FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 171–180, 2023
DOI: 10.2478/forma-2023-0016
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part X – Diophantine Equations

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

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

MSC: 11A41 11D72 68V20

Keywords: number theory; Diophantine equations

MML identifier: `NUMBER10`, version: `8.1.14 5.76.1452`

Introduction

In this paper, Problems 84, 94, 99 from Section IV, 170, 173, 174, 175, 177, 179, 186, 187, 189, 190, 193, 194, 197, and 199 from Section V of [10] are formalized, using the Mizar formalism [1]. It contributes to the project announced in [6].

Some of the problems in the book are formulated in terms of *positive integers*. To represent such numbers in the Mizar Mathematical Library [2], we use notions either `positive Integer` or `positive Nat` or `non zero Nat`, which are automatically understood as equivalent due to the built-in processing of adjectives by the Mizar checker.

For proving the infiniteness of the set of pairs of consecutive primes that are not twin primes (Problem 84), we implemented the operation $\max\langle 0, 6\cdot n+1\rangle_{\mathbb{P}}$, which represents the largest prime $\leqslant 6n+1$ denoted as p_{k_n} in the book. We noted a small misprint in the proof presented in the book in the equation $(6n+5)+(6n+1)=4$ – it should be $(6n+5)-(6n+1)=4$.

Problem 179 asks about all rational solutions of the equation

$$(x+1)^3+(x+2)^3+(x+3)^3+(x+4)^3=(x+10)^3.$$

We generalized the problem to real numbers and presented the only solution $x = 10$ in reals, which is also the only solution in rationals. Moreover, we computed that the substitution $x = t + 10$ proposed in the book results in the equation $t(t^2 + 30t + 230) = 0$.

The infiniteness of sets defined in Problems 189, 190, and 199 is proven using function `recSeqCart` [4] with parameters adequate to given problems.

Problem 197 is devoted to the existence of solutions of the equation

$$x_1 + x_2 + \cdots + x_n = x_1 x_2 \cdots x_n$$

in positive integers. In the case of $n > 2$, the proof in the book proposes $x_{n-1} = 1$, but we computed that x_{n-1} must be equal to 2.

Proofs of other problems are straightforward formalizations of solutions given in the book, by means of available development of number theory in Mizar [9], using ellipsis [3] extensively, looking forward for more advanced automatization of arithmetical calculations [7].

1. Preliminaries

From now on a, b, c, k, m, n denote natural numbers, i, j, x, y denote integers, p, q denote prime numbers, and r, s denote real numbers. Now we state the propositions:

(1) Let us consider natural numbers i, j. If $i < j$, then there exists a positive natural number k such that $j = i + k$.

(2) Let us consider a positive yielding, integer-valued finite sequence f. Then $\prod f \geqslant 1$.

PROOF: Define $\mathcal{P}[\text{set}] \equiv$ for every positive yielding, integer-valued finite sequence F such that $F = \$_1$ holds $\prod F \geqslant 1$. For every finite sequence p of elements of $\mathbb{Z}$ and for every element x of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p ^\frown \langle x \rangle]$. For every finite sequence p of elements of $\mathbb{Z}$, $\mathcal{P}[p]$. $\square$

(3) If $m \geqslant 2$ and $n \geqslant 2$, then $m \cdot n$ is composite.

(4) If $p \nmid n$, then n and p are relatively prime.

(5) $-1 \bmod p = p - 1$.

2. Problem 84

Let r, s be complex numbers. We say that r and s are twin if and only if

(Def. 1) $|s - r| = 2$.

One can verify that the predicate is irreflexive and symmetric. Now we state the proposition:

(6) If $r \leqslant s$, then r and s are twin iff $s - r = 2$.

Let us consider n. The functor $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 2) $\{a$, where a is a natural number : $a \leqslant 6 \cdot n + 1\}$.

Now we state the propositions:

(7) $a \leqslant 6 \cdot n + 1$ if and only if $a \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$.

(8) $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \subseteq \mathbb{Z}_{6 \cdot n+2}$.

Let us consider n. Observe that $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$ is non empty and finite. Now we state the propositions:

(9) If $m \leqslant n$, then $\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{N}} \subseteq \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$. The theorem is a consequence of (7).

