FORMALIZED MATHEMATICS
Vol. 32, No. 1, pp. 47–63, 2024
DOI: 10.2478/forma-2024-0004
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

# Elementary Number Theory Problems. Part XIV – Diophantine Equations

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

**Summary.** This paper continues the formalization of chosen problems defined in the book "250 Problems in Elementary Number Theory" by Wacław Sierpiński.

MSC: 11A41 11D72 68V20

Keywords: number theory; prime number; Diophantine equation

MML identifier: `NUMBER14`, version: `8.1.14 5.81.1467`

## Introduction

In this paper, Problems 45 and 49 from section *"Relatively prime numbers"*, 120 and 131 from section *"Prime and composite numbers"*, 144, and 148–152 from section *"Diophantine equations"* of *"250 Problems in Elementary Number Theory"* by Wacław Sierpiński [16] are formalized, using the Mizar system [6], [11].

In the preliminary section, we proved several properties about divisibility and coprimeness of integers and absolute values of integers – in the process of revision [5] they can be moved to earlier Mizar articles stored in the Mizar Mathematical Library [1] and potentially used for possible generalizations of theorems from naturals to integers.

In section *"Chinese remainder theorem"*, we defined functors representing solutions of families of congruences satisfying conditions of the theorem – to prove the correctness conditions of the functors, we utilized adequate theorems from *"Modular Integer Arithmetic"* (INT_6) by Christoph Schwarzweller [14].

Problem 49 concerns a proof (the idea was given originally by A. Schinzel [12]) that for every positive integer $m$ every even number $2k$ can be represented as a difference of two positive integers relatively prime to $m$.

To construct such two positive integers, we defined a finite sequence Sierp49FS of m,k (LaTeXed as Sierpiński49 finite sequence) for every positive natural m and every natural k, and stated the required property in the following two forms (we consider the finite sequence of naturally ordered prime divisors [4]):

```
theorem :: NUMBER14:54
  for m being positive Nat, k being Nat
  for S being Sierp49FS of m,k
  for q being CR_Sequence st q = PrimeDivisorsFS(m)
  ex a,b being positive Nat st 2*k = a-b &
     a,m are_coprime & b,m are_coprime &
     a = CRT(S,q) + Product(q) + 2*k & b = CRT(S,q) + Product(q);
```

and

```
theorem :: NUMBER14:55
  for m being positive Nat, k being Nat
  ex a,b being positive Nat st 2*k = a-b &
     a,m are_coprime & b,m are_coprime;
```

Problem 131 searches all integers $k \geqslant 0$ for which the sequence of consecutive numbers $k+1, k+2, \ldots, k+10$ contains a maximal number of primes. It is proven that for $k = 1$, the segment contains five primes (2, 3, 5, 7, and 11), while for other values of $k$, the number of primes in the sequences is less or equal to four. Sierpiński leaves the question about the infinitude of the number of such $k$'s open, but based on his own hypothesis given by A. Schinzel [13] gives rather the affirmative answer to this question. In its most general form, Schinzel's hypothesis H is still an open problem.

Problem 144 is devoted to the infiniteness of the set of all solutions of the equation $x^2 - Dy^2 = z^2$ in positive integers $x$, $y$, $z$ such that $(x, y) = 1$ for arbitrary non-zero integers $D$. The problem is well recognized in the literature – see e.g. §8 in Carmichael's classical handbook [3], including Pell's equation theory [2].

The proof given in the book is split into 2 cases that consider odd and even numbers $D$ separately using facts proven in [8]. Unfortunately, the proof of the even case is based on an invalid equation and proposes incorrect solutions. The correct equation which leads to the proper solutions $x = |\frac{1}{2}dy^2+1|$, $z = |\frac{1}{2}dy^2-1|$ for $y$ being positive even integers and $D = 2 \cdot d$ is

$$\left(\frac{1}{4}Dy^2 + 1\right)^2 - Dy^2 = \left(\frac{1}{4}Dy^2 - 1\right)^2$$

Problem 149 stated in the book as: “Prove the theorem of Euler that the equation $4xy - x - y = z^2$ has no solutions in positive integers $x, y, z$, and prove that this equation has infinitely many solutions in negative integers $x, y, z$.” is formalized in the article in two separate theorems. To prove the second part of the problem, we defined the injective function `exampleSierpinski149`, which assigns triplets $[-1, -5n^2 - 2n, -5n - 1]$ to every positive natural number and showed that the range of the function is contained in the set of all possible negative solutions of the equation $4xy - x - y = z^2$, which allows the conclusion that the equation has infinitely many solutions in negative integers.

Problem 150 asks for an elementary proof (without using the theory of Pell’s equation) of the infiniteness of the set of all solutions of the equation $x^2 + Dy^2 = 1$ in positive integers $x$ and $y$ for positive $D = m^2 + 1$, while the proof presented in the book solves the problem for the equation $x^2 - Dy^2 = 1$. We formalized the later case.

The proof of Problem 151 given in Sierpiński’s book, was based again on the original idea of A. Schinzel as shown in [17].

Problem 152 concerns finding all solutions of the equation

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m$$

in relatively prime positive integers $x$, $y$, $z$ for every natural number $m$.

Even though the statement of the problem considers only positive integers $x$, $y$, $z$, the proof given in the book solved the problem for all non-zero integers $x$, $y$, and $z$. Then, we formulated the problem in three variants: we showed that $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$ if and only if $x = y = z = 1$ for positive $x$, $y$, $z$; $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$ if and only if $x = y = z = 1$ or $x = y = z = -1$ if non-zero integers $x$, $y$, $z$ are allowed; and the equation has no solutions for $m \neq 3$.

To prove Problem 148, facts from [9] were heavily used. Proofs of other problems are direct formalizations of solutions given in the book, following also [15] in some places.

