{oraz} \quad \overline{\omega} = 1 - \omega. \tag{16.1}$$

Natomiast ze wzoru (13.12) i tego, że $a^2+ab+b^2 = (a+\frac{b}{2})^2 + \frac{3}{4}b^2 \geqslant 0$ uzyskujemy, że $(\mathbb{Z}[\omega])^* = \{\alpha \in \mathbb{Z}[\omega] : N(\alpha) = 1\}$. Jeśli $\alpha = a+b\omega$, gdzie $a, b \in \mathbb{Z}$, to $N(\alpha) = 1$ wtedy i tylko wtedy, gdy $(a+\frac{b}{2})^2 + \frac{3}{4}b^2 = 1$. Ponadto, gdy $|b| \geqslant 2$, to lewa strona tej równości jest nie mniejsza niż 3, skąd $|b| \leqslant 1$, czyli $b \in \{-1, 0, 1\}$. Dla $b = -1$, $(a-\frac{1}{2})^2 = \frac{1}{4}$, skąd $a = 0$ lub $a = 1$, czyli $\alpha = -\omega$ lub $\alpha = 1-\omega = \omega^2$. Dla $b = 0$, $a^2 = 1$, skąd $a = \pm 1$ oraz $\alpha = \pm 1$. Natomiast dla $b = 1$, $(a+\frac{1}{2})^2 = \frac{1}{4}$, skąd $a = 0$ lub $a = -1$, czyli $\alpha = \omega$ lub $\alpha = -1+\omega = -\omega^2$ na mocy

(16.1). W ten sposób wykazaliśmy, że grupa $(\mathbb{Z}[\omega])^*$ ma dokładnie sześć elementów: $1, -1, \omega, -\omega, \omega^2 = \omega - 1, -\omega^2 = 1 - \omega$, czyli zachodzi wzór (13.13).

Lemat 16.1. *Elementy α i $\overline{\alpha}$, gdzie $\alpha = a + b\omega$ oraz $a, b \in \mathbb{Z}$ są względnie pierwsze w pierścieniu Eisensteina wtedy i tylko wtedy, gdy $a \not\equiv b \pmod 3$ i $\mathrm{NWD}(a, b) = 1$.*

Dowód. Jeśli $a \equiv b \pmod 3$, to $a = b + 3k$ dla pewnego $k \in \mathbb{Z}$, więc $a + b\omega = 3k + b(1 + \omega)$, ale $3k = \sqrt{-3} \cdot (-\sqrt{-3}k)$ oraz $1 + \omega = \frac{3+\sqrt{-3}}{2} = \sqrt{-3} \cdot \frac{-\sqrt{-3}-1}{2} = (-\omega) \cdot \sqrt{-3}$, więc $\sqrt{-3} \mid \alpha$. Zatem $\alpha = \sqrt{-3} \cdot \beta$ dla pewnego $\beta \in \mathbb{Z}[\omega]$, skąd $\overline{\alpha} = \sqrt{-3} \cdot (-\overline{\beta})$, czyli $\sqrt{-3} \mid \overline{\alpha}$. Ponadto $\sqrt{-3} \neq 0$ oraz $\sqrt{-3} = 2\omega - 1$, więc z (13.13), $\sqrt{-3} \notin (\mathbb{Z}[\omega])^*$. Wobec tego elementy α i $\overline{\alpha}$ nie są względnie pierwsze w pierścieniu Eisensteina. Podobnie, jeśli $d = \mathrm{NWD}(a, b) > 1$, to $d \mid \alpha$, skąd $d \mid \overline{\alpha}$, a ponieważ $d \neq 0$ i $d \notin (\mathbb{Z}[\omega])^*$, więc elementy α i $\overline{\alpha}$ nie są względnie pierwsze w pierścieniu Eisensteina.

Na odwrót, niech $a \not\equiv b \pmod 3$ i $\mathrm{NWD}(a, b) = 1$. Wtedy $ak + bl = 1$ dla pewnych $k, l \in \mathbb{Z}$. Przypuśćmy, że elementy α i $\overline{\alpha}$ nie są względnie pierwsze w pierścieniu Eisensteina. Wtedy istnieje element pierwszy π tego pierścienia taki, że $\pi \mid \alpha$ oraz $\pi \mid \overline{\alpha}$. Jeśli $\pi \mid a$ i $\pi \mid b$, to $\pi \mid ak + bl$, czyli $\pi \mid 1$, co prowadzi do sprzeczności. Zatem $\pi \nmid a$ lub $\pi \nmid b$. Dalej, $\overline{\alpha} = a + b\overline{\omega} = a + b(1 - \omega) = (a + b) + b\omega$ oraz $\pi \mid \alpha + \overline{\alpha}$ i $\pi \mid \alpha - \overline{\alpha}$. Zatem $\pi \mid b + 2a$ oraz $\pi \mid b(1 - 2\omega)$. Z drugiej zależności wynika, że $\pi \mid b$ lub $\pi \mid 1 - 2\omega$. Jednak jeśli $\pi \mid b$, to ponieważ $\pi \mid a + 2b$, więc $\pi \mid a$, co jest niemożliwe. Zatem $\pi \nmid b$ oraz $\pi \mid 1 - 2\omega$, ale $1 - 2\omega = -\sqrt{-3}$, więc $N(\pi) \mid N(-\sqrt{-3}) = 3$. Ponadto $N(\pi) > 1$, a zatem $N(\pi) = 3$. Lecz, jak pokazaliśmy, $\pi \mid b + 2a$, a więc $N(\pi) \mid N(b + 2a)$, skąd $3 \mid (b + 2a)^2$. Zatem $3 \mid b + 2a$, skąd $b \equiv a \pmod 3$ i mamy sprzeczność. Wobec tego elementy α i $\overline{\alpha}$ są względnie pierwsze w pierścieniu Eisensteina. □

Niech $a, b \in \mathbb{Z}$. Wtedy na mocy (16.1) mamy, że $(a + b\omega)^3 = a^3 + 3a^2b\omega + 3ab^2\omega^2 + b^3\omega^3 = a^3 + 3a^2b\omega + 3ab^2(\omega - 1) - b^3$, czyli zachodzi wzór:

$$(a + b\omega)^3 = (a^3 - 3ab^2 - b^3) + 3ab(a + b)\omega. \tag{16.2}$$

Ze wzorów (16.1) i (16.2) wynika, że dla dowolnych $a, b \in \mathbb{Z}$:

$$\omega(a+b\omega)^3 = -3ab(a+b) + (a^3 + 3a^2b - b^3)\omega \tag{16.3}$$

oraz

$$\omega^2(a+b\omega)^3 = (b^3 - 3a^2b - a^3) + (a^3 - 3ab^2 - b^3)\omega. \tag{16.4}$$

16.2 Najprostsze przypadki twierdzenia Cohna

W 1993 roku J. H. E. Cohn udowodnił następujący rezultat, zwany dalej **twierdzeniem Cohna**:

Twierdzenie 16.2. *Dla naturalnych $n \geqslant 3$ równanie $x^2 + 3 = y^n$ nie posiada rozwiązania w liczbach całkowitych x i y.*

W tym rozdziale podamy dowód tego twierdzenia, będący pewną modyfikacją oryginalnego dowodu J. H. E. Cohna opublikowanego w [11]. Rozpoczynamy od prostych obserwacji związanych z tym tematem.

Stwierdzenie 16.3. *Dla $m \in \mathbb{N}$ równanie $x^2 + 3 = y^{2m}$ posiada rozwiązanie w liczbach całkowitych x i y wtedy i tylko wtedy, gdy $m = 1$. Ponadto, wszystkimi rozwiązaniami równania $x^2 + 3 = y^2$ w liczbach całkowitych x i y są; $x = \pm 1$ i $y = \pm 2$.*

Dowód. Niech $a, b \in \mathbb{Z}$ i $a^2+3 = b^2$. Wtedy $3 = b^2 - a^2 = (b-a)(b+a)$, skąd $b - a = 1$ i $b + a = 3$ albo $b - a = -1$ i $b + a = -3$ albo $b - a = 3$ i $b + a = 1$ albo $b - a = -3$ i $b + a = -1$. Zatem $b = \pm 2$ i $a = \pm 1$. Ponadto $(\pm 1)^2 + 3 = 4 = (\pm 2)^2$. Wobec tego wszystkimi rozwiązaniami równania $x^2 + 3 = y^2$ w liczbach całkowitych x i y są; $x = \pm 1$ i $y = \pm 2$.

Niech teraz $m \in \mathbb{N}$ i $m > 1$. Załóżmy, że $x^2 + 3 = y^{2m}$ dla pewnych $x, y \in \mathbb{Z}$. Wtedy $x^2 + 3 = (y^m)^2$, więc z pierwszej części dowodu $y^m = \pm 2$. Zatem $y = 2t$ dla pewnego $t \in \mathbb{Z}$ i $2^m t^m = \pm 2$, ale $m \geqslant 2$, więc stąd $4 \mid 2$, co prowadzi do sprzeczności. Kończy to dowód naszego stwierdzenia. □

Lemat 16.4. *Niech $n \in \mathbb{N}$ i $n \geqslant 3$. Jeśli $x, y \in \mathbb{Z}$ oraz $x^2+3 = y^n$, to $2 \mid x$ i $3 \nmid x$ oraz w pierścieniu Eisensteina elementy $x + \sqrt{-3}$ i $x - \sqrt{-3}$ są względnie pierwsze.*

Dowód. Jeżeli $2 \nmid x$, to $x^2 \equiv 1 \pmod 8$ i z równości $x^2+3 = y^n$ wynika, że $2 \mid y$. Ponadto $n \geqslant 3$, więc $8 \mid y^n$. Dodatkowo $x^2 + 3 \equiv 1 + 3 \equiv 4 \pmod 8$, więc $4 \equiv 0 \pmod 8$, co prowadzi do sprzeczności. Wobec tego $2 \mid x$.

Podobnie, jeśli $3 \mid x$, to z równości $x^2 + 3 = y^n$ wynika, że $3 \mid y$, ale $n \geqslant 3$, więc $9 \mid y^n$. Ponadto $9 \mid x^2$, więc $x^2 + 3 \equiv 3 \pmod 9$. Wobec tego $3 \equiv 0 \pmod 9$ i mamy sprzeczność. W takim razie $3 \nmid x$.

Stąd wynika, że $x - 1 \not\equiv 2 \pmod 3$ oraz $\mathrm{NWD}(x - 1, 2) = 1$. Z lematu 16.1 elementy $\alpha = (x - 1) + 2\omega$ i $\overline{\alpha}$ są względnie pierwsze w pierścieniu Eisensteina. Jednak $\sqrt{-3} = 2\omega - 1$, więc $\alpha = x + \sqrt{-3}$ i $x - \sqrt{-3} = \overline{\alpha}$, co kończy dowód. □

Stwierdzenie 16.5. *Dla naturalnych m równanie $x^2+3 = y^{3m}$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Dowód. Załóżmy, że tak nie jest. Ponieważ $u^{3m} = (u^m)^3$ dla $u \in \mathbb{Z}$, więc stąd $x^2 + 3 = y^3$ dla pewnych $x, y \in \mathbb{Z}$. Z lematu 16.4, $2 \mid x$ i $3 \nmid x$ oraz w pierścieniu Eisensteina $\mathbb{Z}[\omega]$ elementy $x+\sqrt{-3}$ i $x-\sqrt{-3}$ są względnie pierwsze. Zatem na mocy twierdzenia 13.20, $x + \sqrt{-3} = u\alpha^3$ dla pewnego $u \in (\mathbb{Z}[\omega])^*$ i dla pewnego $\alpha \in \mathbb{Z}[\omega]$. Ze wzoru (13.16) grupa $(\mathbb{Z}[\omega])^*$ ma dokładnie 6 elementów: $1, -1, \omega, -\omega, \omega^2, -\omega^2$. Ponadto $(-1) = (-1)^3$, więc istnieją $a, b \in \mathbb{Z}$ takie, że $x + \sqrt{-3} = (a + b\omega)^3$ albo $x + \sqrt{-3} = \omega(a + b\omega)^3$ albo $x + \sqrt{-3} = \omega^2(a + b\omega)^3$. Ponadto $x + \sqrt{-3} = (x - 1) + 2\omega$, więc na mocy (16.2) pierwszy przypadek odpada. W przypadku drugim na mocy (16.3), $x - 1 = -3ab(a + b)$. Liczba $ab(a + b)$ jest parzysta dla dowolnych $a, b \in \mathbb{Z}$ (jest to oczywiste, gdy $2 \mid a$ lub $2 \mid b$, a w przeciwnym przypadku $2 \mid a + b$), zaś liczba $x - 1$ jest nieparzysta, czyli ten przypadek też prowadzi do sprzeczności. W ostatnim przypadku z (16.4), $x + 1 = (x-1)+2 = -3ab(a+b)$, ale liczba $x+1$ jest nieparzysta, zaś liczba $ab(a + b)$ jest parzysta, więc też otrzymujemy sprzeczność.

Przypuszczenie, że dla pewnych $x, y \in \mathbb{Z}$ i dla pewnego $m \in \mathbb{N}$ jest $x^2 + 3 = y^{3m}$ doprowadziło nas zatem do sprzeczności. □

Lemat 16.6. *Jeżeli dla pewnego naturalnego $n \geqslant 3$ równanie $x^2 + 3 = y^n$ posiada rozwiązanie w liczbach całkowitych x i y, to dla pewnej liczby pierwszej $p > 3$ równanie $x^2 + 3 = y^p$ też ma rozwiązanie w liczbach całkowitych x i y.*

Dowód. Załóżmy, że $x^2 + 3 = y^n$ dla pewnego naturalnego $n \geqslant 3$ i dla pewnych $x, y \in \mathbb{Z}$. Wtedy ze stwierdzeń 16.3 i 16.5 mamy, że $2 \nmid n$ i $3 \nmid n$. Ponadto $n > 1$, więc n posiada dzielnik pierszy p i oczywiście $p > 3$. Stąd $n = pm$ dla pewnego $m \in \mathbb{N}$ i $x^2 + 3 = (y^m)^p$ oraz $y^m \in \mathbb{Z}$, więc równanie $x^2 + 3 = y^p$ też ma rozwiązanie w liczbach całkowitych x i y. □

16.3 Dowód twierdzenia Cohna

Rozpoczynamy od wykazania kilku technicznych lematów.

Lemat 16.7. *Dla liczb naturalnych $k \geqslant 2$ liczba $k(2k + 1)$ nie jest podzielna przez 3^{k-1}.*

Dowód. Dla $k = 2$ mamy, że $k(2k + 1) = 10$ i $3^{k-1} = 3$, więc teza zachodzi. Niech dalej $k \geqslant 3$. Zauważmy, że liczby k i $2k+1$ są względnie pierwsze, bo $\mathrm{NWD}(k, 2k + 1) = \mathrm{NWD}(k, 1) = 1$. Wobec tego, jeżeli $3^{k-1} \mid k(2k + 1)$, to $3^{k-1} \mid k$ lub $3^{k-1} \mid 2k + 1$. Stąd $3^{k-1} \leqslant 2k + 1$. Ponadto $k \geqslant 3$, więc z dwumianu Newtona, $3^{k-1} = (1 + 2)^{k-1} \geqslant$ $\geqslant 1+(k-1)\cdot 2+\binom{k-1}{2}2^2 \geqslant 1+2k-2+4 > 2k+1$ i mamy sprzeczność, co kończy dowód naszego lematu. □

Lemat 16.8. *Niech $a, b \in \mathbb{Z}$ i $a \equiv b \pmod 9$. Wówczas $a^{3^v} \equiv b^{3^v} \pmod{3^{v+2}}$ dla każdego $v \in \mathbb{N}_0$.*

Dowód. Zastosujemy indukcję ze względu na $v \in \mathbb{N}_0$. Dla $v = 0$ teza wynika od razu z założenia, że $a \equiv b \pmod 9$. Przypuśćmy, że $a^{3^v} \equiv b^{3^v} \pmod{3^{v+2}}$ dla pewnego $v \in \mathbb{N}_0$. Wówczas $a^{3^v} b^{3^v} \equiv a^{2\cdot 3^v} \pmod{3^{v+2}}$ i $b^{2\cdot 3^v} \equiv a^{2\cdot 3^v} \pmod{3^{v+2}}$, więc $a^{2\cdot 3^v} + a^{3^v} b^{3^v} + b^{2\cdot 3^v} \equiv 3a^{2\cdot 3^v} \pmod{3^{v+2}}$, skąd $3 \mid a^{2\cdot 3^v} + a^{3^v} b^{3^v} + b^{2\cdot 3^v}$. Ponadto,

$$a^{3^{v+1}} - b^{3^{v+1}} = (a^{3^v})^3 - (b^{3^v})^3 = (a^{3^v} - b^{3^v})(a^{2\cdot 3^v} + a^{3^v} b^{3^v} + b^{2\cdot 3^v})$$

i z założenia indukcyjnego $3^{v+2} \mid a^{3^v} - b^{3^v}$, więc $3^{v+3} \mid a^{3^{v+1}} - b^{3^{v+1}}$, czyli $a^{3^{v+1}} \equiv b^{3^{v+1}} \pmod{3^{v+3}}$. Zatem wówczas teza zachodzi dla liczby $v+1$. Kończy to dowód naszego lematu. □

Lemat 16.9. *Dla dowolnego $v \in \mathbb{N}_0$: $3^{v+1}-1$ jest resztą z dzielenia liczby 2^{3^v} przez liczbę 3^{v+2}.*

Dowód. Dla $v \in \mathbb{N}_0$ jest: $0 < 2 \leqslant 3^{v+1} - 1 < 3^{v+1} < 3^{v+2}$, więc wystarczy pokazać, że $2^{3^v} \equiv 3^{v+1} - 1 \pmod{3^{v+2}}$.