(10) If $m < n$, then $\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{N}} \subset \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$. The theorem is a consequence of (9) and (7).

(11) If $\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{N}} = \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$, then $m = n$. The theorem is a consequence of (10).

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

(12) $2 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

(13) $3 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

(14) $5 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

(15) $7 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

Let n be a non zero natural number. Observe that $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$ is non empty.

The functor $\max\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{P}}$ yielding a prime number is defined by the term

(Def. 3) $\max(\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P})$.

Now we state the propositions:

(16) Let us consider non zero natural numbers m, n. Suppose $m \leqslant n$. Then $\max\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{P}} \leqslant \max\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{P}}$. The theorem is a consequence of (9).

(17) $\max\langle 0, 6 \cdot 20 + 1 \rangle_{\mathbb{P}} = \max\langle 0, 6 \cdot 19 + 1 \rangle_{\mathbb{P}}$.
Proof: Set $a = 20$. Set $b = 19$. Set $X = \langle 0, 6 \cdot a + 1 \rangle_{\mathbb{N}}$. Set $B = \max\langle 0, 6 \cdot b + 1 \rangle_{\mathbb{P}}$. $B \leqslant 6 \cdot b + 1$. For every extended real x such that $x \in X \cap \mathbb{P}$ holds $x \leqslant B$. □

(18) $\langle 0, 6 \cdot 1 + 1 \rangle_{\mathbb{N}} = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

(19) $\max\langle 0, 6 \cdot 1 + 1 \rangle_{\mathbb{P}} = 7$.

(20) If $\mathrm{pr}(m) = \mathrm{pr}(n)$, then $m = n$.

Let p be a natural number. Assume p is prime. The functor $\mathrm{primeindex}(p)$ yielding an element of $\mathbb{N}$ is defined by

(Def. 4) $\mathrm{pr}(it) = p$.

Now we state the propositions:

(21) If $\mathrm{primeindex}(p) = \mathrm{primeindex}(q)$, then $p = q$.

(22) $\mathrm{primeindex}(2) = 0$.

(23) $\mathrm{primeindex}(3) = 1$.

(24) $\mathrm{primeindex}(5) = 2$.

(25) $\mathrm{primeindex}(7) = 3$.

(26) $\mathrm{primeindex}(11) = 4$.

(27) $\mathrm{primeindex}(13) = 5$.

(28) If $n > 0$, then $p < \mathrm{pr}(n + \mathrm{primeindex}(p))$.

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

(29) $\mathrm{pr}(1 + \mathrm{primeindex}(\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}})) \geqslant 6 \cdot n + 5$. The theorem is a consequence of (28).

(30) $\mathrm{pr}(1 + \mathrm{primeindex}(\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}})) - \max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}} \geqslant 4$. The theorem is a consequence of (7) and (29).

(31) $\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}$ and $\mathrm{pr}(1 + \mathrm{primeindex}(\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}))$ are not twin. The theorem is a consequence of (28), (30), and (6).

(32) Let us consider a non zero natural number m. Suppose $6 \cdot m + 1$ is prime. Then $6 \cdot m + 1 = \max\langle 0, 6 \cdot m + 1\rangle_{\mathbb{P}}$. The theorem is a consequence of (7).

Let us consider non zero natural numbers m, n. Now we state the propositions:

(33) If $6 \cdot n + 1$ is prime and $m < n$, then $\max\langle 0, 6 \cdot m + 1\rangle_{\mathbb{P}} < \max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}$. The theorem is a consequence of (16), (32), and (7).

(34) Suppose $6 \cdot m + 1$ is prime and $6 \cdot n + 1$ is prime and $\max\langle 0, 6 \cdot m + 1\rangle_{\mathbb{P}} = \max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}$. Then $m = n$. The theorem is a consequence of (33).

The functor $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 5) $\{6 \cdot n + 1$, where n is a natural number : $6 \cdot n + 1$ is prime$\}$.

Note that $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$ has non empty elements. Now we state the proposition:

(35) $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}} \subseteq \mathbb{P}$.