## 1. Preliminaries

From now on $a$, $b$, $c$, $h$ denote integers, $k$, $m$, $n$ denote natural numbers, $i$, $j$, $z$ denote integers, and $p$ denotes a prime number.

Let $a$, $b$, $c$ be integers. One can verify that $\langle a, b, c\rangle (\in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})$ reduces to $\langle a, b, c\rangle$.

Let us consider real numbers $a$, $b$. Now we state the propositions:

(1) If $0 \leqslant a < b$, then $|a| < |b|$.

(2) If $b < a \leqslant 0$, then $|a| < |b|$.

(3) If $j \neq 0$ and $z = \frac{i}{j}$, then $z \mid i$.

(4) $i \mid j$ if and only if $i \mid |j|$.

(5) $i \mid j$ if and only if $|i| \mid j$.

(6) If $p \mid i^n$, then $p \mid i$. The theorem is a consequence of (4).

(7) Let us consider natural numbers $m$, $n$. Suppose $m \mid n \cdot p$. Then

   (i) $m \mid n$, or

   (ii) there exists a natural number $z$ such that $m = z \cdot p$ and $z \mid n$.

(8) Let us consider integers $m$, $n$. Suppose $m \mid n \cdot p$. Then

   (i) $m \mid n$, or

   (ii) there exists an integer $z$ such that $m = z \cdot p$ and $z \mid n$.

   The theorem is a consequence of (7) and (4).

(9) $i$ and $j$ are relatively prime if and only if $|i|$ and $|j|$ are relatively prime.

(10) $i$ and $j$ are relatively prime if and only if $|i|$ and $j$ are relatively prime.

(11) $i$ and $j$ are relatively prime if and only if $-i$ and $-j$ are relatively prime.

(12) $i$ and $j$ are relatively prime if and only if $-i$ and $j$ are relatively prime.

Let us consider integers $i$, $j$, $k$. Now we state the propositions:

(13) If $i \neq 0$, then if $i \mid k$ and $i \cdot j$ and $k$ are relatively prime, then $i = 1$ or $i = -1$.

(14) If $i \mid j$ and $i$ and $j$ are relatively prime, then $i = 1$ or $i = -1$.

(15) If $i \mid j$, then $j \equiv 0 \pmod{i}$.

(16) Let us consider integers $a$, $b$, $c$. Suppose $a \neq 0$ and $c \neq 0$ and $a$ and $c$ are relatively prime and $b$ and $c$ are relatively prime. Then $a \cdot b$ and $c$ are relatively prime.

(17) If $i \equiv j \pmod{2}$, then $i$ is odd iff $j$ is odd.

(18) If $i \equiv j \pmod{2}$, then $i$ is even iff $j$ is even.

(19) Let us consider integers $i$, $j$, $k$. If $i > 0$ and $j \equiv k \pmod{i}$, then $i \mid j$ iff $i \mid k$.

Proof: If $i \mid j$, then $i \mid k$. □

Let us consider objects $a$, $b$ and a finite sequence $f$. Now we state the propositions:

(20) $1, 2 \in \operatorname{dom}(\langle a, b \rangle \frown f)$.

(21) (i) $(\langle a, b \rangle \frown f)(1) = a$, and

(ii) $(\langle a, b \rangle \frown f)(2) = b$.

(22) If $n \in \operatorname{dom} f$, then $n + 2 \in \operatorname{dom}(\langle a, b \rangle \frown f)$.

(23) If $n \in \operatorname{dom} f$, then $(\langle a, b \rangle \frown f)(n + 2) = f(n)$.

(24) Let us consider a decreasing, real-valued finite sequence $f$. Then $\min_{\mathrm{p}} f = \operatorname{len} f$.

(25) Let us consider an increasing, real-valued finite sequence $f$. Then $\max_{\mathrm{p}} f = \operatorname{len} f$.

Let $X$ be an included in a segment, real-membered set. Note that $\operatorname{Sgm} X$ is increasing.

## 2. Chinese Remainder Theorem

Let $f$ be a Chinese remainder, integer-valued finite sequence. Let us observe that $-f$ is Chinese remainder.

Let $f$ be a Chinese remainder, integer-valued, non-empty finite sequence. Observe that $f \cdot f$ is Chinese remainder.

Let $a_1$, $n_1$, $a_2$, $n_2$ be integers and $x$ be an integer. We say that $a_1 \equiv_{n_1} x \equiv_{n_2} a_2$ if and only if

(Def. 1) $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$.

Now we state the propositions:

(26) Let us consider integers $a_1$, $n_1$, $a_2$, $n_2$, and an integer $x$. Suppose $a_1 \equiv_{n_1} x \equiv_{n_2} a_2$. Let us consider an integer $k$. Then $a_1 \equiv_{n_1} x + k \cdot n_1 \cdot n_2 \equiv_{n_2} a_2$.

(27) Let us consider integers $a_1$, $a_2$, and natural numbers $n_1$, $n_2$. Suppose $n_1 > 0$ and $n_2 > 0$. Let us consider an integer $x$. Suppose $a_1 \equiv_{n_1} x \equiv_{n_2} a_2$. Then $a_1 \equiv_{n_1} x \bmod n_1 \cdot n_2 \equiv_{n_2} a_2$.

Let $a_1$, $a_2$ be integers and $n_1$, $n_2$ be natural numbers. Assume $n_1$ and $n_2$ are relatively prime and $n_1 > 0$ and $n_2 > 0$. The functor $\mathrm{CRT}(a_1, n_1, a_2, n_2)$ yielding an element of $\mathbb{N}$ is defined by

(Def. 2) $a_1 \equiv_{n_1} \mathit{it} \equiv_{n_2} a_2$ and $\mathit{it} < n_1 \cdot n_2$.