Zrobimy to przez indukcję względem $v \in \mathbb{N}_0$. Dla $v = 0$, $3^{v+2} = 9$, $2^{3^v} = 2$ i $3^{v+1} - 1 = 2$, więc teza wtedy zachodzi. Przypuśćmy, że teza zachodzi dla pewnej liczby $v \in \mathbb{N}_0$. Wtedy $2^{3^v} = 3^{v+2}k + 3^{v+1} - 1 = 3^{v+1}(3k+1) - 1$ dla pewnego $k \in \mathbb{Z}$, ale $2^{3^{v+1}} = (2^{3^v})^3$, więc $2^{3^{v+1}} = (3^{v+1}(3k+1)-1)^3 = 3^{3v+3}(3k+1)^3 - 3\cdot 3^{2v+2}(3k+1)^2 + 3\cdot 3^{v+1}(3k+1) - 1$. Ponadto $3v+3 \geqslant 2v+3 \geqslant v+3$, a zatem $2^{3^{v+1}} \equiv 3\cdot 3^{v+1}(3k+1) - 1 = 3^{v+3}k + 3^{v+2} - 1 \equiv 3^{v+2} - 1 \pmod{3^{v+3}}$, czyli teza zachodzi wtedy także dla liczby $v+1$, co kończy dowód naszego lematu. □

Lemat 16.10. *Dla dowolnego $v \in \mathbb{N}_0$: $4^{3^v} \equiv 1 + 3^{v+1} \pmod{3^{v+2}}$ oraz $7^{3^v} \equiv 1 + 2 \cdot 3^{v+1} \pmod{3^{v+2}}$.*

Dowód. Ponieważ $4^{3^v} = (2^{3^v})^2$, więc z lematu 16.9, $4^{3^v} \equiv (3^{v+1}-1)^2 \equiv 3^{2v+2} - 2\cdot 3^{v+1} + 1 \equiv 3^{v+1} + 1 \pmod{3^{v+2}}$. Ponadto $7 \equiv 16 \pmod 9$, więc z lematu 16.8, $7^{3^v} \equiv 16^{3^v} \pmod{3^{v+2}}$, ale $16^{3^v} = (4^{3^v})^2$, więc z pierwszej części dowodu, $7^{3^v} \equiv (1 + 3^{v+1})^2 \equiv 1 + 2 \cdot 3^{v+1} + 3^{2v+2} \equiv 1 + 2 \cdot 3^{v+1} \pmod{3^{v+2}}$. □

Lemat 16.11. *Załóżmy, że $p \in \mathbb{P}$, $p > 3$ i $x^2 + 3 = y^p$ dla pewnych $x, y \in \mathbb{Z}$. Wówczas $p \equiv 1 \pmod 3$ i istnieje parzysta liczba całkowita a niepodzielna przez 3 i taka, że $y = a^2 + 3$ oraz*

$$1 = \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} (-3)^k a^{p-2k-1}. \tag{16.5}$$

Dowód. W pierścieniu Eisensteina mamy, że $(x+\sqrt{-3})(x-\sqrt{-3}) = y^p$ i na mocy lematu 16.4 elementy $x + \sqrt{-3}$ oraz $x - \sqrt{-3}$ są względnie pierwsze. Zatem z twierdzenia 13.20 mamy, że $x + \sqrt{-3} = u\alpha^3$ dla

pewnego $u \in (\mathbb{Z}[\omega])^*$ i dla pewnego $\alpha \in \mathbb{Z}[\omega]$. Jak wiemy, grupa $(\mathbb{Z}[\omega])^*$ ma rząd 6 oraz $\mathrm{NWD}(p,6) = 1$, gdyż $p \in \mathbb{P}$ i $p > 3$, więc $u = v^p$ dla pewnego $v \in (\mathbb{Z}[\omega])^*$, więc $x + \sqrt{-3} = \beta^p$ dla pewnego $\beta \in \mathbb{Z}[\omega]$. Ponadto $\beta = U + V\omega$ dla pewnych $U, V \in \mathbb{Z}$, skąd $\beta = \frac{(2U+V)+V\sqrt{-3}}{2}$. Oznaczmy $A = 2U + V$ i $B = V$. Wtedy $A, B \in \mathbb{Z}$, $A \equiv B \pmod 2$ i $\beta = \frac{A+B\sqrt{-3}}{2}$. Wobec tego $x + \sqrt{-3} = \left(\frac{A+B\sqrt{-3}}{2}\right)^p$, skąd

$$2^p x + 2^p\sqrt{-3} = (A + B\sqrt{-3})^p. \tag{16.6}$$

Stosując wzór dwumianowy Newtona uzyskujemy stąd, że

$$2^p x + 2^p\sqrt{-3} =$$

$$= \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k} A^{p-2k} B^{2k} (-3)^k + \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} A^{p-2k-1} B^{2k+1} (-3)^k \sqrt{-3}.$$

Wobec tego $2^p = B\sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} A^{p-2k-1} B^{2k} (-3)^k$. Stąd $B \mid 2^p$. Zatem, jeśli B jest nieparzyste, to $B = \pm 1$ i $2^p = \pm\sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} A^{p-2k-1} (-3)^k$. Z pierwszości p, $p \mid \binom{p}{2k+1}$ dla każdego $k = 0, 1, \ldots, \frac{p-1}{2} - 1$, więc $2^p \equiv \pm(-3)^{\frac{p-1}{2}} \pmod p$. Jednak $p > 3$, więc $3^{p-1} \equiv 1 \pmod p$ z Małego twierdzenia Fermata, skąd $(-3)^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ i w takim razie $2^p \equiv \pm 1 \pmod p$. Z Małego twierdzenia Fermata $2^p \equiv 2 \pmod p$, więc $2 \equiv \pm 1 \pmod p$, skąd $p \mid 2 - 1$ lub $p \mid 2 - (-1)$, co przeczy założeniu, że $p > 3$. Stąd B musi być parzyste, a ponieważ $A \equiv B \pmod 2$, więc $2 \mid A$. W takim razie $A = 2a$ i $B = 2b$ dla pewnych $a, b \in \mathbb{Z}$ i wzór (16.6) przybiera postać:

$$x + \sqrt{-3} = (a + b\sqrt{-3})^p. \tag{16.7}$$

Porównując moduły obu stron tego wzoru uzyskujemy, że $x^2 + 3 = (a^2 + 3b^2)^p$, skąd $y = a^2 + 3b^2$. Ponadto, ze wzoru dwumianowego Newtona mamy stąd, że

$$x + \sqrt{-3} =$$

$$= \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k} a^{p-2k} b^{2k} (-3)^k + \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-2k-1} b^{2k+1} (-3)^k \sqrt{-3}.$$

Wobec tego $1 = b \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-2k-1} b^{2k} (-3)^k$, więc $b \mid 1$, czyli $b = \pm 1$ i $b = \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-2k-1} (-3)^k$. Zatem $y = a^2 + 3$, a ponieważ y jest nieparzyste (bo $2 \mid x$ i $x^2 + 3 = y^p$), więc a jest parzyste i $y \equiv 3 \pmod 4$. Dalej, $-3 \equiv 1 \pmod 4$ i $a^{p-2k-1} = (a^2)^{\frac{p-1}{2}-k}$, więc dla $k < \frac{p-1}{2}$ jest: $4 \mid a^{p-2k-1}$. Wobec tego $b \equiv (-3)^{\frac{p-1}{2}} \equiv 1 \pmod 4$ i $b = \pm 1$, czyli $b = 1$. W ten sposób wykazaliśmy prawdziwość wzoru (16.5). Ponadto $y = a^2 + 3$ i $3 \nmid x$ oraz $x^2 + 3 = y^p$, więc $3 \nmid a$. Wobec tego $a^2 \equiv 1 \pmod 3$, skąd $a^{p-1} \equiv 1 \pmod 3$ i ze wzoru (16.5) uzyskujemy, że $1 \equiv pa^{p-1} \equiv p \pmod 3$, czyli $p \equiv 1 \pmod 3$. □

W pracy [13] Cohn zastosował dalej dość skomplikowane rozumowanie związane z wyliczaniem współczynników w rozwinięciu Taylora pewnej funkcji rzeczywistej. My dokończymy dowód twierdzenia Cohna metodami bardziej elementarnymi.

Stosujemy oznaczenia i rezultaty uzyskane w Lemacie 16.11 i jego dowodzie. Z lematu 16.11 i jego dowodu wynika, że $p = 2 \cdot 3^v s + 1$ dla pewnego $s \in \mathbb{N}$, przy czym $3 \nmid s$.

Najpierw pokażemy, że $3^{v+2} \mid \binom{p}{2k+1} (-3)^k a^{p-2k-1}$ dla każdego $k = 2, 3, \ldots, \frac{p-1}{2}$. W tym celu wystarczy wykazać, że $3^{v+2} \mid \binom{p}{2k+1} 3^k$. Ponadto $\binom{p}{2k+1} = \frac{p(p-1)}{(2k+1)\cdot 2k} \cdot \binom{p-2}{2k-1}$ i $3^v \mid p-1$ oraz na mocy lematu 16.7, $3^{k-1} \nmid (2k+1) \cdot 2k$, więc $(2k+1) \cdot 2k = 3^u V$ dla pewnych $u, V \in \mathbb{N}_0$ takich, że $u \leqslant k-2$ i $3 \nmid V$. Wobec tego rzeczywiście $3^{v+2} \mid \binom{p}{2k+1} 3^k$.

Stąd i na mocy wzoru (16.5), uzyskujemy zatem, że

$$1 \equiv pa^{p-1} - 3\binom{p}{3} a^{p-3} \pmod{3^{v+2}}. \tag{16.8}$$

Ponadto $3 \nmid a$, więc $a^2 \equiv 1, 4, 7 \pmod 9$. Dalej, $3\binom{p}{3} = \frac{p(p-1)(p-2)}{2} =$

$= 3^v s(p^2 - 2p) = 3^v s((p-1)^2 - 1) = 3^v s(4 \cdot 3^{2v} s^2 - 1) \equiv -3^v s \pmod{3^{v+2}}$, bo $v \in \mathbb{N}$.

Jeżeli $a^2 \equiv 1 \pmod 9$, to $(a^2)^{3^v} \equiv 1 \pmod{3^{v+2}}$ na mocy lematu 16.8, skąd $(a^2)^{3^v s} \equiv 1 \pmod{3^{v+2}}$, czyli $a^{p-1} \equiv 1 \pmod{3^{v+2}}$. Zatem wówczas $1 \equiv p + 3^v s a^{p-3} \pmod{3^{v+2}}$, czyli $-2 \cdot 3^v s \equiv 3^v s a^{p-3} \pmod{3^{v+2}}$. Stąd $-2 \equiv a^{p-3} \pmod 9$, ale $2 \mid p-3$ i $a^2 \equiv 1 \pmod 9$, więc $a^{p-3} \equiv 1 \pmod 9$ i wobec tego $-2 \equiv 1 \pmod 9$, co prowadzi do sprzeczności.

Niech teraz $a^2 \equiv 4 \pmod 9$. Wtedy z lematu 16.8, $(a^2)^{3^v} \equiv 4^{3^v} \pmod{3^{v+2}}$, skąd na mocy lematu 16.10, $a^{2 \cdot 3^v} \equiv 1 + 3^{v+1} \pmod{3^{v+2}}$. Stąd i ze wzoru dwumianowego Newtona mamy, że $a^{2 \cdot 3^v s} \equiv (1 + 3^{v+1})^s \equiv 1 + 3^{v+1} s \pmod{3^{v+2}}$, a więc $a^{p-1} \equiv 1 + 3^{v+1} s \pmod{3^{v+2}}$. Zatem $pa^{p-1} \equiv (2 \cdot 3^v s + 1)(1 + 3^{v+1} s) \equiv 1 + 3^{v+1} s + 2 \cdot 3^v s \equiv 1 + 5 \cdot 3^v s \pmod{3^{v+2}}$ i mamy, że $0 \equiv 5 \cdot 3^v s + 3^v s a^{p-3} \pmod{3^{v+2}}$, skąd $0 \equiv 5 + a^{p-3} \pmod 9$. Zatem $0 \equiv 5a^2 + a^{p-1} \pmod 9$, ale $a^2 \equiv 4 \pmod 9$ i $a^{p-1} \equiv 1 + 3^{v+1} s \pmod{3^{v+2}}$, więc $a^{p-1} \equiv 1 + 3^{v+1} s \pmod 9$ i stąd $0 \equiv 2 + 1 + 3^{v+1} s \equiv 3 \pmod 9$, czyli $9 \mid 3$, co prowadzi do sprzeczności.

W końcu, niech $a^2 \equiv 7 \pmod 9$. Wtedy na mocy lematu 16.10, $(a^2)^{3^v} \equiv 1 + 2 \cdot 3^{v+1} \pmod{3^{v+2}}$. Stąd i ze wzoru dwumianowego Newtona, $a^{2 \cdot 3^v s} \equiv (1 + 2 \cdot 3^{v+1})^s \equiv 1 + 2s3^{v+1} \pmod{3^{v+2}}$, a więc $a^{p-1} \equiv 1 + 2s3^{v+1} \pmod{3^{v+2}}$. Zatem $pa^{p-1} \equiv (2 \cdot 3^v s + 1)(1 + 2s3^{v+1}) \equiv 1 + 2s3^{v+1} + 2 \cdot 3^v s \equiv 1 + 8s3^v \equiv 1 - s3^v \pmod{3^{v+2}}$, skąd $1 \equiv 1 - 3^v s + 3^v s a^{p-3} \pmod{3^{v+2}}$. Zatem $3^v s \equiv 3^v a^{p-3} s \pmod{3^{v+2}}$ i $1 \equiv a^{p-3} \pmod 9$. Stąd $a^2 \equiv a^{p-1} \pmod 9$, ale $a^2 \equiv 7 \pmod 9$ i $a^{p-1} \equiv 1 + 2s3^{v+1} \pmod{3^{v+2}}$, więc $a^{p-1} \equiv 1 \pmod 9$ i $7 \equiv 1 \pmod 9$, co prowadzi do sprzeczności.

Tym samym, dowód twierdzenia Cohna został zakończony.

16.4 Wielkie twierdzenie Fermata dla wykładnika 3

Pierre de Fermat urodził się 17 sierpnia 1601 roku w Beaumont-de-Lomagne jako syn zamożnego i powszechnie szanowanego kupca Dominique'e Fermata. Pierre de Fermat z wykształcenia był prawnikiem,

a matematyką interesował się wyłącznie jako amator, jako intelektualną rozrywkę traktował lekturę dzieł matematyków greckich. Komentarze umieszczane na marginesie czytanych lektur oraz bogata korespondencja to jedyna spuścizna po Fermacie, który nie publikował wyników swojej pracy. Najsłynniejszy komentarz, później nazwany **Wielkim twierdzeniem Fermata**, zamieścił w latach 30. XVII wieku na marginesie łacińskiego przekładu *Arytmetyki* Diofantosa: „*Niemożliwością jest podzielenie sześcianu na dwa sześciany, czwartej potęgi na dwie czwarte potęgi i ogólnie potęgi wyższej niż druga na dwie takie potęgi. Odkryłem dowód prawdziwie zadziwiający, którego ten wąski margines nie pomieści.*" Dziś, stwierdzenie Fermata zapisalibyśmy następująco: równanie diofantyczne

$$x^n + y^n = z^n$$

nie posiada rozwiązań dla $n \geqslant 3$. W pismach, które pozostawił po sobie Fermat nie odnajdziemy śladu dowodu wspomnianej hipotezy, a nie znając go, nie możemy ocenić na ile mógł on być poprawny. Być może Pierre de Fermat wierzył, że odkrył poprawny dowód, ale bardziej prawdopodobnym jest, że znalazł w swoim dowodzie błąd lub uznał go niepełnym. Faktem jest, że podejmowane przez wiele pokoleń matematyków próby udowodnienia Wielkiego twierdzenia Fermata przyczyniły sie do rozwoju nowych gałęzi matematyki na czele z algebraiczną teorią liczb. Ostatecznie dowód hipotezy Fermata przedstawił Andrew Wiles w 1995 w pracy [41]. Wielkie twierdzenie Fermata, i jego historia, są tematem wielu ciekawych monografii, zainteresowanych czytelników odsyłamy, na przykład, do [1] i [34].