One can check that $\{6n+1 : n \in \mathbb{N}\}_{\mathbb{P}}$ is infinite. Now we state the proposition:

(36) $\{\langle p, q\rangle$, where p, q are prime numbers : p and q are not twin$\}$ is infinite.
Proof: Set $A = \{\langle p, q\rangle$, where p, q are prime numbers : p and q are not twin$\}$. Define $\mathcal{S}(\text{non zero natural number}) = \max\langle 0, 6 \cdot \$_1 + 1\rangle_{\mathbb{P}}$. Define $\mathcal{F}(\text{non zero natural number}) = \langle \mathcal{S}(\$_1), \mathrm{pr}(1 + \mathrm{primeindex}(\mathcal{S}(\$_1)))\rangle$.

Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv$ there exists a non zero natural number n such that $n = \$_1$ and $\$_2 = \mathcal{F}(n)$. Set $P = \{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$. Define $\mathcal{C}(\text{element of } P) = (\$_1 - 1 \operatorname{div} 6)(\in \mathbb{N})$. Consider C being a function from P into $\mathbb{N}$ such that for every element p of P, $C(p) = \mathcal{C}(p)$. C is one-to-one. Reconsider $D = \operatorname{rng} C$ as an infinite subset of $\mathbb{N}$. For every element d of D, $6 \cdot d + 1$ is prime. For every element i of D, there exists an object j such that $\mathcal{P}[i, j]$. Consider f being a many sorted set indexed by D such that for every element d of D, $\mathcal{P}[d, f(d)]$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

3. Problem 94

Let c be a complex number. We say that c is a product of three different primes if and only if

(Def. 6) there exist prime numbers p, q, r such that p, q, r are mutually different and $c = p \cdot q \cdot r$.

Now we state the propositions:

(37) If $n > 4$, then there exists a natural number k such that $n = 2 \cdot k$ and $k > 2$ or $n = 2 \cdot k + 1$ and $k > 1$.

(38) If $n > 4$, then there exists a natural number m such that $n < m < 2 \cdot n$ and m is a product of two different primes. The theorem is a consequence of (37) and (3).

(39) If $n > 15$, then there exists a natural number m such that $n < m < 2 \cdot n$ and m is a product of three different primes. The theorem is a consequence of (3).

4. Problem 99

Now we state the proposition:

(40) $5 \mid 2^{4 \cdot n + 2} + 1$.

Let us consider n. Note that $\frac{1}{5} \cdot (2^{4 \cdot n + 2} + 1)$ is natural. Now we state the proposition:

(41) If $n > 1$, then $\frac{1}{5} \cdot (2^{4 \cdot n + 2} + 1)$ is composite. The theorem is a consequence of (40) and (3).

5. Problem 170

Now we state the proposition:

(42) $\{\langle x, y, z \rangle$, where x, y, z are integers : $x + y + z = 3$ and $x^3 + y^3 + z^3 = 3\} = \{\langle 1, 1, 1 \rangle, \langle -5, 4, 4 \rangle, \langle 4, -5, 4 \rangle, \langle 4, 4, -5 \rangle\}$.

PROOF: Set $A = \{\langle x, y, z \rangle$, where x, y, z are integers : $x + y + z = 3$ and $x^3 + y^3 + z^3 = 3\}$. Set $B = \{\langle 1, 1, 1 \rangle, \langle -5, 4, 4 \rangle, \langle 4, -5, 4 \rangle, \langle 4, 4, -5 \rangle\}$. $A \subseteq B$ by [8, (2)]. □

6. Problem 173

Now we state the proposition:

(43) Let us consider positive natural numbers m, n. Then there exist integers a, b, c such that $\{\langle x, y\rangle$, where x, y are natural numbers : $a \cdot x + b \cdot y = c\} = \{\langle m, n\rangle\}$.
PROOF: Consider a being a prime number such that $a > m + n$. Consider b being a prime number such that $b > a$. Set $A = \{\langle x, y\rangle$, where x, y are natural numbers : $a \cdot x + b \cdot y = c\}$. Set $B = \{\langle m, n\rangle\}$. $A \subseteq B$. $\square$

7. Problem 174

Let us consider a positive natural number m. Now we state the propositions:

(44) $\overline{\overline{\{\langle x, y\rangle, \text{ where } x, y \text{ are positive natural numbers} : x + y = m + 1\}}} = m$.
PROOF: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $x+y = m + 1\}$. $\mathrm{Seg}\, m \approx A$. $\square$

(45) There exist positive natural numbers a, b, c such that $\overline{\overline{\{\langle x, y\rangle, \text{ where } x, y \text{ are positive natural numbers} : a \cdot x + b \cdot y = c\}}} = m$. The theorem is a consequence of (44).