Let us consider integers $a_1$, $a_2$ and natural numbers $n_1$, $n_2$. Now we state the propositions:

(28) If $n_1$ and $n_2$ are relatively prime and $n_1 > 0$ and $n_2 > 0$, then $\{x$, where $x$ is a positive natural number : $a_1 \equiv_{n_1} x \equiv_{n_2} a_2\}$ is infinite. The theorem is a consequence of (26).

(29) If $n_1$ and $n_2$ are relatively prime and $n_1 > 0$ and $n_2 > 0$, then $\{x$, where $x$ is a natural number : $a_1 \equiv_{n_1} x \equiv_{n_2} a_2\}$ is infinite. The theorem is a consequence of (28).

Let $u$, $m$ be integer-valued finite sequences and $z$ be an integer. We say that $z \equiv_{u(\cdot)} m(\cdot)$ if and only if

(Def. 3) for every natural number $i$ such that $i \in \operatorname{dom} u$ holds $z \equiv u(i) \pmod{m(i)}$.

Let $u$ be an integer-valued finite sequence and $m$ be a CR-sequence. Assume $\operatorname{dom} u = \operatorname{dom} m$. The functor $\mathrm{CRT}(u, m)$ yielding an element of $\mathbb{N}$ is defined by

(Def. 4) $\mathit{it} \equiv_{u(\cdot)} m(\cdot)$ and $\mathit{it} < \prod m$.

Now we state the proposition:

(30) Let us consider an integer-valued finite sequence $u$, and a CR-sequence $m$. Suppose $\operatorname{dom} u = \operatorname{dom} m$. Let us consider an integer $z$. Suppose $z \equiv_{u(\cdot)} m(\cdot)$. Let us consider an integer $k$. Then $z + k \cdot (\prod m) \equiv_{u(\cdot)} m(\cdot)$.

Let us consider an integer-valued finite sequence $u$ and a CR-sequence $m$. Now we state the propositions:

(31) If $\operatorname{dom} u = \operatorname{dom} m$, then $\{z$, where $z$ is a positive natural number : $z \equiv_{u(\cdot)} m(\cdot)\}$ is infinite. The theorem is a consequence of (30).

(32) If $\operatorname{dom} u = \operatorname{dom} m$, then $\{z$, where $z$ is a natural number : $z \equiv_{u(\cdot)} m(\cdot)\}$ is infinite. The theorem is a consequence of (31).

## 3. Problem 45

Let $a$, $b$, $c$ be integers. We say that two or more among numbers $a$, $b$, $c$ are even if and only if

(Def. 5) $a$ is even and $b$ is even and $c$ is odd or $a$ is even and $b$ is odd and $c$ is even or $a$ is odd and $b$ is even and $c$ is even or $a$ is even and $b$ is even and $c$ is even.

We say that two or more among numbers $a$, $b$, $c$ are odd if and only if

(Def. 6) $a$ is odd and $b$ is odd and $c$ is even or $a$ is odd and $b$ is even and $c$ is odd or $a$ is even and $b$ is odd and $c$ is odd or $a$ is odd and $b$ is odd and $c$ is odd.

Let $a$, $b$, $c$, $n$ be integers. We say that $a$, $b$, $c$ give three different remainders upon dividing by $n$ if and only if

(Def. 7) $a \bmod n$, $b \bmod n$, $c \bmod n$ are mutually different.

We say that at least two of the numbers $a$, $b$, $c$ are not divisible by $n$ if and only if

(Def. 8) $n \nmid a$ and $n \nmid b$ and $n \mid c$ or $n \nmid a$ and $n \mid b$ and $n \nmid c$ or $n \mid a$ and $n \nmid b$ and $n \nmid c$ or $n \nmid a$ and $n \nmid b$ and $n \nmid c$.

Let $a$, $b$, $c$ be integers. The functor $\mathrm{numberR}(a, b, c)$ yielding an element of $\mathbb{N}$ is defined by the term

(Def. 9) $$\begin{cases} 1, & \textbf{if } \text{two or more among numbers } a,\ b,\ c \text{ are even}, \\ 0, & \textbf{otherwise}. \end{cases}$$

Now we state the proposition:

(33) Let us consider a natural number $r$. If $r = \mathrm{numberR}(a, b, c)$, then two or more among numbers $a + r$, $b + r$, $c + r$ are odd.

Let $a$, $b$, $c$ be integers. The functor $\mathrm{numberR}_0(a, b, c)$ yielding an element of $\mathbb{Z}$ is defined by the term

(Def. 10) $$\begin{cases} 0, & \textbf{if } a,\ b,\ c \text{ give three different remainders} \\ & \text{upon dividing by } 3, \\ 1 - (a \bmod 3), & \textbf{if } a \bmod 3 = b \bmod 3 \text{ or } a \bmod 3 = c \bmod 3, \\ 1 - (b \bmod 3), & \textbf{otherwise}. \end{cases}$$

Now we state the proposition:

(34) Let us consider an integer $r_0$. Suppose $r_0 = \mathrm{numberR}_0(a, b, c)$. Then at least two of the numbers $a + r_0$, $b + r_0$, $c + r_0$ are not divisible by 3.

Let $h$ be an integer. The functor $\mathrm{PrimeDivisors}_{>3}(h)$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 11) $\mathrm{PrimeDivisors}(h) \cap \langle 4, \infty)_{\mathbb{N}}$.

Now we state the propositions:

(35) If $i \in \mathrm{PrimeDivisors}_{>3}(h)$, then $i > 3$.

(36) If $i \in \mathrm{PrimeDivisors}_{>3}(h)$, then $i \mid h$.

(37) If $i \in \mathrm{PrimeDivisors}_{>3}(h)$, then $i$ is prime.

(38) If $i$ is prime and $i > 3$ and $i \mid h$, then $i \in \mathrm{PrimeDivisors}_{>3}(h)$.