W tym paragrafie udowodnimy Wielkie twierdzenie Fermata dla $n = 3$.

Udowodnimy najpierw techniczny, lecz bardzo użyteczny

Lemat 16.12. *Niech $c, x, y \in \mathbb{Z}$, $3 \mid y$ i $\mathrm{NWD}(x, y) = 1$. Jeżeli $x^2 - 3xy + 3y^2 = c^3$, to istnieją względnie pierwsze liczby całkowite t i s takie, że $y = 3st(s - t)$.*

Dowód. Z założenia wynika, że $3 \nmid x$. Wobec tego $3 \nmid b$. Niech $\alpha = (x - y) - y\omega$. Ponieważ $\mathrm{NWD}(x - y, -y) = \mathrm{NWD}(x, y) = 1$ oraz $x - y \not\equiv -y \pmod 3$, gdyż $3 \nmid x$, więc na mocy lematu 16.1 elementy α

i $\overline{\alpha}$ są względnie pierwsze w pierścieniu Eisensteina. Jednak $\alpha \cdot \overline{\alpha} = N(\alpha) = (x-y)^2 - (x-y)y + y^2 = x^2 - 3xy + 3y^2 = c^3$, więc na mocy twierdzenia 13.20, $\alpha = u\beta^3$ dla pewnego $\beta \in \mathbb{Z}[\omega]$ i pewnego $u \in (\mathbb{Z}[\omega])^*$. Ponadto $-1 = (-1)^3$, więc ze wzoru (13.13) wystarczy rozpatrzeć przypadki, gdy $u \in \{1, \omega, \omega^2\}$ oraz $\beta = a + b\omega$ dla pewnych $a, b \in \mathbb{Z}$. Gdyby liczby a i b nie były względnie pierwsze, to istniałaby liczba pierwsza p taka, że $p \mid a$ i $p \mid b$. Wtedy $p \mid u\beta^3$, skąd $p \mid \alpha$, czyli $p \mid x-y$ i $p \mid -y$, co przeczy temu, że $\mathrm{NWD}(x-y, -y) = 1$. Zatem liczby a i b są względnie pierwsze. Jeżeli $u \in \{\omega, \omega^2\}$, to ze wzorów (16.3) i (16.4) wynika, że $3 \mid x - y$ lub $3 \mid x - 2y$. Ponadto $3 \mid y$, więc wtedy $3 \mid x$, co prowadzi do sprzeczności. Wobec tego $u = 1$ i ma mocy (16.2), $-y = 3ab(a+b)$, skąd $y = 3a(-b)(a-(-b))$. Zatem wystarczy obrać $s = a$ i $t = -b$. □

Twierdzenie 16.13. *Równanie*

$$x^3 + y^3 = z^3 \tag{16.9}$$

nie posiada rozwiązania w niezerowych liczbach całkowitych x, y, z.

Dowód. Załóżmy, że tak nie jest. Wtedy na mocy zasady minimum istnieją liczby całkowite x, y, z spełniające równanie (16.9) i takie, że $|xyz|$ jest minimalne. Wówczas liczby x, y, z są parami względnie pierwsze.

Z twierdzenia Sophie-Germain wynika, że pewna z liczb x, y, z jest podzielna przez 3. Jeśli $3 \mid x$, to $z^3 + (-y)^3 = x^3$ i $|z(-y)x| = |xyz|$, a jeśli $3 \mid y$, to $z^3 + (-x)^3 = y^3$ i $|z(-x)y| = |xyz|$. Uwzględniając to, że liczby x, y, z są parami względnie pierwsze, bez zmniejszania ogólności rozważań możemy zatem dalej zakładać, że $3 \mid z$, $3 \nmid x$ oraz $3 \nmid y$. Ponadto z Małego twierdzenia Fermata, $x^3 \equiv x \pmod 3$ i $y^3 \equiv y \pmod 3$ oraz $3 \mid z$, więc $3 \mid x + y$. Bez zmniejszania ogólności możemy dalej zakładać, że $x \equiv 1 \pmod 3$ oraz $y \equiv 2 \pmod 3$. Zauważmy, że $x^2 - xy + y^2 = (x+y)^3 - 3xy$ i $3 \mid x+y$, więc $9 \mid (x+y)^3$ oraz $3 \mid x^2 - xy + y^2$. Jeśli więc $9 \mid x^2 - xy + y^2$, to $9 \mid 3xy$, skąd $3 \mid xy$, a zatem $3 \mid x$ lub $3 \mid y$, co prowadzi do sprzeczności. Wobec tego liczba $x^2 - xy + y^2$ jest podzielna przez 3 i nie jest podzielna przez 9. Dalej, $z^3 = x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ i $27 \mid z^3$, skąd $27 \mid (x+y)(x^2 - xy + y^2)$. Dlatego $9 \mid x+y$ oraz $x + y = 9r$ oraz $x^2 - xy + y^2 = 3s$ dla pewnych niezerowych $r, s \in \mathbb{Z}$.

Pokażemy, że liczby r i s są względnie pierwsze. Gdyby tak nie było to dla pewnej liczby pierwszej p mielibyśmy, że $p \mid r$ i $p \mid s$. Ponadto $9 \nmid x^2-xy+y^2$, więc $p \neq 3$. Dalej, $p \mid x+y$ i $p \mid x^2-xy+y^2 = (x+y)^2-3xy$, więc $p \mid xy$, skąd $p \mid x$ lub $p \mid y$. Dodatkowo $p \mid x+y$, więc $p \mid x$ i $p \mid y$, co przeczy względnej pierwszości liczb x i y. Wobec tego liczby r i s są względnie pierwsze i $rs = (\frac{z}{3})^3$ oraz $\frac{z}{3} \in \mathbb{Z}$. Zatem z twierdzenia 1.28 wynika, że $r = a^3$ oraz $s = b^3$ dla pewnych $a, b \in \mathbb{Z}$ oraz $x + y = 9a^3$ i $x^2 - xy + y^2 = 3b^3$, przy czym liczby a i b są niezerowe i względnie pierwsze oraz $3 \nmid b$.

Dalej, $y = 9a^3 - x$, więc $3b^3 = x^2 + x^2 - 9a^3x + 81a^6 - 18a^3x + x^2$, skąd

$$x^2 - 3(3a^3)x + 3(3a^3)^2 = b^3.$$

Dodatkowo $\mathrm{NWD}(x, 3a^3) = \mathrm{NWD}(x, 3(x + y)) = \mathrm{NWD}(x, 3y) = 1$, gdyż $3 \nmid x$ i $\mathrm{NWD}(x, y) = 1$ oraz $3 \mid 3a^3$, więc z lematu 16.12 istnieją względnie pierwsze liczby całkowite s i t takie, że $3a^3 = 3st(s - t)$. Stąd $st(s - t) = a^3$, a ponieważ liczby $s.t, s - t$ są parami względnie pierwsze, więc z twierdzenia 1.29 wynika, że $s = u^3$, $t = v^3$ i $s - t = w^3$ dla pewnych $u, v, w \in \mathbb{Z}$. Ponadto $u, v, w \neq 0$, bo $a \neq 0$. Zatem $u^3-v^3 = w^3$, czyli $v^3+w^3 = u^3$. Z minimalności $|z|$ wynika, że $|u| \geqslant |z|$. Tymczasem mamy, że $|u|^3 = |s| \leqslant |st(s-t)| = |a|^3 = |r| \leqslant |rs| = |\frac{z}{3}|^3$, więc $|u| \leqslant \frac{|z|}{3} < |z|$, co prowadzi do sprzeczności. □

Twierdzenie 16.14. *Równanie $x^3 + y^3 = 4z^3$ nie posiada rozwiązania w liczbach całkowitych x, y, z takich, że $z \neq 0$.*

Dowód. Przypuśćmy, że tak nie jest. Wtedy z zasady minimum istnieje $z \in \mathbb{Z} \setminus \{0\}$ takie, że $4z^3 = x^3 + y^3$ dla pewnych $x, y \in \mathbb{Z}$ oraz $|z|$ jest najmniejsze. Wtedy liczby x, y, z są parami względnie pierwsze. Wobec tego $2 \nmid x$ i $2 \nmid y$, ale $4 \mid (x + y)(x^2 - xy + y^2)$ i liczba $x^2 - xy + y^2$ jest nieparzysta, więc $4 \mid x + y$. Zauważmy, że dla każdego $a \in \mathbb{Z}$ jest $a^3 \equiv -1, 0, 1 \pmod 9$, przy czym $a^3 \equiv 0 \pmod 9$ wtedy i tylko wtedy, gdy $3 \mid a$. Zatem jeśli $3 \nmid z$, to $4z^3 \equiv \pm 4 \pmod 9$ oraz $x^3+y^3 \equiv$ $\equiv -2, -1, 0, 1, 2 \pmod 9$. Zatem wtedy $\pm 4 \equiv -2, -1, 0, 1, 2 \pmod 9$, co jest niemożliwe. Wobec tego $3 \mid z$. Dalej, $x^3 \equiv x \pmod 3$ i $y^3 \equiv y \pmod 3$, więc $x^3 + y^3 \equiv x + y \pmod 3$, skąd $x + y \equiv 0 \pmod 3$.

Dalej $(x+y)(x^2-xy+y^2)=4z^3$, czyli $27 \mid (x+y)(x^2-xy+y^2)$, ale $x^2-xy+y^2=(x+y)^2-3xy$, więc $3 \mid x^2-xy+y^2$. Jeśli $9 \mid x^2-xy+y^2$, to ponieważ $9 \mid (x+y)^2$, więc $9 \mid 3xy$, skąd $3 \mid x$ lub $3 \mid y$. Ponadto $3 \mid x+y$, więc $3 \mid x$ i $3 \mid y$, co przeczy temu, że $\mathrm{NWD}(x,y)=1$. Wobec tego $9 \nmid x^2-xy+y^2$ i $9 \mid x+y$. Zatem $\frac{z}{3}, \frac{x+y}{9}, \frac{x^2-xy+y^2}{3} \in \mathbb{Z}$ oraz

$$\frac{x+y}{9} \cdot \frac{x^2-xy+y^2}{3} = 4\left(\frac{z}{3}\right)^3.$$

Ponadto, $4 \mid x+y$, a ponieważ liczby 4 i 9 są względnie pierwsze i dzielą liczbę $x+y$, więc $\frac{x+y}{36} \in \mathbb{Z}$ oraz

$$\frac{x+y}{36} \cdot \frac{x^2-xy+y^2}{3} = \left(\frac{z}{3}\right)^3.$$

Przypuśćmy, że liczby $\frac{x+y}{36}$ i $\frac{x^2-xy+y^2}{3}$ nie są względnie pierwsze. Wtedy istnieje ich wspólny dzielnik pierwszy p, ale $3 \nmid \frac{x^2-xy+y^2}{3}$, więc $p \neq 3$ oraz $p \mid x+y$ i $p \mid x^2-xy+y^2$, skąd $p \mid 3x^2$, czyli $p \mid x$. Lecz $p \mid x+y$, a zatem $p \mid y$, co przeczy temu, że $\mathrm{NWD}(x,y)=1$. Wobec tego liczby $\frac{x+y}{36}$ i $\frac{x^2-xy+y^2}{3}$ są względnie pierwsze i z twierdzenia 1.28 istnieją $a,b \in \mathbb{Z}$ takie, że $\frac{x+y}{36}=a^3$ i $\frac{x^2-xy+y^2}{3}=b^3$. Ponieważ $2 \nmid x$ i $3 \nmid x$ oraz $\mathrm{NWD}(x,y)=1$, więc stąd $\mathrm{NWD}(a,x)=1$. Ponadto $b^3=\frac{(x+y)^2-3xy}{3}=\frac{(x+y)^2}{3}-xy$ oraz $y=36a^3-x$, więc $b^3=\frac{(36a^3)^2}{3}-$ $+x(36a^3-x)=x^2-36a^3x+12\cdot 36a^6$. Stąd

$$x^2-3(12a^3)x+3(12a^3)^2=b^3.$$

Ponadto, $\mathrm{NWD}(x,12a^3)=1$, bo $2 \nmid x$, $3 \nmid x$ i $\mathrm{NWD}(a,x)=1$, więc z lematu 16.12 istnieją względnie pierwsze liczby całkowite s i t takie, że $12a^3=3st(s-t)$, czyli $st(s-t)=4a^3$. Liczby $s,t,s-t$ są parami względnie pierwsze, więc dokładnie jedna z nich jest podzielna przez 4. Bez zmniejszania ogólności możemy zakładać, że $4 \mid s$ lub $4 \mid s-t$. W pierwszym przypadku $\frac{s}{4}t(s-t)=a^3$, więc z twierdzenia 13.20 istnieją liczby całkowite u,v,w takie, że $\frac{s}{4}=u^3$, $t=v^3$ i $s-t=w^3$, skąd $v^3+w^3=4u^3$. Jeśli $u=0$, to $a=0$, skąd $x+y=0$ i $z=0$, wbrew założeniu. Zatem $u \neq 0$ i z minimalności $|z|$, $|u| \geqslant |z|$. Tymczasem $|u|^3 \leqslant |a|^3 \leqslant |a|^3|b|^3=\left(\frac{|z|}{3}\right)^3$, skąd $|u|<|z|$ i mamy sprzeczność.

Podobnie w drugim przypadku, $st\frac{s-t}{4} = a^3$, więc znowu z twierdzenia 13.20 istnieją liczby całkowite u, v, w takie, że $s = u^3$, $t = v^3$ i $\frac{s-t}{4} = w^3$, skąd $u^3 + (-v)^3 = 4w^3$. Jeśli $w = 0$, to $a = 0$, skąd $z = 0$, wbrew założeniu. Wobec tego $w \neq 0$ i z minimalności $|z|$ mamy, że $|w| \geqslant |z|$. Tymczasem $|w|^3 \leqslant |a|^3 \leqslant |a|^3|b|^3 = \left(\frac{|z|}{3}\right)^3$, skąd $|w| < |z|$ i mamy sprzeczność.

Przypuszczenie, że istnieją liczby całkowite x, y, z takie, że $z \neq 0$ i $x^3 + y^3 = 4z^3$ doprowadziło nas zatem do sprzeczności. Wobec tego takich liczb całkowitych nie ma. □

Z udowodnionego twierdzenia wynika, że **liczba** 4 **nie jest sumą sześcianów dwóch liczb wymiernych**.

Wniosek 16.15. *Wszystkimi rozwiązaniami w liczbach całkowitych x, y, z równania $x^3 + y^3 = 4z^3$ są trójki: $(k, -k, 0)$, gdzie $k \in \mathbb{Z}$.*

Dowód. Oczywiście $k^3 + (-k)^3 = 4 \cdot 0^3$ dla każdego $k \in \mathbb{Z}$. Jeżeli zaś $x^3 + y^3 = 4z^3$ oraz $x, y, z \in \mathbb{Z}$, to na mocy twierdzenia 16.14, $z = 0$, skąd $y^3 = (-x)^3$, a zatem $y = -x$. □

Z wniosku 16.15 otrzymujemy od razu następujące wnioski:

Wniosek 16.16. *Jedynym rozwiązaniem w liczbach całkowitych x, y równania $x^3 - 4y^3 = 1$ jest $x = 1$ i $y = 0$.*

Wniosek 16.17. *Jedynym rozwiązaniem w liczbach całkowitych x, y równania $x^3 - 4y^3 = -1$ jest $x = -1$ i $y = 0$.*

Zadanie 16.18. Stosując metodę podaną w dowodzie twierdzenia 16.14 uzasadnij, że jeżeli $x, y, z \in \mathbb{Z}$ i $x^3 + y^3 = 3z^3$, to $z = 0$ i $y = -x$.

Rozdział 17

Twierdzenie Ramanujana-Nagella

17.1 Podstawowe wiadomości i spostrzeżenia

Z teorii liczb wiemy, że jeśli $p \in \mathbb{P}$ i $M_p = 2^p - 1 \in \mathbb{P}$, to M_p nazywamy liczbą pierwszą Mersenna i wówczas liczba trójkątna $\frac{M_p(M_p+1)}{2}$ jest tak zwaną liczbą doskonałą, czyli taką liczbą naturalną, która jest sumą wszystkich swoich właściwych dzielników. Około 1919 roku genialny matematyk hinduski S. A. Ramanujana postawił hipotezę, że jedynie skończenie wiele liczb M_p to liczby trójkątne.