(39) If $h \neq 0$, then $\mathrm{PrimeDivisors}_{>3}(h) \subseteq \mathrm{Seg}\,|h|$. The theorem is a consequence of (35), (36), and (4).

Let $h$ be a non zero integer. One can verify that $\mathrm{PrimeDivisors}_{>3}(h)$ is included in a segment.

Let us consider a natural number $n$. Now we state the propositions:

(40) If $h \neq 0$, then if $n \in \mathrm{dom}(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))$,
then $(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))(n) > 3$. The theorem is a consequence of (35).

(41) If $h \neq 0$, then if $n \in \mathrm{dom}(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))$, then $(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))(n) \mid h$. The theorem is a consequence of (36).

(42) If $h \neq 0$, then if $n \in \mathrm{dom}(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))$, then $(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))(n)$ is prime. The theorem is a consequence of (37).

Let $a$, $b$, $c$ be integers. Assume $a$, $b$, $c$ are mutually different.

A Sierpiński45 finite sequence of $a$, $b$, $c$ is a finite sequence of elements of $\mathbb{Z}$ defined by

(Def. 12) there exists an integer $h$ and there exists a finite sequence $F$ of elements of $\mathbb{N}$ such that $h = (a-b)\cdot(a-c)\cdot(b-c)$ and $F = \mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h)$ and $\mathrm{len}\, \mathit{it} = \mathrm{len}\, F$ and for every object $i$ such that $i \in \mathrm{dom}\, \mathit{it}$ holds $F(i) \nmid a + \mathit{it}(i)$ and $F(i) \nmid b + \mathit{it}(i)$ and $F(i) \nmid c + \mathit{it}(i)$.

Now we state the propositions:

(43) Let us consider integers $a$, $b$, $c$, $h$. Suppose $h = (a-b)\cdot(a-c)\cdot(b-c)$. Let us consider a Sierpiński45 finite sequence $S$ of $a$, $b$, $c$. Suppose $a$, $b$, $c$ are mutually different. Let us consider a natural number $n$. Suppose $n \equiv \mathrm{numberR}(a,b,c) \pmod 2$ and $n \equiv \mathrm{numberR}_0(a,b,c) \pmod 3$ and for every natural number $i$ such that $i \in \mathrm{dom}\, S$ holds $n \equiv S(i) \pmod{(\mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h))(i)}$. Then $a+n$, $b+n$, $c+n$ are mutually coprime.

(44) If $h \neq 0$, then $\mathrm{rng}(\langle 2,3\rangle \frown \mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h)) \subseteq \mathbb{P}$.

Proof: Set $X = \mathrm{PrimeDivisors}_{>3}(h)$. Set $F = \mathrm{Sgm}\, X$. Set $f = \langle 2,3\rangle$. $\mathrm{rng}\, f \subseteq \mathbb{P}$. $\mathrm{rng}\, F \subseteq \mathbb{P}$. □

(45) If $h \neq 0$, then $\langle 2,3\rangle \frown \mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h)$ is Chinese remainder. The theorem is a consequence of (44), (21), (40), (23), and (42).

(46) If $a$, $b$, $c$ are mutually different, then $\{n$, where $n$ is a positive natural number : $a+n$, $b+n$, $c+n$ are mutually coprime$\}$ is infinite.

Proof: Set $A = \{n$, where $n$ is a positive natural number : $a+n$, $b+n$, $c+n$ are mutually coprime$\}$. Set $S =$ the Sierpiński45 finite sequence of $a$, $b$, $c$. Set $r = \mathrm{numberR}(a,b,c)$. Set $r_0 = \mathrm{numberR}_0(a,b,c)$.

Consider $h$ being an integer, $F$ being a finite sequence of elements of $\mathbb{N}$ such that $h = (a-b)\cdot(a-c)\cdot(b-c)$ and $F = \mathrm{Sgm}\,\mathrm{PrimeDivisors}_{>3}(h)$ and $\mathrm{len}\, S = \mathrm{len}\, F$ and for every object $i$ such that $i \in \mathrm{dom}\, S$ holds $F(i) \nmid a + S(i)$ and $F(i) \nmid b + S(i)$ and $F(i) \nmid c + S(i)$.

Set $m = \langle 2,3\rangle \frown F$. Set $u = \langle r, r_0\rangle \frown S$. $m(1) = 2$. $m(2) = 3$. $m$ is positive yielding. Set $Z = \{z$, where $z$ is a positive natural number : $z \equiv_{u(\cdot)} m(\cdot)\}$. $Z \subseteq A$. □

## 4. Problem 49

Let $n$ be a non zero natural number. One can check that PrimeDivisors($n$) is finite and PrimeDivisors($n$) is included in a segment.

Let $X$ be a non trivial, natural-membered set. Let us observe that there exists a subset of $X$ which is non empty and included in a segment.

Let $X$ be a non empty, included in a segment subset of $\mathbb{P}$. One can check that Sgm $X$ is non empty.

Let $X$ be an included in a segment subset of $\mathbb{P}$. Note that Sgm $X$ is positive yielding and Sgm $X$ is Chinese remainder.

Let $n$ be a non zero natural number. The functor $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n)$ yielding a finite sequence of elements of $\mathbb{P}$ is defined by the term

(Def. 13) Sgm PrimeDivisors($n$).

Let us note that $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n)$ is increasing. Now we state the proposition:

(47) Let us consider a non zero natural number $n$, and a natural number $i$. Suppose $i \in \mathrm{dom}(\mathrm{PrimeDivisors}_{\mathrm{FS}}(n))$. Then $(\mathrm{PrimeDivisors}_{\mathrm{FS}}(n))(i)$ is prime.

Let $m$ be a non zero natural number and $k$ be a natural number.