Jeśli M_p jest liczbą trójkątną, to $M_p = \frac{n(n+1)}{2}$ dla pewnego $n \in \mathbb{N}$, skąd $2^p - 1 = \frac{n(n+1)}{2}$, czyli $2^{p+3} - 8 = 4n^2 + 4n$, a zatem $(2n+1)^2 + 7 = 2^{p+3}$. W naturalny sposób pojawia się zatem następujące równanie:

$$x^2 + 7 = 2^y, \quad \text{gdzie, } x, y \in \mathbb{N}. \tag{17.1}$$

W 1948 roku T. Nagell rozwiązał hipotezę Ramanujana udowadniając w [29] następujące

Twierdzenie 17.1. *Wszystkimi liczbami naturalnymi x spełniającymi dla pewnego $y \in \mathbb{N}$ równanie* (17.1) *są* $x = 1, 3, 5, 11, 181$.

Ten wynik jest nazywany **Twierdzeniem Ramanujana-Nagella**. Naszym celem będzie podanie elementarnego dowodu tego twierdzenia. Rozpoczynamy od podstawowych spostrzeżeń i uwag stanowiących fundament dla głównego rozumowania, które będzie przedstawione w drugim paragrafie.

Po pierwsze zauważmy, że z równania (17.1), dla $x = 1$ uzyskujemy $y = 3$, dla $x = 3$ jest $y = 4$, dla $x = 5$ mamy $y = 5$, dla $x = 11$ jest $y = 7$, a dla $x = 181$ mamy $y = 15$. Należy zatem pokazać, że to równanie nie posiada innego rozwiązania w liczbach naturalnych.

Jeśli $x, y \in \mathbb{N}$ i $x > 1$ oraz $x^2 + 7 = 2^y$, to $2^y > 1 + 7 = 2^3$, więc $y > 3$. Ponadto x jest nieparzyste. Jeśli y jest parzyste, to $y = 2t$ dla pewnego $t \in \mathbb{N}$ i wtedy $7 = (2^t - x)(2^t + x)$, skąd $2^t + x = 7$ i $2^t - x = 1$, a zatem $2x = 6$ i $x = 3$ oraz $t = 2$. Możemy zatem dalej rozważać jedynie nieparzyste $y > 3$. Ponadto $7 \nmid x$, bo inaczej $7 \mid 2^y$, co jest niemożliwe. Podstawiając $z = y - 2$ uzyskujemy, że z jest nieparzyste i $z > 1$ oraz z nieparzystości x, w pierścieniu euklidesowym $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ równanie (17.1) możemy zapisać w postaci:

$$\frac{x + \sqrt{-7}}{2} \cdot \frac{x - \sqrt{-7}}{2} = 2^z. \tag{17.2}$$

Jeśli istnieje element pierwszy π pierścienia $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ będący wspólnym dzielnikiem elementów $\frac{x+\sqrt{-7}}{2}$ i $\frac{x-\sqrt{-7}}{2}$, to π jest dzielnikiem różnicy tych elementów i ich sumy, czyli $\pi \mid \sqrt{-7}$ i $\pi \mid x$, ale $-7 = (\sqrt{-7})^2$, więc $\pi \mid 7$. Ponadto $7 \nmid x$, więc $1 = 7k + xl$ dla pewnych $k, l \in \mathbb{Z}$, skąd $\pi \mid 1$ i mamy sprzeczność. Wobec tego elementy $\frac{x+\sqrt{-7}}{2}$ i $\frac{x-\sqrt{-7}}{2}$ są względnie pierwsze w pierścieniu $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

Ponadto w tym pierścieniu, $2 = \frac{1+\sqrt{-7}}{2} \cdot \frac{1-\sqrt{-7}}{2}$, przy czym elementy $\frac{1+\sqrt{-7}}{2}$ i $\frac{1-\sqrt{-7}}{2}$ mają normy równe 2, więc zgodnie z przykładem 13.12 są one elementami pierwszymi pierścienia $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Dodatkowo ze wzoru (13.17) elementami odwracalnymi pierścienia $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ są jedynie 1 i -1, więc elementy $\frac{1+\sqrt{-7}}{2}$ i $\frac{1-\sqrt{-7}}{2}$ nie są stowarzyszone w tym pierścieniu. Zatem równanie (17.2) przybiera postać:

$$\frac{x + \sqrt{-7}}{2} \cdot \frac{x - \sqrt{-7}}{2} = \left(\frac{1 + \sqrt{-7}}{2}\right)^z \cdot \left(\frac{1 - \sqrt{-7}}{2}\right)^z. \tag{17.3}$$

Ze zrobionych wyżej spostrzeżeń oraz z jednoznaczności rozkładu pierścienia $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ na mocy (17.3) wynika, że $\frac{x+\sqrt{-7}}{2} = u\left(\frac{1+\sqrt{-7}}{2}\right)^z$ lub $\frac{x+\sqrt{-7}}{2} = u\left(\frac{1-\sqrt{-7}}{2}\right)^z$ dla pewnego $u \in \{1, -1\}$.

W pierwszym przypadku mamy, że $\frac{x-\sqrt{-7}}{2} = \overline{\frac{x+\sqrt{-7}}{2}} = u\left(\frac{1-\sqrt{-7}}{2}\right)^z$, skąd $u\frac{x+\sqrt{-7}}{2} = \left(\frac{1+\sqrt{-7}}{2}\right)^z$ i $u\frac{x-\sqrt{-7}}{2} = \left(\frac{1-\sqrt{-7}}{2}\right)^z$, więc

$$u\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^z - \left(\frac{1-\sqrt{-7}}{2}\right)^z.$$

Podobnie, w drugim przypadku $u\sqrt{-7} = \left(\frac{1-\sqrt{-7}}{2}\right)^z - \left(\frac{1+\sqrt{-7}}{2}\right)^z$, czyli $(-u)\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^z - \left(\frac{1-\sqrt{-7}}{2}\right)^z$. Ponadto $u, -u \in \{1, -1\}$, więc ostatecznie mamy zależność:

$$\left(\frac{1+\sqrt{-7}}{2}\right)^z - \left(\frac{1-\sqrt{-7}}{2}\right)^z = \pm\sqrt{-7}. \tag{17.4}$$

Dalej, zauważmy, że

$$\left(\frac{1-\sqrt{-7}}{2}\right)^2 = \frac{-3-\sqrt{-7}}{2}$$

oraz

$$\left(\frac{1+\sqrt{-7}}{2}\right)^2 - 1 = \left(\frac{1+\sqrt{-7}}{2} - 1\right) \cdot \left(\frac{1+\sqrt{-7}}{2} + 1\right) =$$

$$= \frac{1-\sqrt{-7}}{2} \cdot \frac{-3-\sqrt{-7}}{2},$$

więc w pierścieniu $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$:

$$\left(\frac{1+\sqrt{-7}}{2}\right)^2 \equiv 1 \pmod{\left(\frac{1-\sqrt{-7}}{2}\right)^2}$$

i na mocy (17.4) oraz z nieparzystości z mamy kongruencję:

$$\frac{1+\sqrt{-7}}{2} \equiv \pm\sqrt{-7} \pmod{\left(\frac{1-\sqrt{-7}}{2}\right)^2}.$$

Dodatkowo $\frac{1+\sqrt{-7}}{2} - \sqrt{-7} = \frac{1-\sqrt{-7}}{2}$ nie jest podzielne przez $\left(\frac{1-\sqrt{-7}}{2}\right)^2$, więc po pomnożeniu obu stron przez 2^z wzór (17.4) przybiera postać:

$$(1+\sqrt{-7})^z - (1-\sqrt{-7})^z = -2^z\sqrt{-7}. \tag{17.5}$$

Ze wzoru dwumianowego Newtona i z nieparzystości z mamy, że

$$(1+\sqrt{-7})^z = \sum_{k=0}^{\frac{z-1}{2}} (-1)^k \binom{z}{2k} 7^k + \sqrt{-7} \cdot \sum_{k=0}^{\frac{z-1}{2}} (-1)^k \binom{z}{2k+1} 7^k,$$

więc po zastosowaniu sprzężenia,

$$(1-\sqrt{-7})^z = \sum_{k=0}^{\frac{z-1}{2}} (-1)^k \binom{z}{2k} 7^k - \sqrt{-7} \cdot \sum_{k=0}^{\frac{z-1}{2}} (-1)^k \binom{z}{2k+1} 7^k$$

i na mocy (17.5) uzyskujemy, że

$$2\sqrt{-7} \cdot \sum_{k=0}^{\frac{z-1}{2}} (-1)^k \binom{z}{2k+1} 7^k = -2^z\sqrt{-7},$$

czyli:

$$\sum_{k=0}^{\frac{z-1}{2}} (-1)^k \binom{z}{2k+1} 7^k = -2^{z-1}. \tag{17.6}$$

Ze wzoru (17.6) otrzymujemy kongruencję:

$$2^{z-1} \equiv -z \pmod 7. \tag{17.7}$$

Lemat 17.2. *Jeśli liczba naturalna nieparzysta z spełnia kongruencję* (17.7)*, to* $z \equiv 3, 5, 13 \pmod{42}$.

Dowód. Zauważmy, że $2^3 \equiv 1 \pmod 7$, więc $2^{3t} \equiv 1 \pmod 7$ dla każdego $t \in \mathbb{N}$. Ponieważ z jest nieparzyste i $z \in \mathbb{N}$, więc $z = 6k+1$ lub $z = 6k+3$ lub $z = 6k+5$ dla pewnego $k \in \mathbb{N}_0$.

Niech $z = 6k+1$. Wtedy $2^{z-1} = 2^{6k} \equiv 1 \pmod 7$, więc $1 \equiv -6k-1 \pmod 7$, skąd $2 \equiv k \pmod 7$. Zatem $k = 7l+2$ dla pewnego $l \in \mathbb{N}_0$ i $z = 42l+13$, czyli $z \equiv 13 \pmod{42}$.

Niech $z = 6k + 3$. Wtedy $2^{z-1} = 4 \cdot 2^{6k} \equiv 4 \pmod 7$, więc $4 \equiv$ $\equiv -6k - 3 \pmod 7$, skąd $0 \equiv k \pmod 7$. Zatem $k = 7l$ dla pewnego $l \in \mathbb{N}_0$ i $z = 42l + 3$, czyli $z \equiv 3 \pmod{42}$.

Niech $z = 6k + 5$. Wtedy $2^{z-1} = 16 \cdot 2^{6k} \equiv 2 \pmod 7$, więc $2 \equiv$ $\equiv -6k - 5 \pmod 7$, skąd $0 \equiv k \pmod 7$. Zatem $k = 7l$ dla pewnego $l \in \mathbb{N}_0$ i $z = 42l + 5$, czyli $z \equiv 5 \pmod{42}$. □

17.2 Dowód twierdzenia Ramanujana-Nagella

Przypuśćmy, że istnieje liczba naturalna $x \neq 1, 3, 5, 11, 181$ oraz istnieje $y \in \mathbb{N}$ takie, że $x^2 + 7 = 2^y$. Wtedy z poprzedniego paragrafu wiemy, że $z = y - 2$ jest nieparzystą liczbą naturalną różną od 1, 3, 5 i 13, $z \equiv 3, 5, 13 \pmod{42}$, x jest nieparzyste i zachodzi wzór (17.6).

Rozważmy najpierw przypadek, gdy $z \equiv 3 \pmod{42}$. Ponieważ $z \neq 3$, więc istnieje największa liczba naturalna t taka, że $7^t \mid z - 3$. Stąd $z - 3 = 7^t \cdot 6 \cdot h$ dla pewnego naturalnego h, takiego, że $7 \nmid h$. Zauważmy, że dla $k = 2, \ldots, \frac{z-1}{2}$ zachodzi wzór:

$$\binom{z}{2k+1} = \frac{z(z-1)(z-2)(z-3)}{(2k+1)2k(2k-1)(2k-2)} \cdot \binom{z-4}{2k-3}. \tag{17.8}$$

Spośród czterech kolejnych liczb naturalnych: $2k-2, 2k-1, 2k, 2k+1$ tylko jedna liczba może być podzielna przez 7. Stąd jeśli 7^{k-1} dzieli iloczyn tych liczb, to dzieli jedną z nich, a więc $7^{k-1} \leqslant 2k + 1$. Jednak $k \geqslant 2$, więc $7^{k-1} = (1+6)^{k-1} \geqslant 1 + 6(k-1) > 2k + 1$. Stąd i ze wzoru (17.8) wynika, że dla takich k liczba $(-1)^k \binom{z}{2k+1} 7^k$ jest podzielna przez 7^{t+1}, gdyż $7^t \mid z - 3$. Ze wzoru (17.6) uzyskujemy zatem, że $z - 7\binom{z}{3} \equiv$ $\equiv -2^{z-1} \pmod{7^{t+1}}$. Oznaczmy $A = 7\binom{z}{3} = 7^{\frac{z(z-1)(z-2)}{6}}$. Wtedy $6A =$ $= 7(3 + 7^t \cdot 6 \cdot h)(2 + 7^t \cdot 6 \cdot h)(1 + 7^t \cdot 6 \cdot h) \equiv 3 \cdot 2 \cdot 7 \pmod{7^{t+1}}$, co wobec $\mathrm{NWD}(6, 7^{t+1}) = 1$ daje $A \equiv 7 \pmod{7^{t+1}}$. Wobec tego $z - 7 \equiv$ $\equiv -2^{z-1} \pmod{7^{t+1}}$. Z twierdzenia Eulera mamy, że $2^{\varphi(7^{t+1})} \equiv 1$ $\pmod{7^{t+1}}$ i $\varphi(7^{t+1}) = 6 \cdot 7^t$, więc $2^{z-3} \equiv 1 \pmod{7^{t+1}}$, skąd $2^{z-1} \equiv 4$ $\pmod{7^{t+1}}$. Zatem $-2^{z-1} \equiv -4 \pmod{7^{t+1}}$ i $z - 7 \equiv -4 \pmod{7^{t+1}}$,

czyli $z-3 \equiv 0 \pmod{7^{t+1}}$. Wobec tego $7^{t+1} \mid z-3$, co przeczy maksymalności t.

Teraz rozpatrzmy przypadek, gdy $z \equiv 5 \pmod{42}$. Ponieważ $z \neq 5$, więc istnieje największa liczba naturalna t taka, że $7^t \mid z-5$. Wobec tego $z-5 = 7^t \cdot 6 \cdot h$ dla pewnego naturalnego h, takiego, że $7 \nmid h$. Zauważmy, że dla $k = 3, \ldots, \frac{z-1}{2}$ zachodzi wzór:

$$\binom{z}{2k+1} = \frac{z(z-1)(z-2)(z-3)(z-4)(z-5)}{(2k+1)2k(2k-1)(2k-2)(2k-3)(2k-4)} \cdot \binom{z-6}{2k-5}. \tag{17.9}$$

Spośród sześciu kolejnych liczb naturalnych: $2k-4, 2k-3, 2k-2$, $2k-1, 2k, 2k+1$ tylko jedna liczba może być podzielna przez 7. Stąd jeśli 7^{k-1} dzieli iloczyn tych liczb, to dzieli jedną z nich, a więc $7^{k-1} \leqslant \leqslant 2k+1$, co jak wiemy z przypadku pierwszego, jest niemożliwe. Stąd i ze wzoru (17.9) wynika, że dla takich k liczba $(-1)^k\binom{z}{2k+1}7^k$ jest podzielna przez 7^{t+1}, gdyż $7^t \mid z-3$. Ze wzoru (17.6) uzyskujemy zatem, że

$$z - 7\binom{z}{3} + 7^2\binom{z}{5} \equiv -2^{z-1} \pmod{7^{t+1}}. \tag{17.10}$$

Oznaczmy $A = 7\binom{z}{3} = 7\frac{z(z-1)(z-2)}{6}$. Wtedy $6A = 7(5+7^t \cdot 6 \cdot h)(4+7^t \cdot 6 \cdot h)(3+7^t \cdot 6 \cdot h) \equiv 5 \cdot 4 \cdot 3 \cdot 7 \pmod{7^{t+1}}$, co wobec $\mathrm{NWD}(6, 7^{t+1}) = 1$ daje $A \equiv 70 \pmod{7^{t+1}}$. Oznaczmy $B = 7^2 \cdot \binom{z}{5}$. Wtedy $B = 7^2 \cdot \cdot\frac{z(z-1)(z-2)(z-3)(z-4)}{120}$, więc $120B = 7^2 \cdot (5+7^t \cdot 6 \cdot h)(4+7^t \cdot 6 \cdot h)(3+ +7^t \cdot 6 \cdot h) \cdot (2+7^t \cdot 6 \cdot h)(1+7^t \cdot 6 \cdot h) \equiv 7^2 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \pmod{7^{t+1}}$, co wobec $\mathrm{NWD}(120, 7^{t+1}) = 1$ daje $B \equiv 7^2 \equiv 49 \pmod{7^{t+1}}$. Dodatkowo, jak pokazaliśmy w pierwszym przypadku, $2^{7^t \cdot 6h} \equiv 1 \pmod{7^{t+1}}$ i $z-1 = 4+7^t \cdot 6h$, więc $2^{z-1} \equiv 2^4 \equiv 16 \pmod{7^{t+1}}$. Podstawiając wyliczone wartości do wzoru (17.10) uzyskujemy, że $z-70+49 \equiv -16 \pmod{7^{t+1}}$. Stąd $z-5 \equiv 0 \pmod{7^{t+1}}$, czyli $7^{t+1} \mid z-5$, co przeczy maksymalności t.