A Sierpiński49 finite sequence of $m$, $k$ is a finite sequence of elements of $\mathbb{Z}$ defined by

(Def. 14) $\mathrm{len}\, it = \mathrm{len}\, \mathrm{PrimeDivisors}_{\mathrm{FS}}(m)$ and for every object $i$ such that $i \in \mathrm{dom}\, it$ holds $(\mathrm{PrimeDivisors}_{\mathrm{FS}}(m))(i) \nmid it(i) \cdot (it(i) + 2 \cdot k)$.

Let $n$ be a non zero natural number. Observe that $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n)$ is Chinese remainder and positive yielding and $\mathrm{PrimeDivisors}_{\mathrm{FS}}(1)$ is empty.

Let us consider a non zero natural number $n$. Now we state the propositions:

(48) support PFExp($n$) = PrimeDivisors($n$).

Proof: Set $S$ = support PFExp($n$). Set $X$ = PrimeDivisors($n$). $S \subseteq X$ by [10, (34), (36)]. □

(49) If PrimeDivisors($n$) is empty, then $n = 1$.

(50) If $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n)$ is empty, then $n = 1$. The theorem is a consequence of (49).

Let $n$ be a non trivial natural number. Let us note that PrimeDivisors($n$) is non empty and $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n)$ is non empty.

Let us consider a non zero natural number $n$. Now we state the propositions:

(51) $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n) = \mathrm{sort}_{\mathrm{a}}\, \mathrm{CFS}(\mathrm{support}\, \mathrm{PFExp}(n))$. The theorem is a consequence of (48).

(52) $\mathrm{PrimeDivisors}_{\mathrm{FS}}(n) = \mathrm{sort}_{\mathrm{a}}\,\mathrm{CFS}(\mathrm{support}\,\mathrm{PPF}(n))$. The theorem is a consequence of (51).

(53) Let us consider an integer $j$. Suppose $j \neq 0$. Let us consider a positive natural number $n$. Suppose for every natural number $i$ such that $i \in \mathrm{dom}(\mathrm{PrimeDivisors}_{\mathrm{FS}}(n))$ holds $j$ and $(\mathrm{PrimeDivisors}_{\mathrm{FS}}(n))(i)$ are relatively prime. Then $j$ and $n$ are relatively prime. The theorem is a consequence of (52) and (10).

(54) Let us consider a positive natural number $m$, a natural number $k$, a Sierpiński49 finite sequence $S$ of $m$, $k$, and a CR-sequence $q$. Suppose $q = \mathrm{PrimeDivisors}_{\mathrm{FS}}(m)$. Then there exist positive natural numbers $a$, $b$ such that

(i) $2 \cdot k = a - b$, and

(ii) $a$ and $m$ are relatively prime, and

(iii) $b$ and $m$ are relatively prime, and

(iv) $a = \mathrm{CRT}(S, q) + \prod q + 2 \cdot k$, and

(v) $b = \mathrm{CRT}(S, q) + \prod q$.

Proof: Define $\mathcal{F}(\text{integer}) = \$_1 \cdot (\$_1 + 2 \cdot k)(\in \mathbb{Z})$. Consider $f$ being a function from $\mathbb{Z}$ into $\mathbb{Z}$ such that for every element $x$ of $\mathbb{Z}$, $f(x) = \mathcal{F}(x)$. Set $x_0 = \mathrm{CRT}(S, q) + 1 \cdot (\prod q)$. For every natural number $i$ such that $i \in \mathrm{dom}\, q$ holds $f(x_0) \equiv f(S(i)) \pmod{q(i)}$. For every natural number $i$ such that $i \in \mathrm{dom}\, q$ holds $f(S(i)) \not\equiv 0 \pmod{q(i)}$. For every natural number $i$ such that $i \in \mathrm{dom}\, q$ holds $f(x_0)$ and $q(i)$ are relatively prime. $f(x_0)$ and $m \cdot 1$ are relatively prime. □

(55) Let us consider a positive natural number $m$, and a natural number $k$. Then there exist positive natural numbers $a$, $b$ such that

(i) $2 \cdot k = a - b$, and

(ii) $a$ and $m$ are relatively prime, and

(iii) $b$ and $m$ are relatively prime.

The theorem is a consequence of (54) and (50).

## 5. Problem 120

Now we state the proposition:

(56) Let us consider a non zero natural number $m$. Then there exists a natural number $s$ such that for every natural number $n$ such that $n > s$ holds $2^m \cdot 2^{2^n} + 1$ is composite.

## 6. Problem 131

Let $i$ be an integer. A multiple of $i$ is an integer defined by

(Def. 15) $i \mid it$.

Now we state the propositions:

(57) $i \cdot j$ is a multiple of $i$.

(58) If $j$ is a multiple of $i$, then $j + h \cdot i$ is a multiple of $i$.

(59) If $i \neq 1$ and $i \neq -1$, then for every multiple $m$ of $i$ such that $m$ is prime holds $m = i$ or $m = -i$.

(60) If $n \neq 1$, then for every multiple $m$ of $n$ such that $m$ is prime holds $m = n$. The theorem is a consequence of (59).

Let us consider $i$. The functor multiples($i$) yielding a subset of $\mathbb{Z}$ is defined by the term

(Def. 16) the set of all $m$ where $m$ is a multiple of $i$.

Now we state the propositions:

(61) Let us consider an object $x$. If $x \in$ multiples($i$), then $x$ is a multiple of $i$.

(62) $j \in$ multiples($i$) if and only if $i \mid j$. The theorem is a consequence of (61).

(63) $i \cdot j \in$ multiples($i$). The theorem is a consequence of (57).

Let us consider $i$. Note that multiples($i$) is non empty. Now we state the propositions:

(64) multiples(0) $= \{0\}$. The theorem is a consequence of (61).

(65) multiples(1) $= \mathbb{Z}$.

(66) multiples($-1$) $= \mathbb{Z}$.