W ostatnim przypadku, $z \equiv 13 \pmod{42}$. Ponieważ $z \neq 13$, więc istnieje największa liczba naturalna t taka, że $7^t \mid z-13$. Stąd $z-13 = = 7^t \cdot 6 \cdot h$ dla pewnego naturalnego h, takiego, że $7 \nmid h$. Zauważmy, że

dla $k = 7, \ldots, \frac{z-1}{2}$ zachodzi wzór:

$$\binom{z}{2k+1} = \frac{z(z-1)(z-2)(z-3)\cdot\ldots\cdot(z-13)}{(2k+1)2k(2k-1)\cdot\ldots\cdot(2k-12))} \cdot \binom{z-14}{2k-13}. \tag{17.11}$$

Spośród czternastu liczb naturalnych $2k-12, \ldots, 2k-1, 2k, 2k+1$ co najwyżej jedna jest podzielna przez 7^2 i co najwyżej dwie są podzielne przez 7. Stąd gdyby iloczyn tych liczb był podzielny przez 7^{k-1}, to jedna z nich byłaby podzielna przez 7^{k-2}, skąd $7^{k-2} \leqslant 2k+1$. Dla $k \geqslant 7$ ze wzoru Newtona: $7^{k-2} = (1+6)^{k-2} > 1 + 6(k-2) > 2k+1$, więc 7^{k-1} nie dzieli liczby $(2k-12)\cdot\ldots\cdot 2k(2k+1)$. Ponadto $7^t \mid z-13$, więc dla $k = 7, \ldots, \frac{z-1}{2}$ liczba $(-1)^k\binom{z}{2k+1}7^k$ jest podzielna przez 7^{t+1}. Ze wzoru (17.6) uzyskujemy zatem, że

$$7^{t+1} \mid z - 7\binom{z}{3} + 7^2\binom{z}{5} - 7^3\binom{z}{7} + 7^4\binom{z}{9} - 7^5\binom{z}{11} + 7^6\binom{z}{13} + 2^{z-1}. \tag{17.12}$$

Rozumując podobnie jak w poprzednich przypadkach uzyskamy, że

$$(-1)^k\binom{z}{2k+1}7^k \equiv (-1)^k\binom{13}{2k+1}7^k \pmod{7^{t+1}}$$

dla każdego $k = 1, 2, 3, 4, 5, 6$. Zatem $-7\binom{z}{3} + 7^2\binom{z}{5} - 7^3\binom{z}{7} + 7^4\binom{z}{9} - +7^5\binom{z}{11} + 7^6\binom{z}{13} \equiv -7\binom{13}{3} + 7^2\binom{13}{5} - 7^3\binom{13}{7} + 7^4\binom{13}{9} - 7^5\binom{13}{11} + 7^6\binom{13}{13} = = -4109 \pmod{7^{t+1}}$. Dodatkowo, $2^{7^t\cdot 6h} \equiv 1 \pmod{7^{t+1}}$ i $z - 1 = = 12 + 7^t \cdot 6h$, więc $2^{z-1} \equiv 2^{12} = 4096 \pmod{7^{t+1}}$. Stąd na mocy (17.12) mamy, że $z - 4109 \equiv -4096 \pmod{7^{t+1}}$, skąd $z - 13 \equiv 0 \pmod{7^{t+1}}$. Zatem $7^{t+1} \mid z - 13$, co przeczy maksymalności t.

W ten sposób dowód twierdzenia Ramanujana-Nagella został zatem zakończony.

Zadanie 17.3. Znajdź wszystkie rozwiązania w liczbach całkowitych x, y równania:

$$x^2 + x + 2 = y^5. \tag{17.13}$$

Rozdział 18

Równanie Mordella

18.1 Równania nieposiadające rozwiązania

Równaniem Mordella lub **równaniem Bacheta** nazywamy równanie diofantyczne postaci

$$x^2 + k = y^3,$$

gdzie $k \in \mathbb{Z} \setminus \{0\}$. Specjalny jego przypadek był rozpatrywany już przez Diofantosa w jego *Artmetyce*; mianowicie Problem VI.17 (sformułowany w terminach geometrycznych) polegał na znalezieniu takiej liczby naturalnej x, że $x^2 + 2$ jest sześcianem pewnej liczby naturalnej.

Mordell pisał, że „równanie Bacheta odegrało fundamentalną rolę w rozwoju teorii liczb"([25], s. 238). Było ono badane przez ostatnie 300 lat. Specjalne przypadki były rozwiązywane przez różnych matematyków, między innymi Euler przedstawił fundamentalną, nową ideę do rozwiązania równania $x^2 + 2 = y^3$, polegającą na zapisaniu go w postaci $(x + \sqrt{2}i)(x - \sqrt{2}i) = y^3$. Było to pierwsze użycie liczb zespolonych w Teorii Liczb.

W 1922 roku wielki matematyk filadelfijski Louis J. Mordell udowodnił, że dla każdej niezerowej liczby całkowitej k zbiór rozwiązań tego równania w liczbach całkowitych x i y jest skończony, a w latach 60. Baker i Stark podali ograniczenia górne na x i y w terminach

k, więc wszystkie rozwiązania dla danego k można znaleźć wykonując obliczenia na przykład na komputerze (por. [6]).

Twierdzenie 18.1. (Mordell). *Niech a i b będą liczbami całkowitymi takimi, że $2 \nmid a$, $2 \mid b$ i $3 \nmid b$. Jeżeli a i b nie posiadają wspólnego dzielnika pierwszego postaci $4k+3$ i $k = b^2 - a^3 \not\equiv -1 \pmod 8$, to równanie $x^2 + k = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Dowód. Załóżmy, że przy tych założeniach istnieją $x, y \in \mathbb{Z}$ takie, że $x^2+k = y^3$. Wtedy $x^2+b^2 = y^3+a^3$. Przypuśćmy, że x jest nieparzyste. Wtedy y jest parzyste i $y^3 + a^3 \equiv a^3 \pmod 8$ oraz $x^2 \equiv 1 \pmod 8$, więc $1+b^2 \equiv a^3 \pmod 8$, skąd $k = b^2-a^3 \equiv -1 \pmod 8$, co prowadzi do sprzeczności.

Wobec tego $2 \mid x$, a ponieważ $x^2+b^2 = y^3+a^3$, więc $2 \nmid y$, skąd $y^2 \equiv \equiv 1 \pmod 8$. Ponadto $y^3+a^3 = (y+a)(y^2-ay+a^2)$, liczba x^2-ax+a^2 jest nieparzysta i $4 \mid x^2+b^2$, więc $4 \mid y+a$, skąd $y \equiv -a \pmod 4$, czyli $-ay \equiv a^2 \equiv 1 \pmod 4$. Wobec tego $y^2 - ay + a^2 \equiv 1+1+1 \pmod 4$, czyli $y^2-ay+a^2 \equiv 3 \pmod 4$. Dalej, $y^2-ay+a^2 = (y-\frac{a}{2})^2+\frac{3}{4}a^2 > 0$, więc y^2-ay+a^2 jest nieparzystą liczbą naturalną większą od 1. Ponadto $y^2-ay+a^2 \equiv 3 \pmod 4$, więc y^2-ay+a^2 posiada dzielnik pierwszy $p \equiv \equiv 3 \pmod 4$, który wchodzi w rozwinięcie kanoniczne liczby y^2-ay+a^2 z nieparzystym wykładnikiem α. Stąd $p \mid x^2+b^2$, więc ze stwierdzenia 2.15: $p \mid x$ i $p \mid b$, ale $3 \nmid b$, więc $p \neq 3$. Dodatkowo $p^\alpha \mid x^2+b^2$ oraz $\alpha = 2\beta - 1$ dla pewnego $\beta \in \mathbb{N}$ oraz na mocy twierdzenia 14.18 liczba p wchodzi w rozkład kanoniczny liczby x^2+a^2 z parzystym wykładnikiem, więc $p^{2\beta} \mid y^3+a^3$, czyli $p^{\alpha+1} \mid (y+a)(y^2-ay+a^2)$. Ponadto $p^\alpha \nmid y^2-ay+a^2$, więc $p \mid y+a$. Zatem $y \equiv -a \pmod p$, skąd $y^2-ay+a^2 \equiv 3a^2 \pmod p$. Lecz $p \mid y^2-ay+a^2$, więc $p \mid 3a^2$ i jak pokazalismy, $p \neq 3$. Wobec tego $p \mid b$. Zatem liczby a i b mają wspólny dzielnik pierwszy $p \equiv 3 \pmod 4$, co prowadzi do sprzeczności.

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

Wniosek 18.2. *Jeżeli $k \in \{3, 5, 17, -11, -13, -23\}$, to równanie Mordella $x^2 + k = y^3$ nie posiada rozwiązania w liczbach całkowitych.*

Dowód. Zauważmy, że $3 = 2^2 - 1^3$, $5 = 2^2 - (-1)^3$, $17 = 4^2 - 1^3$, $-11 = 4^2 - 3^3$, $-13 = 70^2 - 17^3$ i $-23 = 2^2 - 3^3$ oraz spełnione są założenia twierdzenia 18.1. □

Lemat 18.3. *Każda liczba pierwsza p taka, że $p \equiv \pm 3 \pmod 8$ jest elementem pierwszym pierścienia $\mathbb{Z}[\sqrt{2}]$. W szczególności, dla dowolnych liczb całkowitych x i y: jeżeli $p \mid x^2 - 2y^2$, to $p \mid x$ i $p \mid y$.*

Dowód. Ponieważ jak wiemy pierścień $\mathbb{Z}[\sqrt{2}]$ jest euklidesowy z normą N taką, że $N(a + b\sqrt{2}) = |a^2 - 2b^2|$ i $N(p) = p^2 > 1$, więc wystarczy wykazać, ze p jest elementem nierozkładalnym. Załóżmy, że tak nie jest. Wtedy $p = \alpha \cdot \beta$ dla pewnych $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ takich, że $N(\alpha), N(\beta) > 1$. Stad $p^2 = N(\alpha) \cdot N(\beta)$, a ponieważ dodatkowo $N(\alpha), N(\beta) \in \mathbb{N}$, więc $N(\alpha) = p$. Dalej, $\alpha = a + b\sqrt{2}$ dla pewnych $a, b \in \mathbb{Z}$. Stąd $|a^2 - 2b^2| = p$, czyli $a^2 - 2b^2 = \pm p$. Wobec tego liczba a jest nieparzysta, skąd $a^2 \equiv 1 \pmod 8$, ale $p \equiv \pm 3 \pmod 8$, więc $1 - 2b^2 \equiv \pm 3 \pmod 8$. Zatem $2b^2 \equiv 6 \pmod 8$ lub $2b^2 \equiv 4 \pmod 8$, skąd $b^2 \equiv 3 \pmod 4$ lub $b^2 \equiv 2 \pmod 4$, co prowadzi do sprzeczności. Wobec tego p jest elementem pierwszym pierścienia $\mathbb{Z}[\sqrt{2}]$.

Weźmy teraz dowolne $x, y \in \mathbb{Z}$ takie, że $p \mid x^2 - 2y^2$. Ponieważ $x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2})$ i p jest elementem pierwszym w $\mathbb{Z}[\sqrt{2}]$, więc $p \mid x + y\sqrt{2}$ lub $p \mid x - y\sqrt{2}$. Zatem istnieją $c, d \in \mathbb{Z}$ takie, że $x + y\sqrt{2} = p(c + d\sqrt{2})$ lub $x - y\sqrt{2} = p(c + d\sqrt{2})$. Zatem $x = pc$ i $y = pd$ lub $x = pc$ i $-y = pd$. Wobec tego $p \mid x$ i $p \mid y$. □

Lemat 18.4. *Niech $p \equiv \pm 3 \pmod 8$ będzie liczbą pierwszą i niech $x, y \in \mathbb{Z}$ oraz niech $t \in \mathbb{N}_0$. Jeżeli $p^{2t+1} \mid x^2 - 2y^2$, to $p^{t+1} \mid x$ i $p^{t+1} \mid y$. W szczególności $p^{2t+2} \mid x^2 - 2y^2$.*

Dowód. Zastosujemy indukcję względem t. Dla $t = 0$ teza wynika z lematu 18.3. Przypuśćmy, że teza zachodzi dla pewnego $t \in \mathbb{N}_0$ i niech $p^{2t+3} \mid x^2 - 2y^2$ dla pewnych $x, y \in \mathbb{Z}$. Wtedy z założenia indukcyjnego $x = 2^{t+1}a$ i $y = 2^{t+1}b$ dla pewnych $a, b \in \mathbb{Z}$. Stąd $p^{2t+3} \mid p^{2t+2}a^2 - 2p^{2t+2}b^2$, skąd $p \mid a^2 - 2b^2$. Z lematu 18.3, $a = pc$ i $b = pd$ dla pewnych $c, d \in \mathbb{Z}$. Zatem $x = p^{t+2}c$ i $y = p^{t+2}d$, skąd $p^{2t+4} \mid x^2 - 2y^2$. Wobec tego teza zachodzi też dla $t + 1$, co kończy nasz dowód. □

Twierdzenie 18.5. *Niech a i b będą liczbami całkowitymi takimi, że $2 \nmid b$, $3 \nmid b$, $a \equiv 2 \pmod 8$ i liczby a i b nie posiadają wspólnego dzielnika pierwszego p takiego, że $p \equiv \pm 3 \pmod 8$. Wówczas równanie Mordella $x^2 + (a^3 - 2b^2) = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Dowód. Przypuśćmy, że istnieją $x, y \in \mathbb{Z}$ takie, że $x^2 + (a^3 - 2b^2) = y^3$. Jeśli liczba x jest parzysta, to y też jest parzyste i $x = 2k$ oraz $y = 2l$ dla pewnych $k, l \in \mathbb{Z}$, skąd $4k^2 + (a^3 - 2b^2) = 8l^3$. Wobec tego $4 \mid 4k^2 + (a^3 - 2b^2)$, skąd $4 \mid 2b^2$, co prowadzi do sprzeczności. Zatem liczba x jest nieparzysta. Stąd $x^2 \equiv 1 \pmod 8$ i liczba y też jest nieparzysta, skąd $y^2 \equiv 1 \pmod 8$. Zatem $y^3 \equiv y \pmod 8$ i wobec tego $y \equiv 1 - 2 \equiv 7 \pmod 8$. Dalej, $x^2 - 2b^2 = y^3 - a^3 = (y-a)(y^2 + ay + a^2)$ oraz $y - a \equiv 7 - 2 \equiv -3 \pmod 8$. Jeśli wszystkie dzielniki pierwsze liczby nieparzystej $y - a$ przystają jedynie do ± 1 modulo 8, to $y - a \equiv \pm 1 \pmod 8$, skąd $-3 \equiv \pm 1 \pmod 8$, co jest niemożliwe. Wobec tego liczba $y - a$ posiada dzielnik pierwszy p taki, że $p \equiv \pm 3 \pmod 8$. Jeśli wszystkie dzielniki pierwsze p liczby $y - a$ przystające do ± 3 modulo 8 mają parzyste wykładniki, to $y - a \equiv \pm 1 \pmod 8$, co też prowadzi do sprzeczności. Wobec tego istnieje liczba pierwsza $p \equiv \pm 3 \pmod 8$, która wchodzi w rozkład liczby $y - a$ na czynniki pierwsze z nieparzystym wykładnikiem α. Jednak $p^\alpha \mid x^2 - 2b^2$, więc z lematu 18.3, $p \mid b$ oraz z lematu 18.4, $p^{\alpha+1} \mid x^2 - 2b^2$. Wobec tego $p^{\alpha+1} \mid (y - a)(y^2 + ay + a^2)$, ale $p^{\alpha+1} \nmid y - a$, więc $p \mid y^2 + ay + a^2$. Mamy zatem, że $y \equiv a \pmod p$ i $0 \equiv y^2 + ay + a^2 \equiv 3a^2 \pmod p$. Stąd $p \mid 3a^2$, ale $p \mid b$, więc $p \neq 3$. Zatem $p \mid a$. Wobec tego liczba p jest wspólnym dzielnikiem pierwszym liczb a i b oraz $p \equiv \pm 3 \pmod 8$, co prowadzi do sprzeczności.

Przypuszczenie, że istnieją $x, y \in \mathbb{Z}$ takie, że $x^2 + (a^3 - 2b^2) = y^3$ doprowadziło nas do sprzeczności. Wobec tego równanie $x^2 + (a^3 - +2b^2) = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y. □

Ponieważ $6 = 2^3 - 2 \cdot 1^2$, $-42 = 2^3 - 2 \cdot 5^2$ i $-58 = 10^3 - 2 \cdot 23^2$, więc z twierdzenia 18.5 otrzymujemy od razu następujący

Wniosek 18.6. *Dla $k \in \{6, -42, -58\}$ równanie $x^2 + k = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Twierdzenie 18.7. *Niech a i b będą liczbami całkowitymi, które nie posiadają wspólnego dzielnika pierwszego postaci $4k+3$. Jeżeli $a \equiv 2 \pmod 4$ i $b \equiv \pm 1 \pmod 6$ oraz $k = b^2 - a^3$, to równanie Mordella $x^2 + k = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Dowód. Załóżmy, że $x^2 + k = y^3$ dla pewnych $x, y \in \mathbb{Z}$. Ponieważ $2 \nmid b$, więc $b^2 \equiv 1 \pmod 8$. Ponadto $a \equiv 2 \pmod 4$, skąd $a^3 \equiv 0 \pmod 8$ i wobec tego $k \equiv 1 \pmod 8$. Zatem jeśli $2 \nmid x$, to y jest parzyste, skąd $8 \mid x^2 + k$, ale wtedy $x^2 \equiv 1 \pmod 8$, więc $x^2 + k \equiv 2 \pmod 8$, co prowadzi do sprzeczności. Wobec tego $2 \mid x$. Stąd $2 \nmid y$. Zatem $y^2 \equiv 1 \pmod 8$, czyli $y^3 \equiv y \pmod 8$. Ponadto $x^2 \equiv 0, 4 \pmod 8$, więc $y \equiv 1 \pmod 8$ lub $y \equiv 5 \pmod 8$, czyli $y \equiv 1 \pmod 4$. Dalej, $x^2 + b^2 = y^3 + a^3$ i $y^3 + a^3 = (y+a)(y^2 - ay + a^2)$, skąd $x^2 + b^2 = (y+a)(y^2 - ay + a^2)$. Zauważmy, że $y + a \equiv 2 + 1 \equiv 3 \pmod 4$. Zatem liczba $y + a$ jest nieparzysta. Ponadto $x^2 + b^2 > 0$, bo $2 \nmid b$ i $y^2 - ay + y^2 = (y - \frac{a}{2})^2 + \frac{3}{4}a^2 \geqslant 0$, więc $y + a \geqslant 3$. Jeśli wszystkie dzielniki pierwsze liczby $y + a$ przystają do 1 modulo 4, to $y + a \equiv 1 \pmod 4$, co prowadzi do sprzeczności. Wobec tego liczba ta posiada dzielnik pierwszy przystający do 3 modulo 4. Gdyby każdy taki dzielnik pierwszy miał parzysty wykładnik w rozkładzie liczby $y + a$ na czynniki pierwsze, to $y + q \equiv 1 \pmod 4$, co jest niemozliwe. Zatem istnieje dzielnik pierwszy $p \equiv 3 \pmod 4$ liczby $y + a$, który wchodzi w rozkład kanoniczny tej liczby z wykładnikiem nieparzystym α. Stąd $p^\alpha \mid x^2 + b^2$, więc ze stwierdzenia 2.15 mamy, że $p \mid b$, ale $3 \nmid b$, więc $p \neq 3$. Ponadto na mocy twierdzenia 14.18 liczba p wchodzi w rozkład kanoniczny liczby $x^2 + b^2$ z parzystym wykładnikiem, więc $p^{\alpha+1} \mid y^3 + a^3$, czyli $p^{\alpha+1} \mid (y + a)(y^2 - ay + a^2)$. Ponadto $p^{\alpha+1} \nmid y + a$, więc $p \mid y^2 - ay + a^2$. Zatem $y \equiv -a \pmod p$ i stąd $0 \equiv y^2 - ay + a^2 \equiv 3a^2 \pmod p$. Stąd $p \mid 3a^2$, a ponieważ $p \neq 3$, to $p \mid a$. Wobec tego liczby a i b mają wspólny dzielnik pierwszy $p \equiv 3 \pmod 4$, co prowadzi do sprzeczności.

Przypuszczenie, że równanie $x^2 + k = y^3$ posiada rozwiązanie w liczbach całkowitych doprowadziło nas zatem do sprzeczności. Wobec tego to równanie nie posiada rozwiązania w liczbach całkowitych. □

Ponieważ $-7 = 1^2 - 2^3$, $9 = 1^2 - (-2)^3$ i $33 = 5^2 - (-2)^3$, więc na mocy twierdzenia 18.7 otrzymujemy od razu następujący

Wniosek 18.8. *Dla $k \in \{-7, 9, 33\}$ równanie $x^2 + k = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Twierdzenie 18.9. (Mordell). *Niech a i b będą liczbami całkowitymi, które nie posiadają wspólnego dzielnika pierwszego postaci $4k+3$. Jeżeli $a \equiv \pm 1 \pmod 6$ i $b \equiv 3 \pmod 4$ oraz $k = (2a)^2 - (2b)^3$, to równanie Mordella $x^2 + k = y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Dowód. Załóżmy, że $x^2 + k = y^3$ dla pewnych $x, y \in \mathbb{Z}$. Ponieważ $2 \nmid a$, więc $a^2 \equiv 1 \pmod 8$, skąd $k = (2a)^2 - (2b)^3 \equiv 4 \pmod 8$. Jeśli x jest parzyste, to y też jest parzyste, skąd $x = 2u$ i $y = 2v$ dla pewnych $u, v \in \mathbb{Z}$ oraz $4u^2+4a^2-8b^3 = 8v^3$. Zatem $u^2+a^2-2b^3 = 2v^3$. Stąd $2 \nmid u$ i $u^2 \equiv 1 \pmod 8$, a zatem $u^2 + a^2 - 2b^3 \equiv 2 - 2b^3 \pmod 8$, ale $2 \nmid b$, więc $b^2 \equiv 1 \pmod 8$, skąd $b^3 \equiv b \pmod 8$. Ponadto $b \equiv 3 \pmod 4$, więc $b \equiv 3 \pmod 8$ lub $b \equiv 7 \pmod 8$, skąd $2b^3 \equiv 6 \pmod 8$. Wobec tego $x^2 + a^2 - 2b^3 \equiv 2 - 6 \equiv 4 \pmod 8$. Zatem $2v^3 \equiv 4 \pmod 8$, skąd $v^3 \equiv 2 \pmod 4$, co jest niemożliwe.

Wobec tego liczba x jest nieparzysta. Stąd liczba y też jest nieparzysta. Zatem $y^3 \equiv y \pmod 8$, ale $y^3 \equiv x^2+(2a)^2 \equiv 1+4 \equiv 5 \pmod 8$, więc $y \equiv 5 \pmod 8$, czyli $y \equiv 1 \pmod 4$. Dalej, $x^2+(2a)^2 = y^3+(2b)^3$, a zatem $x^2 + (2a)^2 = (y + 2b)(y^2 - 2by + 4b^2)$.

Ponadto, $y^2 - 2by + 4b^2 = (y - b)^2 + 3b^2 \geqslant 3$, gdyż $b \equiv 3 \pmod 4$ oraz $x^2 + (2a)^2 > 0$, bo $a \equiv \pm 1 \pmod 6$. Wobec tego $y + 2b > 0$, a ponieważ $y + 2b \equiv 1 + 2 \cdot 3 \equiv 3 \pmod 4$, więc $y + 2b > 1$. Jeśli każdy dzielnik pierwszy liczby $y + 2a$ przystaje do 1 modulo 4, to $y + 2b \equiv 1 \pmod 4$, co prowadzi do sprzeczności. Wobec tego liczba $y + 2b$ posiada dzielnik pierwszy postaci $4k + 3$. Gdyby wszystkie takie dzielniki pierwsze liczby $y + 2b$ miały parzysty wykładnik w rozwinięciu liczby $y + 2b$ na czynniki pierwsze, to $y + 2b \equiv 1 \pmod 4$, co też jest niemożliwe. Wobec tego istnieje dzielnik pierwszy $p \equiv 3 \pmod 4$ liczby $y + 2b$, który wchodzi w jej rozkład kanoniczny z nieparzystym wykładnikiem α. Zatem $p^\alpha \mid y + 2b$ i $p^{\alpha+1} \nmid y + 2b$ oraz p^α dzieli $x^2 + (2a)^2$. Ze stwierdzenia 2.15 uzyskujemy, że $p \mid 2a$, skąd $p \mid a$, ale $3 \nmid a$, więc $p \neq 3$. Ponadto, na mocy twierdzenia 14.18 liczba p wchodzi w rozkład kanoniczny liczby $x^2+(2a)^2$ z parzystym wykładnikiem, więc

$p^{\alpha+1} \mid y^3+(2b)^3$, czyli $p^{\alpha+1} \mid (y+2b)(y^2-2by+4b^2)$. Ponadto $p^{\alpha+1}$ nie dzieli $y+2b$, więc $p \mid y^2-2by+4b^2$. Zatem $y \equiv -2b \pmod{p}$ i stąd $0 \equiv$ $\equiv y^2-2by+4b^2 \equiv 12a^2 \pmod{p}$. Stąd $p \mid 12b^2$. Lecz jak pokazaliśmy, $p \neq 3$, więc $p \mid b$. Wobec tego liczby a i b posiadają wspólny dzielnik pierwszy $p \equiv 3 \pmod{4}$. Otrzymaliśmy zatem sprzeczność, która kończy dowód naszego twierdzenia. □

Ponieważ $12 = (2\cdot 1)^2-(2\cdot(-1))^3$, $-20 = (2\cdot 7)^2-(2\cdot 3)^3$ i $44 =$ $= (2\cdot 3)^2-(2\cdot(-1))^3$, więc z twierdzenia 18.9 uzyskujemy następujący

Wniosek 18.10. *Dla $k \in \{-20, 12, 44\}$ równanie $x^2+k=y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.*

Zadanie 18.11. Udowodnij, że nie istnieją liczby całkowite x i y takie, że $x^2+16=y^3$.

Zadanie 18.12. Udowodnij, że nie istnieją liczby całkowite x i y takie, że $x^2-6=y^3$.

Zadanie 18.13. Udowodnij, że istnieje nieskończenie wiele dodatnich liczb całkowitych k i istnieje nieskończenie wiele ujemnych liczb całkowitych k, dla których równanie Mordella $x^2+k=y^3$ nie posiada rozwiązania w liczbach całkowitych x i y.

18.2 Równania posiadające rozwiązanie

Przykład 18.14. Znajdziemy wszystkie rozwiązania w liczbach całkowitych x i y równania:

$$x^2+11=y^3. \tag{18.1}$$

Niech zatem liczby całkowite x i y spełniają równanie (18.1). Jeżeli $11 \mid x$, to $11 \mid y^3$, skąd $11 \mid y$ i w konsekwencji, $11^2 \mid y^3$, czyli 11^2 dzieli x^2+11, ale $11^2 \mid x^2$, więc $11^2 \mid 11$ i mamy sprzeczność. Wobec tego $11 \nmid x$. Jeżeli x jest nieparzyste, to y jest parzyste i $x^2 \equiv 1 \pmod{8}$, skąd $x^2+11 \equiv 12 \equiv 4 \pmod{8}$ oraz $y^3 \equiv 0 \pmod{8}$, więc mamy sprzeczność. Zatem x jest liczbą parzystą.

Z przykładu 13.26 wiemy, że pierścień $\mathbb{Z}[\omega_{-11}]$ z normą N daną wzorem $N(a+b\omega_{-11}) = (a+\frac{b}{2})^2 + \frac{11}{4}b^2$ dla $a, b \in \mathbb{Z}$ jest euklidesowy. Na mocy (18.1) uzyskujemy, że $(x+\sqrt{-11})\cdot(x-\sqrt{-11}) = y^3$ w pierścieniu $\mathbb{Z}[\omega_{-11}]$. Przypuśćmy, że elementy $x+\sqrt{-1}$ i $x-\sqrt{-11}$ nie są względnie pierwsze. Wtedy istnieje element pierwszy $\pi \in \mathbb{Z}[\omega_{-11}]$ będący ich wspólnym dzielnikiem. Wtedy π dzieli różnicę tych elementów, czyli $\pi \mid 2\sqrt{-11}$, skąd $\pi \mid 2$ lub $\pi \mid \sqrt{-11}$. Jeżeli $\pi \mid 2$, to $\pi \mid x$, bo liczba x jest parzysta. Ponadto $\pi \mid x+\sqrt{-11}$, więc $\pi \mid \sqrt{-11}$. Natomiast, jeśli $\pi \mid \sqrt{-11}$, to ponieważ $\pi \mid x+\sqrt{-11}$, więc $\pi \mid x$. Zatem w obu przypadkach $\pi \mid x$ i $\pi \mid \sqrt{-11}$, skąd $N(\pi) \mid N(x) = x^2$ i $N(\pi)$ dzieli $N(\sqrt{-11}) = 11$. Ponadto $N(\pi) > 1$, więc $N(\pi) = 11$ i $11 \mid x^2$, skąd $11 \mid x$, co prowadzi do sprzeczności. Wobec tego elementy $x+\sqrt{-11}$ i $x-\sqrt{-11}$ są względnie pierwsze. Ponieważ $(x+\sqrt{-11})\cdot$ $\cdot(x-\sqrt{-11}) = y^3$, więc na mocy twierdzenia 13.20, $x+\sqrt{-11} = u\alpha^3$ dla pewnego $\alpha \in \mathbb{Z}[\omega_{-11}]$ i dla pewnego elementu odwracalnego u. Ze wzoru (13.17), $u = 1$ lub $u = -1$, ale $-1 = (-1)^3$, więc $x+\sqrt{-11} = (a+b\omega_{-11})^3$ dla pewnych $a, b \in \mathbb{Z}$. Oznaczmy $\omega = \omega_{-11} = \frac{1+\sqrt{-11}}{2}$. Wtedy $\sqrt{-11} = 2\omega - 1$, skąd $-11 = 4\omega^2 - 4\omega + 1$, a zatem $\omega^2 = \omega - 3$ i $\omega^3 = -2\omega - 3$. Stąd $(x-1)+2\omega = (a+b\omega)^3 = a^3 + 3a^2b\omega + 3ab^2(\omega - +3) - b^3(2\omega+3)$, więc $x-1 = a^3 - 9ab^2 - 3b^3$ oraz $2 = 3a^2b + 3ab^2 - 2b^3$. Z drugiej równości wynika, że $b \mid 2$, a zatem $b = 1$ lub $b = 2$ lub $b = -1$ lub $b = -2$.

Jeśli $b = 1$, to $2 = 3a^2 + 3a - 2$, skąd $3 \mid 4$ i mamy sprzeczność. Zatem $b \neq 1$.

Jeśli $b = -1$, to $2 = -3a^2 + 3a + 2$, skąd $a = 0$ lub $a = 1$. Dla $a = 0$ uzyskujemy $x = 1 + 3 = 4$, więc $y^3 = 27$, skąd $y = 3$. Dla $a = 1$ uzyskujemy $x = 1 + 1 - 9 + 3 = -4$, więc $y^3 = 27$ i $y = 3$.

Jeśli $b = 2$, to $2 = 6a^2 + 12a - 16$, czyli $a^2 + 2a = 3$, skąd $a = 1$ lub $a = -3$. Dla $a = 1$ uzyskujemy $x = -58$, więc $y^3 = 3375$, skąd $y = 15$. Dla $a = -3$ uzyskujemy $x = 58$, więc $y^3 = 3375$, skąd $y = 15$.

Jeśli $b = -2$, to $2 = -6a^2 + 12a + 16$, skąd $3 \mid -14$ i mamy sprzeczność. Zatem $b \neq -2$.

Podsumowując, równanie (18.1) posiada dokładnie 4 rozwiązania w liczbach całkowitych: $x = \pm 4$ i $y = 3$ oraz $x = \pm 58$ i $y = 15$.

Następny przykład zawiera metodę rozwiązania inną niż ta, która

jest podana na stronie 319 w [2].

Przykład 18.15. Znajdziemy wszystkie $x \in \mathbb{Z}$ i $n \in \mathbb{N}$ spełniające równanie:

$$x^2 + 11 = 3^n. \tag{18.2}$$

Niech zatem $x \in \mathbb{Z}$ i $n \in \mathbb{N}$ spełniają to równanie. Ponieważ $x^2 + 11 \geqslant$ $\geqslant 11 > 3^2$, więc $n > 2$. Dalej, $3^3 \equiv 1 \pmod{13}$, więc dla $k \in \mathbb{N}$, $3^{3k} \equiv 1 \pmod{13}$ oraz $3^{3k+1} \equiv 3 \pmod{13}$ i $3^{3k+2} \equiv 9 \pmod{13}$. Ponadto $x \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6 \pmod{13}$, skąd $x^2 \equiv 0, 1, 3, 4, 9, 10, 12 \pmod{13}$ oraz $x^2 + 11 \equiv 11, 12, 1, 2, 7, 8, 10 \pmod{13}$. Wobec tego $n = 3k$ dla pewnego $k \in \mathbb{N}$ i $x^2 + 11 = (3^k)^3$. Zatem z przykładu 18.14, $3^k = 3$ lub $3^k = 15$, skąd $k = 1$ i $x^2 + 11 = 27$, więc $x = \pm 4$.