Let $i$ be a non zero integer. Let us note that $i \cdot \mathrm{id}_{\mathbb{Z}}$ is one-to-one. Now we state the proposition:

(67) Let us consider a non zero integer $i$. Then $\mathbb{Z} \approx$ multiples($i$). The theorem is a consequence of (61).

Let $i$ be a non zero integer. Note that multiples($i$) is infinite. Now we state the proposition:

(68) If $i \neq 1$ and $i \neq -1$ and $i$ is not prime and $-i$ is not prime, then multiples($i$) misses $\mathbb{P}$. The theorem is a consequence of (61).

Let us consider $m$ and $n$. The functor PrimeNumbers($m, n$) yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 17) seq$(m, n) \cap \mathbb{P}$.

One can verify that PrimeNumbers($m, n$) is finite. Now we state the propositions:

(69) PrimeNumbers$(0, 10) = \{2, 3, 5, 7\}$.

(70) $\mathrm{PrimeNumbers}(1, 10) = \{2, 3, 5, 7, 11\}$.

(71) $\mathrm{PrimeNumbers}(2, 10) = \{3, 5, 7, 11\}$.

(72) $\mathrm{PrimeNumbers}(3, 10) = \{5, 7, 11, 13\}$.

(73) $\overline{\overline{\mathrm{seq}(m, n)}} = n$.

(74) $\mathrm{seq}(m, n)$ misses $\{m + n + 1, m + n + 2\}$.

(75) If $a$ is even, then $a$ is a multiple of 2.

(76) If $a$ is even, then $a \in \mathrm{multiples}(2)$. The theorem is a consequence of (75).

(77) If $a$ is odd, then $a$ is not a multiple of 2.

(78) If $a$ is odd, then $a \notin \mathrm{multiples}(2)$. The theorem is a consequence of (61) and (77).

(79) If $a$ is even, then $\mathrm{multiples}(2) \cap \{a, a + 1\} = \{a\}$. The theorem is a consequence of (61) and (76).

(80) If $a$ is odd, then $\mathrm{multiples}(2) \cap \{a, a + 1\} = \{a + 1\}$. The theorem is a consequence of (61) and (76).

(81) (i) $\mathrm{multiples}(2) \cap \{a, a + 1\} = \{a\}$, or

(ii) $\mathrm{multiples}(2) \cap \{a, a + 1\} = \{a + 1\}$.

(82) $\overline{\overline{\mathrm{multiples}(2) \cap \{a, a + 1\}}} = 1$. The theorem is a consequence of (79) and (80).

(83) $\overline{\overline{\mathrm{multiples}(2) \cap \mathrm{seq}(k, 2 \cdot m)}} = m$.

PROOF: Set $M = \mathrm{multiples}(2)$. Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{M \cap \mathrm{seq}(k, 2 \cdot \$_1)}} = \$_1$. $\mathcal{P}[0]$. For every natural number $z$ such that $\mathcal{P}[z]$ holds $\mathcal{P}[z + 1]$. For every natural number $z$, $\mathcal{P}[z]$. □

(84) If $n \geqslant 8$, then there exists a multiple $m$ of 3 such that $m \in \mathrm{seq}(k, n)$ and $m$ is odd. The theorem is a consequence of (58).

(85) Let us consider a prime number $p$. Suppose $p \leqslant k$. Then $\mathrm{multiples}(p) \cap \mathrm{seq}(k, m)$ misses $\mathrm{PrimeNumbers}(k, m)$. The theorem is a consequence of (61).

(86) $\overline{\overline{\mathrm{PrimeNumbers}(0, 10)}} = 4$.

(87) $\overline{\overline{\mathrm{PrimeNumbers}(1, 10)}} = 5$. The theorem is a consequence of (70).

(88) If $2 \leqslant k$, then $\overline{\overline{\mathrm{PrimeNumbers}(k, 10)}} \leqslant 4$. The theorem is a consequence of (71), (84), (61), (83), (73), (62), and (60).

## 7. Problem 144

Let $A$ be a set. One can verify that every element of $\mathbb{N}_{\rm even} \setminus A$ is even and there exists an element of $\mathbb{N}_{\rm even} \setminus A$ which is even. Now we state the proposition:

(89) Let us consider a non zero integer $D$. Then $\{\langle x, y, z\rangle$, where $x$, $y$, $z$ are positive natural numbers : $x^{\mathbf{2}} - D \cdot y^{\mathbf{2}} = z^{\mathbf{2}}$ and $x$ and $y$ are relatively prime$\}$ is infinite.

## 8. Problem 148

Now we state the propositions:

(90) Let us consider complex numbers $x$, $y$, $z$. Then $x^{\mathbf{2}}+y^{\mathbf{2}}+z^{\mathbf{2}}+x+y+z = 1$ if and only if $(2 \cdot x+1)^{\mathbf{2}} + (2 \cdot y+1)^{\mathbf{2}} + (2 \cdot z+1)^{\mathbf{2}} = 7$.

(91) Let us consider integers $a$, $b$, $c$. Suppose $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $4 = 0$. Then

(i) $a$ is even, and

(ii) $b$ is even, and

(iii) $c$ is even.

(92) (i) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 0$, or

(ii) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 1$, or

(iii) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 2$, or

(iv) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 3$, or

(v) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 4$, or

(vi) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 5$, or

(vii) $a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$ mod $8 = 6$.