Podsumowując, równanie (18.2) posiada dokładnie dwa rozwiązania w liczbach $x \in \mathbb{Z}$ i $n \in \mathbb{N}$: $n = 3$ i $x = \pm 4$.

Przykład 18.16. Znajdziemy wszystkie rozwiązania w liczbach całkowitych x i y równania:

$$x^2 + 4 = y^3. \tag{18.3}$$

Rozważmy najpierw przypadek, gdy x jest nieparzyste. Wtedy w pierścieniu euklidesowym $\mathbb{Z}[i]$ nasze równanie przybiera postać:

$$(x + 2i)(x - 2i) = y^3.$$

Jeśli elementy $x + 2i$ i $x - 2i$ nie są względnie pierwsze, to istnieje element pierwszy $\pi \in \mathbb{Z}[i]$ będący ich wspólnym dzielnikiem. Stąd π dzieli $(x + 2i) - (x - 2i)$, czyli $\pi \mid 2^2 i$. Jak wiemy, $-i \in (\mathbb{Z}[i])^*$, więc $\pi \mid 2$, skąd $\pi \mid 2i$. Ponadto $\pi \mid x + 2i$, więc $\pi \mid x$. Lecz $x = 2k + 1$ dla pewnego $k \in \mathbb{Z}$ i $\pi \mid 2$, więc $\pi \mid 1$, co prowadzi do sprzeczności. Wobec tego elementy $x + 2i$ i $x - 2i$ są względnie pierwsze i na mocy twierdzenia 13.20, $x + 2i = \alpha^3$ dla pewnego $\alpha \in \mathbb{Z}[i]$, więc $x + 2i =$ $= (a+bi)^3$ dla pewnych $a, b \in \mathbb{Z}$. Dalej, $(a+bi)^3 = a^3+3a^2bi-3ab^2-b^3i$, więc $x = a^3 - 3ab^2$ oraz $2 = 3a^2b - b^3 = b(3a^2 - b^2)$. Zatem $b \mid 2$ i $b \in \mathbb{Z}$, więc $b \in \{1, -1, 2, -2\}$. Jeśli $b = 1$, to $3a^2 - 1 = 2$, skąd $a = \pm 1$ oraz $x = \pm 2$, więc mamy sprzeczność. Jeśli $b = -1$, to $3a^2 - 1 = -2$,

skąd $3 \mid 1$ i mamy sprzeczność. Jeśli $b = 2$, to $3a^2 - 4 = 1$, skąd $3 \mid 4$ i też mamy sprzeczność. Jeśli $b = -2$, to $3a^2 - 4 = -1$, więc $a = \pm 1$ i $x = \pm 11$ oraz $y^3 = 125$, skąd $y = 5$. Podsumowując, dla nieparzystego x wszystkimi rozwiązaniami równania (18.3) w liczbach całkowitych są pary (x, y): $(11, 5), (-11, 5)$.

Teraz rozważmy przypadek, gdy x jest parzyste. Wówczas y też jest parzyste i $x = 2X$ oraz $y = 2Y$ dla pewnych $X, Y \in \mathbb{Z}$. Ponadto po skróceniu przez 4 nasze równanie przybiera postać: $X^2 + 1 = 2Y^3$. Stąd X jest nieparzyste, czyli $X = 2U + 1$ dla pewnego $U \in \mathbb{Z}$. W pierścieniu $\mathbb{Z}[i]$ mamy $2 = (1+i)\cdot(1-i)$ oraz $(X+i)(X-i) = 2Y^3$, więc $\frac{X+i}{1+i} \cdot \overline{(\frac{X+i}{1+i})} = Y^3$. Ponadto $\frac{X+i}{1+i} = \frac{(X+i)(1-i)}{2} = \frac{X+1}{2} + \frac{1-X}{2}i = = (U+1) - Ui \in \mathbb{Z}[i]$, skąd $\overline{(\frac{X+i}{1+i})} = (U+1) + Ui$ oraz

$$((U+1) - Ui) \cdot ((U+1) + Ui) = Y^3.$$

Jeśli elementy $(U+1) - Ui$ i $(U+1) + Ui$ nie są względnie pierwsze, to istnieje element pierwszy $\pi \in \mathbb{Z}[i]$ będący ich wspólnym dzielnikiem. Stąd π dzieli sumę i różnicę tych elementów, więc $\pi \mid 2U + 2$ i $\pi \mid 2Ui$, skąd $\pi \mid 2U$ i wobec tego $\pi \mid (2U + 2) - 2U$, czyli $\pi \mid 2$, ale $2 \sim (1+i)^2$, więc $\pi \mid 1+i$. Zatem $\pi \mid U(1+i)$ oraz $\pi \mid (U+1)+Ui$. Wobec tego $\pi \mid 1$, co prowadzi do sprzeczności. Zatem elementy $(U+1)-Ui$ i $(U+1)+Ui$ są względnie pierwsze i na mocy twierdzenia 13.20, $(U+1)+Ui = v\beta^3$ dla pewnego $\beta \in \mathbb{Z}[i]$ i dla pewnego $v \in \{1, -1, i, -i\}$. Ponadto $-1 = = (-1)^3$, $i = (-i)^3$ oraz $-i = i^3$, więc $(U + 1) + Ui = (c + di)^3$ dla pewnych $c, d \in \mathbb{Z}$. Stąd $U + 1 = c^3 - 3cd^2$ oraz $U = 3c^2d - d^3$, skąd po odjęciu stronami, $1 = c^3 - 3cd^2 - 3c^2d + d^3$. Zatem $1 = (c+d)(c^2 - cd + +d^2) - 3cd(c + d) = (c + d)(c^2 - 4cd + d^2)$. Wobec tego $c + d = 1$ i $c^2 - 4cd + d^2 = 1$ albo $c + d = -1$ i $c^2 - 4cd + d^2 = -1$. W pierwszym przypadku, $c^2 + 2cd + d^2 = 1$, więc po odjęciu stronami, $6cd = 0$, czyli $c = 0$ i $d = 1$ lub $d = 0$ i $c = 1$, skąd $U = 0$ lub $U = -1$ oraz $X = 1$ lub $X = -1$, czyli $x = 2$ lub $x = -2$ i $y = 2$. Natomiast w drugim przypadku, $c^2 + 2cd + d^2 = 1$ i $c^2 - 4cd + d^2 = -1$, więc po dodaniu stronami, $0 = 2c^2 - 2cd + 2d^2 = (c - d)^2 + c^2 + d^2$, skąd $c = d = 0$, co przeczy temu, że $c + d = -1$. Wobec tego dla parzystego x wszystkimi rozwiązaniami równania (18.3) w liczbach całkowitych są pary (x, y): $(2, 2), (-2, 2)$.

Ostatecznie mamy zatem, że wszystkimi rozwiązaniami równania (18.3) w liczbach całkowitych są pary: $(11,5),(-11,5),(2,2),(-2,2)$.

Przykład 18.17. Pokażemy, że wszystkimi rozwiązaniami w liczbach całkowitych x i y równania Mordella:

$$x^2+432=y^3 \tag{18.4}$$

są: $x=\pm 36$ i $y=12$. Ponieważ $432=2^4\cdot 3^3$, więc $(\pm 36)^2+432=$ $=2^4\cdot 3^4+2^4\cdot 3^3=2^4\cdot 3^3\cdot(3+1)=2^6\cdot 3^3=(2^2\cdot 3)^3=12^3$, skąd wynika, że $x=\pm 36$ i $y=12$ są rozwiązaniami równania (18.4) w liczbach całkowitych. Przypuśćmy, że istnieją liczby całkowite x i y takie, że $x\neq\pm 36$ i $x^2+432=y^3$. Wtedy oczywiście $y\neq 12$ oraz istnieją $n\in\mathbb{N}$ oraz $k,m\in\mathbb{Z}$ takie, że $\frac{x}{36}=\frac{k}{n}\neq\pm 1$ i $\frac{y}{12}=\frac{m}{n}\neq 0$. Bez zmniejszania ogólności możemy zakładać, że liczby m,n,k są parzyste. Stąd liczby $u=\frac{n-k}{2}, v=\frac{n+k}{2}$ i $w=m$ są niezerowe i całkowite. Ponadto $u^3+v^3-w^3=\frac{n^3}{4}+\frac{3nk^2}{4}-m^3$, ale $k=\frac{nx}{36}$ i $m=\frac{ny}{12}$, więc $u^3+v^3-w^3=\frac{n^3}{4}+\frac{3n^3x^2}{4\cdot 36^2}-\frac{n^3y^3}{12^3}=\frac{n^3}{12^3}\cdot(3\cdot 12^3+x^2-y^3)=0$, bo $3\cdot 12^2+x^2-y^3=432+x^2-y^3$ i $x^2+432=y^3$. Wobec tego $u^3+v^3=w^3$, przy czym liczby całkowite u, v, i w są niezerowe. Przeczy to twierdzeniu 16.13. Wobec tego nasza teza została wykazana.

Przykład 18.18. Pokażemy, że wszystkimi rozwiązaniami w liczbach całkowitych x i y równania Mordella:

$$x^2-4=y^3 \tag{18.5}$$

są: $x=\pm 2$ i $y=0$. Rozpatrzmy najpierw przypadek, gdy liczba x jest nieparzysta. Wtedy liczby $x-2$ i $x+2$ są nieparzyste i $(x-2)(x+2)=y^3$ oraz $(x+2)-(x-2)=4$, więc liczby $x-2$ i $x+2$ są względnie pierwsze. Z twierdzenia 13.20 wynika zatem, że $x-2=a^3$ i $x+2=b^3$ dla pewnych $a,b\in\mathbb{Z}$. Ponieważ liczba x jest nieparzysta, więc stąd liczby a i b też są nieparzyste oraz $b^3-a^3=(x+2)-(x-2)=4$. Zatem $(b-a)(b^2+ab+a^2)=4$, ale $0\neq a^2+ab+b^2=(a+\frac{b}{2})^2+\frac{3}{4}b^2\geqslant 0$, więc a^2+ab+b^2 jest dodatnią liczbą nieparzystą dzielącą liczbę 4. Stąd $a^2+ab+b^2=1$ i $b-a=4$, ale $a^2+ab+b^2=(b-a)^2+3ab$,

więc $1 = 4^2 + 3ab$, skąd $ab = -5$, czyli $a(a+4) = -5$, a zatem $(a+2)^2 = -1$, co prowadzi do sprzeczności.

Wobec tego liczba x jest parzysta i w konsekwencji tego liczba y też jest parzysta. Zatem $x = 2X$ i $y = 2Y$ dla pewnych $X, Y \in \mathbb{Z}$ oraz $4X^2 - 4 = 8Y^3$, czyli $X^2 - 1 = 2Y^3$. Stąd wynika, że $X = 2u + 1$ dla pewnego $u \in \mathbb{Z}$ i $4u^2 + 4u = 2Y^3$, czyli $2u^2 + 2u = Y^3$. Zatem $Y = 2v$ dla pewnego $v \in \mathbb{Z}$. Stąd $2u^2 + 2u = 8v^3$, czyli $u^2 + u = 4v^3$, skąd $u(u+1) = 4v^3$, ale liczby u i $u+1$ są względnie pierwsze jako kolejne liczby całkowite i ich iloczyn jest podzielny przez 4, więc $u = 4c$ lub $u + 1 = 4c$ dla pewnego $c \in \mathbb{Z}$. W pierwszym przypadku $c(4c+1) = v^3$, więc na mocy twierdzenia 13.20, $c = k^3$ i $4c + 1 = l^3$ dla pewnych $k, l \in \mathbb{Z}$. Zatem $4k^3 + 1 = l^3$ i z wniosku 16.16 dostajemy, że $k = 0$ oraz $l = 1$. Zatem $c = 0$, skąd kolejno: $v = 0$, $Y = 0$, $y = 0$ i $x^2 = 4$, czyli $x = \pm 2$.

Natomiast w drugim przypadku $c(4c-1) = v^3$, więc na mocy twierdzenia 13.20, $c = n^3$ i $4c - 1 = m^3$ dla pewnych $m, n \in \mathbb{Z}$, czyli $4n^3 - 1 = m^3$. Zatem z wniosku 16.17 wynika, że $n = 0$ i $m = -1$. Stąd $c = 0$ i kolejno: $v = 0$, $Y = 0$, $y = 0$ i $x^2 = 4$, czyli $x = \pm 2$.

W ten sposób wykazaliśmy, że $x = \pm 2$ i $y = 0$. W szczególności równanie $x^2 - 4 = y^3$ nie posiada rozwiązania w liczbach naturalnych.

Przykład 18.19. Pokażemy, że wszystkimi rozwiązaniami w liczbach całkowitych równania Mordella:

$$x^2 - 16 = y^3 \tag{18.6}$$

są $x = \pm 4$ i $y = 0$. Jeżeli liczba x jest parzysta, to liczba y też jest parzysta, skąd $8 \mid x^2$, a zatem $x = 4X$ dla pewnego $X \in \mathbb{Z}$ oraz $y = 2Y$ dla pewnego $Y \in \mathbb{Z}$ oraz $16X^2 - 16 = 8Y^3$, skąd $2X^2 - 2 = Y^3$. Wobec tego liczba Y jest parzysta, czyli $Y = 2v$ dla pewnego $v \in \mathbb{Z}$ oraz $2X^2 - 2 = 8v^3$, czyli $X^2 - 1 = 4v^3$. Stąd $X = 2u + 1$ dla pewnego $u \in \mathbb{Z}$ i $4u^2 + 4u = 4v^3$, czyli $u(u+1) = v^3$, ale liczby u i $u+1$ są względnie pierwsze jako kolejne liczby całkowite, więc na mocy twierdzenia 13.20, $u = a^3$ i $u+1 = b^3$ dla pewnych $a, b \in \mathbb{Z}$. Stąd $b^3 - a^3 = 1$, czyli $(b-a)(b^2 + ba + a^2) = 1$. Ponadto $b^2 + ba + a^2 = (b + \frac{a}{2})^2 + \frac{3}{4}a^2 \geqslant 0$, więc $b - a = 1$ i $1 = b^2 + ba + a^2 = (b-a)^2 + 3ab$,

czyli $3ab = 0$. Stąd $a = 0$ lub $b = 0$, więc $v = 0$. Stąd $Y = 0$ i $y = 0$ oraz $x^2 = 16$, czyli $x = \pm 4$.

Pozostaje do rozpatrzenia przypadek, gdy $2 \nmid x$. Wtedy

$$(x-4)(x+4) = y^3$$

oraz liczby $x-4$ i $x+4$ są nieparzyste, a ich różnicą jest 4, a zatem te liczby są względnie pierwsze. Stąd na mocy twierdzenia 1.28, $x-4 = p^3$ i $x+4 = q^3$ dla pewnych $p, q \in \mathbb{Z}$. Zatem $q^3-p^3 = (x+4)-(x-4) = 8$, skąd $(q-p)(q^2+qp+p^2) = 8$, ale liczby p i q są nieparzyste, więc liczba $q^2+qp+p^2 = (q+\frac{p}{2})^2+\frac{3}{4}p^2 \geqslant 0$ jest nieparzystym dzielnikiem dodatnim liczby 8. Wobec tego $q^2+qp+p^2 = 1$ i w konsekwencji tego $q-p = 8$. Stąd $q \equiv p \pmod 8$, czyli $q^2+qp+p^2 \equiv 3p^2 \equiv 3 \pmod 8$, bo $2 \nmid p$. Zatem $1 \equiv 3 \pmod 8$, co prowadzi do sprzeczności.

Podsumowując, wszystkimi rozwiązaniami równania $x^2 - 16 = y^3$ w liczbach całkowitych x i y są: $x = \pm 4$ i $y = 0$. W szczególności równanie to nie posiada rozwiązania w liczbach naturalnych.

Zadanie 18.20. Wyznacz wszystkie liczby całkowite x i y takie, że $x^2 + 8 = y^3$.

Zadanie 18.21. Udowodnij, że istnieje nieskończenie wiele zarówno dodatnich jak też ujemnych liczb całkowitych k, dla których równanie Mordella $x^2 + k = y^3$ posiada rozwiązanie w liczbach naturalnych.

Część VI

Dodatek algebraiczny

Rozdział 19

Ciała abstrakcyjne

19.1 Działanie w zbiorze

Z dowolnych przedmiotów a i b (niekoniecznie różnych) można utworzyć **parę uporządkowaną** (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 $b = d$, tzn. 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 19.1. 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 19.2. 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 19.3. *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 19.3 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 19.4. *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 19.3, $a^n \circ a^m = a^{n+m}$.

(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 19.3, $(a^n)^m = a^{nm}$. □

Wniosek 19.5. *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 19.4, $b^{m+1} = b^m \circ b$, 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 19.3 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 19.6. *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 $n \in \mathbb{N}$. $\square$

19.2 Określenie ciała

Definicja 19.7. 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 działamiami 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 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 $\mathbb{Q}$.

Innym przykładem ciała jest **ciało liczb rzeczywistych** (ze zwykłym dodawaniem i mnożeniem liczb). Oznaczamy je przez $\mathbb{R}$.

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 19.8. Niech $(K, +, \cdot, 0, 1)$ będzie dowolnym ciałem. Wówczas na mocy **A2** i twierdzeń 19.3 i 19.6, 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 19.3 i 19.6, 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 19.9. *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 19.10. 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 19.9 (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:

$$-(-a) = a. \tag{19.1}$$

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

Własność 19.11. *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 19.9 (a), $a \cdot 0 = 0$.

(ii). Jeśli $-a = 0$, to $-(-a) = -0 = 0$, więc na mocy (19.1), $a = 0$. 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 19.10, $(-1) \cdot a = -a$.

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 19.12. 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 19.9 (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 19.11, skąd $0 = 1$ wbrew własności 19.11. 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:

$$(a^{-1})^{-1} = a. \tag{19.2}$$

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 $a, b \in K$:

$$a - b \stackrel{def}{=} a + (-b). \tag{19.3}$$

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

$$a + b = a - (-b). \tag{19.4}$$

Rzeczywiście, $a - (-b) = a + [-(-b)] = a + b$ na mocy (19.3) i (19.1).

Stwierdzenie 19.13. *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 19.9 (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 19.9 (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 (19.4): $a + b = a - (-b)$, 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 19.13 nazywamy **podciałem ciała** $(L, +, \cdot, 0, 1)$.

19.3 Własności działań w ciele

Własność 19.14. *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 19.11 (*iii*) i z uwagi 19.8 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 (19.1).

(*ii*). Ponieważ na mocy wzoru (19.3) 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 19.9 (a), $u=v$. Wobec tego $a-b$ jest jedynym rozwiązaniem równania $b+x=a$ w ciele K.

(*iii*). Z (19.3), **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:

$$a : b = \frac{a}{b} = a\cdot b^{-1}, \quad b\neq 0. \tag{19.5}$$

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

$$\frac{a}{a} = 1 \text{ dla każdego } a\neq 0. \tag{19.6}$$

Własność 19.15. *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 (19.5) 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 19.9 (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 19.16. *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 19.11, $a \cdot b = 0 \cdot b$, skąd $a = 0$ na mocy własności 19.9 (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 19.8 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 19.12 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 19.17. *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 19.12, $\frac{1}{b} \neq 0$, a ponieważ $a \neq 0$, więc z własności 19.16, $a \cdot \frac{1}{b} \neq 0$, 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 19.12, $\frac{b}{a}$ jest elementem odwrotnym do $\frac{a}{b}$, czyli $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Dalej, z własności 19.16, $a \cdot b \neq 0$ i na mocy uwagi 19.8, $(a \cdot b) \cdot \frac{1}{a} \cdot \frac{1}{b} = [a \cdot \frac{1}{a}] \cdot [b \cdot \frac{1}{b}] = 1 \cdot 1 = 1$, więc na mocy uwagi 19.12, $\frac{1}{a} \cdot \frac{1}{b}$ jest elementem odwrotnym do elementu $a \cdot b$, czyli $\frac{1}{a \cdot b} = \frac{1}{a} \cdot \frac{1}{b}$. □

Własność 19.18. *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 (19.5) 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 19.19. *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 19.15, $a = b \cdot \frac{c}{d}$. Stąd i z uwagi 19.8, $a \cdot d = b \cdot (\frac{c}{d} \cdot d) = b \cdot c$, na mocy własności 19.15.

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 19.15 i z **A6**, $\frac{c}{d} = \frac{a}{b}$. □

Własność 19.20. *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 19.16 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 19.19, $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$. □

Własność 19.21. *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 (19.5) 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 19.14, $\frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}$. □

Własność 19.22. *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 (19.5) 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 19.17, więc ze wzoru (19.5), $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.

Z własności 19.20 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 19.21, $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ i $\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d}$. □

Własność 19.23. *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 (19.5) i z własności 19.17, $a : \frac{b}{c} = a \cdot (\frac{b}{c})^{-1} = a \cdot \frac{c}{b}$. □

Własność 19.24. *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 19.8, $(a_1 + \ldots + a_n) + [(-a_1) + \ldots + (-a_n)] = [a_1 + (-a_1)] + \ldots + [a_n + (-a_n)] = 0 + \ldots + 0 = 0$, więc na mocy uwagi 19.10, $(-a_1) + (-a_2) + \ldots + (-a_n)$ jest elementem przeciwnym do $a_1 + \ldots + a_n$, skąd mamy tezę. □

Własność 19.25. *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 19.26. *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 (19.5) i z własności 19.25 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 19.27. *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 19.25 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 19.25 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 19.4 i 19.5 mamy od razu następującą:

Własność 19.28. *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 19.29. *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 19.25, $(a - b) \cdot (a + b) = (a - b) \cdot a + (a - b) \cdot b$. Z własności 19.14 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 19.27 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 19.30. *Dla dowolnych elementów a i b ciała K i dla każdego naturalnego $n \geqslant 2$ zachodzi wzór:*

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}). \tag{19.7}$$

Dowód. Z własności 19.14 (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 19.25 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 19.24 i uwagi 19.8 mamy tezę. □

Własność 19.31. *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 19.25 mamy, że $(-a)^n = [(-a)^2]^k$. Ale na mocy własności 19.14 (i), $(-a)^2 = (-a) \cdot (-a) = a \cdot a = a^2$, więc znowu z własności 19.25, $(-a)^n = (a^2)^k = a^{2k} = a^n$. 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 19.14 (i), $(-a)^n = = -(a^{2k} \cdot a) = -a^{2k+1} = -a^n$. □

Podstawiając we wzorze (19.7): $n = 2m + 1$ dla $m \in \mathbb{N}$ oraz $(-b)$ w miejsce b i wykorzystując własność 19.31, uzyskujemy wzór:

$$a^{2m+1} + b^{2m+1} = (a+b)(a^{2m} - a^{2m-1}b + \ldots + a^2b^{2m-2} - ab^{2m-1} + b^{2m}). \tag{19.8}$$

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

$$k \cdot a \stackrel{def}{=} \begin{cases} \underbrace{a + a + \ldots + a}_{k} & , \text{ gdy } k > 0 \\ 0 & , \text{ gdy } k = 0 \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{|k|} & , \text{ gdy } k < 0 \end{cases} . \tag{19.9}$$

Pokażemy, że wówczas zachodzi następujące

Stwierdzenie 19.32. *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 19.5 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 19.5. 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 19.4, $n \cdot (m \cdot a) = (nm) \cdot a$ 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 19.11 (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 19.28 można teraz uogólnić

w postaci następującego stwierdzenia, którego dowód pominiemy ze względu na jego podobieństwo do dowodu stwierdzenia 19.32.

Stwierdzenie 19.33. *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 19.29 (*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 19.34. *Dla każdego $n \in \mathbb{N}$ i dla dowolnego $j = 0, 1, \ldots, n-1$ zachodzi wzór:*

$$\binom{n}{j+1} + \binom{n}{j} = \binom{n+1}{j+1}. \tag{19.10}$$

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

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}, \tag{19.11}$$

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

Własność 19.35. (Wzór dwumianowy Newtona). *Dla dowolnych elementów a i b ciała K i dla dowolnego $n \in \mathbb{N}$ zachodzi wzór:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{19.12}$$

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 (19.12) 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 (19.10): $\binom{n}{j+1} + \binom{n}{j} = \binom{n+1}{j+1}$ 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 (19.12) jest wówczas prawdziwy także dla liczby $n+1$.

Wobec tego na mocy zasady indukcji wzór (19.12) jest prawdziwy dla dowolnego $n \in \mathbb{N}$. □

Rozdział 20

Ciało liczb zespolonych

20.1 Konstrukcja ciała liczb zespolonych

W zbiorze $\mathbb{R} \times \mathbb{R}$ wprowadzamy działania $+$ i $\cdot$ przy pomocy wzorów:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \tag{20.1}$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + a_2 \cdot b_1), \tag{20.2}$$

dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{R}$.

Twierdzenie 20.1. *Zbiór $\mathbb{R} \times \mathbb{R}$ z działaniami danymi wzorami (20.1) i (20.2) 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 (20.1) 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 (20.1) 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 (20.1) i tego, że 0 jest elementem neutralnym dodawania liczb rzeczywistych $(a,b)+(0,0)=(a+0,b+0)=(a,b)$.

A4. Na mocy wzoru (20.1) mamy, że $(a,b)+(-a,-b)=$ $=(a+(-a),b+(-b))=(0,0)$.

A5. Na mocy wzoru (20.2) 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 (20.2), 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 (20.2) 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 (20.1) i (20.2) 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 (20.2) $(a,b)\cdot(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2})=(a\cdot\frac{a}{a^2+b^2}-b\cdot\frac{(-b)}{a^2+b^2},a\frac{(-b)}{a^2+b^2}+\frac{a}{a^2+b^2}\cdot b)=(\frac{a^2+b^2}{a^2+b^2},0)=$ $=(1,0)$. □

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 (20.1) 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 (20.1) i (20.2) i z dowodu twierdzenia 20.1 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:

$$(a,0)\equiv a. \tag{20.3}$$

Przy takim utożsamieniu $\mathbb{R}\subseteq\mathbb{C}$.

Liczbę zespoloną

$$i=(0,1) \tag{20.4}$$

nazywamy **jednostką urojoną**. Zachodzi dla niej bardzo ważny wzór:

$$i^2=-1. \tag{20.5}$$

Rzeczywiście, na mocy wzoru (20.2):
$i^2=(0,1)\cdot(0,1)=(0\cdot 0-1\cdot 1,0\cdot 1+0\cdot 1)=(-1,0)\equiv -1$.

Z dowodu twierdzenia 20.1 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:

$$(a,b)\equiv a+bi. \tag{20.6}$$

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, 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 zepolonych 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**:

$$z = w \iff [re(z) = re(w) \text{ oraz } im(z) = im(w)]. \tag{20.7}$$

Modułem liczby zespolonej $z = a+bi$, gdzie $a,b \in \mathbb{R}$ nazywamy liczbę rzeczywistą nieujemną

$$|z| = \sqrt{a^2+b^2}. \tag{20.8}$$

Z tych określeń mamy od razu, że

$$re(z) \leqslant |z| \text{ oraz } im(z) \leqslant |z|, \tag{20.9}$$

$$z \cdot \overline{z} = |z|^2. \tag{20.10}$$

20.2 Własności sprzęgania

Własność 20.2. *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 20.3. *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 20.4. *Dla dowolnego $n \in \mathbb{N}$ i dla dowolnego $z \in \mathbb{C}$:*

$$\overline{z^n} = (\overline{z})^n.$$

Dowód. Wystarczy we własności 20.3 podstawić $z = z_1 = \ldots = z_n$. □

Własność 20.5. *Dla dowolnych $z, w \in \mathbb{C}$ takich, że $w \neq 0$ mamy, że $\overline{w} \neq 0$ oraz zachodzi wzór:*

$$\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}.$$

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 20.3, $\overline{z} = \overline{w} \cdot \overline{\left(\frac{z}{w}\right)}$, skąd po podzieleniu obu stron przez $\overline{w} \neq 0$ uzyskamy tezę. □

20.3 Własności modułu

Własność 20.6. *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 (20.10) i własności 20.3 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 20.7. *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 20.6 otrzymujemy, że $|z| = |w| \cdot \left|\frac{z}{w}\right|$ i po podzieleniu obu stron przez $|w|$ uzyskamy tezę. □

Własność 20.8. *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 20.6. □

Własność 20.9. (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. □

Czytelnika pragnącego pogłębić swoją wiedzę na temat liczb zespolonych odsyłamy do monografii [8].

Bibliografia

[1] Aczel A. D., *Wielkie twierdzenie Fermata. Rozwiązanie zagadki starego matematycznego problemu*, Wydawnictwo Prószyński i S-ka, Warszawa 1998.

[2] Andreescu T., Andrica D., Cucurezeanu I., *An Introduction to Diophantine Equantions*, Springer-Birkhauser, New York 2010.

[3] Andruszkiewicz R. R., Andruszkiewicz N., *Elementary proof of Nagell's theorem*, Azerb. J. Math. 20(2), 2020, s. 62-70.

[4] Andruszkiewicz R. R., *Wykłady z algebry ogólnej I*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2005.

[5] Andruszkiewicz R. R., *Wykłady z algebry ogólnej II*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2016.

[6] Baker A., *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge 1990.

[7] Brezinski C., *History of continued fractions and Pade approximants*, Springer-Verlag, New York 1991.

[8] Białynicki-Birula A., *Algebra*, Wydawnictwo Naukowe PWN, Warszawa 2016.

[9] Buchsztab A. A., *Teoria liczb*, Proswieszczenije, Moskwa 1960.

[10] Cel J., *O rozkładzie sześcianu na różnicę bikwadratów*, Matematyka 5, 1983, s. 308-310.

[11] Chao Ko, *On the Diophantine equation* $x^2 = y^n + 1, xy \neq 0$, Sci. Sinica 14, 1965, s. 457-460.

[12] Chein E. Z., *A note on the equation* $x^2 = y^q + 1$, Proc. of American Math. Soc. 56, 1976, s. 83-84.

[13] Cohn J. H. E., *The diophantine equation* $x^2 + 3 = y^n$, Glasgow Math. J. 35, 1993, s. 203-206.

[14] Corless R. M., *Continued Fractions and Chaos*, Amer. Math. Monthly 99(3), 1992, s. 203-215.

[15] Euler L., *Commentationes Arithmeticae I. In Opera Omnia*, Series I, t. II, 1915, s. 56-58.

[16] Lemmermeyer F., *Reciprocity laws: from Euler to Eisenstein*, Springer Science & Business Media, Berlin 2013.

[17] Goldfeld D., *Gauss' class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. 13(1), 1985, s. 23-37.

[18] Khinchin, A. I., *Continued fractions*, University of Chicago Press, Chicago 1964.

[19] Lebesgue V. A., *Sur l'impossibilié, en nombers entiers, de l'équation* $x^m = y^2 + 1$, Nouvelles annales de mathématiques 9, 1850, s. 178-181.

[20] Ljunggren W., *Ber einige Arcustangensgleichungen die auf interessante unbestimmte. Gleichungen fuhrer*, Ark. Mat. Astr. Fys. 29A(13), 1943, s. 1-11.

[21] Marzantowicz W., Zarzycki P., *Elementarna teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2015.

[22] Metsänkylä T., *Catalan's conjecture: another old Diophantine problem solved*, Bull. Amer. Math. Soc 41(1), 2004, s. 43–57.

[23] Maor E., *The Pythagorean Theorem: A 4,000-Year History*, Princeton University Press, New Jersey 2007.

[24] Mihăilescu P., *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Amgew. Math. 572, 2004, s. 167-195.

[25] Mordell L. J., *Diophantine Equations*, Academic Press, London 1969.

[26] Narkiewicz W., *Classical problems in number theory*, Wydawnictwo Naukowe PWN, Warszawa 1986.

[27] Narkiewicz W., *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag Berlin, Heidelberg 2004.

[28] Nagell T., *Sur l'impossibilite de l'equation indeterminee* $y^2 = z^p + 1$, Norsk. Mat. Forenings Skrifter I 4, 1921, s. 1-63.

[29] Nagell T., *The diophantine equation* $x^2 + 7 = 2^n$, Norsk. Mat. Tidsskr. 30, 1948, s. 62-64.

[30] Nagell T., *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. Basel 5, 1954, s. 153-159.

[31] Nowicki A., *Równanie Pella, Podróże po Imperium Liczb 14*, Olsztyńska Wyższa Szkoła Informatyki i Zarządzania, Toruń, 2014.

[32] Ramirez Alfonsin J. L., *The Diophantine Frobenius Problem*, Oxford University Press, USA 2006.

[33] Ribenboim P., *Catalan's Conjecture*, Academic Press, Boston 1994.

[34] Ribenboim P., *Wielkie twierdzenie Fermata dla laików*, WNT Wydawnictwa Naukowo-Techniczne, Warszawa 2001.

[35] Sierpiński W., *Elementary theory of numbers*, Wydawnictwo Naukowe PWN, Warszawa 1954.

[36] Sierpiński W., *Arytmetyka Teoretyczna*, Wydawnictwo Naukowe PWN, Warszawa 1959.

[37] Sierpiński W., *250 zadań z elementarnej teorii liczb*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1987.

[38] Sierpiński W., *Pythagorean Triangles*, Dover Publications Inc., New York 2003.

[39] Sury B., *On the Diophantine equation* $x^2 + 2 = y^n$, Arch. Math. Basel 74, 2000, s. 350-355.

[40] Weil A., *Number Theory: An Approach through History from Hammurapi to Legendre*, Birkhäuser, Boston 1984.

[41] Wiles A., *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. 142, 1995, s. 443-551.