(93) There exist no rational numbers $x$, $y$, $z$ such that $x^{\mathbf{2}} + y^{\mathbf{2}} + z^{\mathbf{2}} = 7$.
Proof: Consider $n_1$, $m_1$ being integers such that $m_1 > 0$ and $x = \frac{n_1}{m_1}$. Consider $n_2$, $m_2$ being integers such that $m_2 > 0$ and $y = \frac{n_2}{m_2}$. Consider $n_3$, $m_3$ being integers such that $m_3 > 0$ and $z = \frac{n_3}{m_3}$. Set $a = n_1 \cdot m_2 \cdot m_3$. Set $b = n_2 \cdot m_1 \cdot m_3$. Set $c = n_3 \cdot m_1 \cdot m_2$. Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \neq 0$ and there exist integers $a$, $b$, $c$ such that $7 \cdot \$_1^{\mathbf{2}} = a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$. Consider $M$ being a natural number such that $\mathcal{P}[M]$ and for every natural number $n$ such that $\mathcal{P}[n]$ holds $M \leqslant n$. Consider $a$, $b$, $c$ being integers such that $7 \cdot M^{\mathbf{2}} = a^{\mathbf{2}} + b^{\mathbf{2}} + c^{\mathbf{2}}$. □

(94) There exist no rational numbers $x$, $y$, $z$ such that $x^{\mathbf{2}}+y^{\mathbf{2}}+z^{\mathbf{2}}+x+y+z = 1$. The theorem is a consequence of (93).

## 9. Problem 149

Now we state the proposition:

(95) There exist no positive integers $x$, $y$, $z$ such that $4 \cdot x \cdot y - x - y = z^{\mathbf{2}}$.
Proof: Consider $p$, $k$ being natural numbers such that $p = 4 \cdot k + 3$ and $p$ is prime and $p \mid 4 \cdot (x - 1) + 3$. $2 \cdot z$ and $p$ are relatively prime by [18, (1)], [7, (15)]. □

The functor SierpińskiEx149 yielding a function from $\mathbb{N}_+$ into $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is defined by

(Def. 18) for every non zero natural number $n$, $it(n) = \langle -1, -5 \cdot n^{\mathbf{2}} - 2 \cdot n, -5 \cdot n - 1 \rangle$.

Note that SierpińskiEx149 is one-to-one. Now we state the propositions:

(96) rng SierpińskiEx149 $\subseteq \{\langle x, y, z \rangle$, where $x, y, z$ are negative integers : $4 \cdot x \cdot y - x - y = z^{\mathbf{2}}\}$.

(97) $\{\langle x, y, z \rangle$, where $x$, $y$, $z$ are negative integers : $4 \cdot x \cdot y - x - y = z^{\mathbf{2}}\}$ is infinite. The theorem is a consequence of (96).

## 10. Problem 150

Let $m$, $D$ be complex numbers. The functor SierpińskiEx150$(m, D)$ yielding a sequence of $\mathbb{C} \times \mathbb{C}$ is defined by

(Def. 19) $it(0) = \langle 2 \cdot m^{\mathbf{2}} + 1, 2 \cdot m \rangle$ and for every natural number $n$, $it(n + 1) = \langle ((it(n))_{\mathbf{1}})^{\mathbf{2}} + D \cdot ((it(n))_{\mathbf{2}})^{\mathbf{2}}, 2 \cdot ((it(n))_{\mathbf{1}}) \cdot ((it(n))_{\mathbf{2}}) \rangle$.

Let $m$, $D$ be real numbers. Let us note that SierpińskiEx150$(m, D)$ is $(\mathbb{R} \times \mathbb{R})$-valued. Let $m$, $D$ be rational numbers. One can verify that SierpińskiEx150$(m, D)$ is $(\mathbb{Q} \times \mathbb{Q})$-valued. Let $m$, $D$ be integers. Let us note that SierpińskiEx150$(m, D)$ is $(\mathbb{Z} \times \mathbb{Z})$-valued.

Let $m$, $D$ be natural numbers. One can verify that SierpińskiEx150$(m, D)$ is $(\mathbb{N} \times \mathbb{N})$-valued. Let $m$, $D$ be positive, natural numbers and $n$ be a natural number. One can verify that $((\text{SierpińskiEx150}(m, D))(n))_{\mathbf{1}}$ is positive and $((\text{SierpińskiEx150}(m, D))(n))_{\mathbf{2}}$ is positive. Now we state the proposition:

(98) Let us consider positive, natural numbers $m$, $D$, and natural numbers $a$, $b$. Suppose $a < b$. Then

(i) $((\text{SierpińskiEx150}(m, D))(a))_{\mathbf{1}} < ((\text{SierpińskiEx150}(m, D))(b))_{\mathbf{1}}$, and

(ii) $((\text{SierpińskiEx150}(m, D))(a))_{\mathbf{2}} < ((\text{SierpińskiEx150}(m, D))(b))_{\mathbf{2}}$.

Proof: Set $f = \text{SierpińskiEx150}(m, D)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 > a$, then $(f(\$_1))_{\mathbf{1}} > (f(a))_{\mathbf{1}}$ and $(f(\$_1))_{\mathbf{2}} > (f(a))_{\mathbf{2}}$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number $k$, $\mathcal{P}[k]$. □

Let $m$, $D$ be positive, natural numbers. One can check that SierpińskiEx150 $(m, D)$ is one-to-one. Now we state the proposition:

(99) Let us consider positive integers $D$, $m$. Suppose $D = m^{\mathbf{2}} + 1$. Then $\{\langle x, y\rangle$, where $x$, $y$ are positive integers : $x^{\mathbf{2}} - D \cdot y^{\mathbf{2}} = 1\}$ is infinite.
PROOF: Set $f =$ SierpińskiEx150$(m, D)$. Define $\mathcal{R}$[complex number, compex number] $\equiv \$_1^{\mathbf{2}} - D \cdot \$_2^{\mathbf{2}} = 1$. Set $A = \{\langle x, y\rangle$, where $x, y$ are positive integers : $\mathcal{R}[x, y]\}$. Define $\mathcal{F}$(real number, real number) $= \$_1^{\mathbf{2}} + D \cdot \$_2^{\mathbf{2}}$. Define $\mathcal{G}$(real number, real number) $= 2 \cdot \$_1 \cdot \$_2$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1) \in A$. For every natural number $a$ such that $\mathcal{N}[a]$ holds $\mathcal{N}[a+1]$. For every natural number $a$, $\mathcal{N}[a]$. $\operatorname{rng} f \subseteq A$. □

## 11. PROBLEM 151

Now we state the propositions:

(100) If $2^2 \leqslant n$ and $2^n \mid i^3$, then $2^2 \mid i$. The theorem is a consequence of (4).

(101) If $2^3 \leqslant n$ and $2^n \mid i^3$, then $2^3 \mid i$. The theorem is a consequence of (4).

(102) If $i$ and $j$ are relatively prime and $p^n \mid i \cdot j$, then $p^n \mid i$ or $p^n \mid j$. The theorem is a consequence of (4).

(103) If $n$ is odd and $i$ and $j$ are relatively prime and $i \cdot j = z^n$, then there exists an integer $k$ such that $i = k^n$.

(104) If $n$ is odd, then for every negative real numbers $r$, $s$ such that $r \leqslant s$ holds $r^n \leqslant s^n$.

(105) If $0 \leqslant j$ and $j^{\mathbf{2}} < z < (j+1)^{\mathbf{2}}$, then there exists no integer $i$ such that $z = i^{\mathbf{2}}$.

(106) $\{\langle x, y\rangle$, where $x, y$ are integers : $y^2 = x^3 + (x+4)^2\} = \{\langle 0, 4\rangle, \langle 0, -4\rangle\}$.
PROOF: Set $A = \{\langle x, y\rangle$, where $x, y$ are integers : $y^2 = x^3 + (x+4)^2\}$. $A \subseteq \{\langle 0, 4\rangle, \langle 0, -4\rangle\}$. □

## 12. PROBLEM 152

Now we state the propositions:

(107) Let us consider a complex number $m$, and non zero complex numbers $x$, $y$, $z$. Then $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m$ if and only if $x^{\mathbf{2}} \cdot z + y^{\mathbf{2}} \cdot x + z^{\mathbf{2}} \cdot y = m \cdot x \cdot y \cdot z$.

(108) Let us consider an integer $m$, and non zero integers $x$, $y$, $z$. Suppose $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m$ and $x$, $y$, $z$ are mutually coprime. Then

(i) $x = 1$ or $x = -1$, and

(ii) $y = 1$ or $y = -1$, and

(iii) $z = 1$ or $z = -1$.

The theorem is a consequence of (107) and (14).

(109) Let us consider an integer $m$, and positive integers $x$, $y$, $z$. Suppose $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m$ and $x$, $y$, $z$ are mutually coprime. Then

(i) $x = 1$, and

(ii) $y = 1$, and

(iii) $z = 1$.

(110) $\{\langle x, y, z \rangle$, where $x, y, z$ are positive integers : $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$ and $x$, $y$, $z$ are mutually coprime$\} = \{\langle 1, 1, 1 \rangle\}$. The theorem is a consequence of (108).

(111) $\{\langle x, y, z \rangle$, where $x, y, z$ are non zero integers : $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$ and $x$, $y$, $z$ are mutually coprime$\} = \{\langle 1, 1, 1 \rangle, \langle -1, -1, -1 \rangle\}$. The theorem is a consequence of (108) and (11).

(112) Let us consider a natural number $m$. Suppose $m \neq 3$. Then there exist no non zero integers $x$, $y$, $z$ such that $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m$ and $x$, $y$, $z$ are mutually coprime. The theorem is a consequence of (108).

## References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Edward J. Barbeau. *Pell's Equation.* Problem Books in Mathematics. Springer, 2003.

[3] Robert D. Carmichael. *Diophantine Analysis.* New York, John Wiley & Sons, 1915.

[4] Adam Grabowski. Elementary number theory problems. Part XII – primes in arithmetic progression. *Formalized Mathematics*, 31(1):277–286, 2023. doi:10.2478/forma-2023-0022.

[5] Adam Grabowski and Christoph Schwarzweller. Revisions as an essential tool to maintain mathematical repositories. In M. Kauers, M. Kerber, R. Miner, and W. Windsteiger, editors, *Towards Mechanized Mathematical Assistants. Lecture Notes in Computer Science*, volume 4573, pages 235–249. Springer: Berlin, Heidelberg, 2007.

[6] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[7] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.

[8] Artur Korniłowicz. Elementary number theory problems. Part IX. *Formalized Mathematics*, 31(1):161–169, 2023. doi:10.2478/forma-2023-0015.

[9] Artur Korniłowicz and Adam Naumowicz. Elementary number theory problems. Part V. *Formalized Mathematics*, 30(**3**):229–234, 2022. doi:10.2478/forma-2022-0018.

[10] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[11] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[12] Andrzej Schinzel. Démonstration d'une conséquence de l'hypothèse de Goldbach. *Compositio Mathematica*, 14:74–76, 1959.

[13] Andrzej Schinzel and Wacław Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, 4(3):185–208, 1958.

[14] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**): 247–252, 2008. doi:10.2478/v10037-008-0029-8.

[15] Wacław Sierpiński. *Elementary Theory of Numbers.* PWN, Warsaw, 1964.

[16] Wacław Sierpiński. *250 Problems in Elementary Number Theory.* Elsevier, 1970.

[17] Wacław Sierpiński. Remarques sur le travail de M. J. W. S. Cassels «On a diophantine equation». *Acta Arithmetica*, 6(4):469–471, 1961.

[18] Li Yan, Xiquan Liang, and Junjie Zhao. Gauss lemma and law of quadratic reciprocity. *Formalized Mathematics*, 16(**1**):23–28, 2008. doi:10.2478/v10037-008-0004-4.

*Accepted October 22, 2024*