8. Problem 175

Now we state the proposition:

(46) Let us consider a positive natural number m. Then $\overline{\overline{\{\langle x, y\rangle, \text{ where } x, y \text{ are positive natural numbers} : x^{\mathbf{2}} + y^{\mathbf{2}} + 2 \cdot x \cdot y - m \cdot x - m \cdot y - m - 1 = 0\}}} = m$. The theorem is a consequence of (44).

9. Problem 177

Let b, e be real numbers and n be a natural number. The functor powersFS(b, e, n) yielding a finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 7) $\mathrm{len}\, it = n$ and for every natural number i such that $1 \leqslant i \leqslant n$ holds $it(i) = (b + i)^e$.

Now we state the propositions:

(47) $\mathrm{powersFS}(-(k + 1), r, 2 \cdot (k + 1)) = (\langle(-k)^r\rangle \frown \mathrm{powersFS}(-k, r, 2 \cdot k)) \frown \langle(k + 1)^r\rangle$.

(48) Let us consider a positive natural number k. Then powersFS$(-(k+1), r, 2\cdot (k+1)-1) = (\langle (-k)^r \rangle ^\frown \text{powersFS}(-k, r, 2\cdot k-1)) ^\frown \langle k^r \rangle$.

(49) $\sum \text{powersFS}(-k, 3, 2\cdot k) = k^3$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \sum \text{powersFS}(-\$_1, 3, 2\cdot \$_1) = {\$_1}^3$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(50) Let us consider a positive natural number k. Then $\sum \text{powersFS}(-k, 3, 2\cdot k-1) = 0$.
PROOF: Define $\mathcal{P}$[non zero natural number] $\equiv \sum \text{powersFS}(-\$_1, 3, 2\cdot \$_1 - 1) = 0$. $\mathcal{P}[1]$. For every non zero natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every non zero natural number n, $\mathcal{P}[n]$. □

(51) Let us consider a positive natural number n. Then there exists an integer x and there exists a natural number y such that $\sum \text{powersFS}(x, 3, n) = y^3$. The theorem is a consequence of (49) and (50).

10. PROBLEM 179

Now we state the proposition:

(52) Let us consider a real number x. Then $(x+1)^3 + (x+2)^3 + (x+3)^3 + (x+4)^3 = (x+10)^3$ if and only if $x = 10$.
PROOF: If $(x+1)^3 + (x+2)^3 + (x+3)^3 + (x+4)^3 = (x+10)^3$, then $x = 10$. □

11. PROBLEM 186

Now we state the proposition:

(53) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x + 1 = y^{\mathbf{2}}\} = \{\langle 3, 3\rangle\}$.
PROOF: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x + 1 = y^{\mathbf{2}}\}$. $A \subseteq \{\langle 3, 3\rangle\}$ by [11, (36)]. □

12. PROBLEM 187

Now we state the proposition:

(54) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x - 1 = y^{\mathbf{2}}\} = \{\langle 1, 1\rangle\}$.
PROOF: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x - 1 = y^{\mathbf{2}}\}$. $A \subseteq \{\langle 1, 1\rangle\}$ by [5, (11)]. □

13. Problem 189

Now we state the propositions:

(55) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $(2\cdot x+1)^{\mathbf{2}}-2\cdot y^{\mathbf{2}}+1=0\}$ is infinite.

Proof: Define $\mathcal{R}$(complex number, complex number) $=(2\cdot\$_1+1)^{\mathbf{2}}-2\cdot\$_2^{\mathbf{2}}+1$. Set $A=\{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x,y)=0\}$. Set $f=\mathrm{recSeqCart}(3,5,3,2,1,4,3,2)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1)\in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. $\mathrm{rng}\, f\subseteq A$. □

(56) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $x^{\mathbf{2}}+(x+1)^{\mathbf{2}}=y^{\mathbf{2}}\}$ is infinite. The theorem is a consequence of (55).

14. Problem 190

Now we state the propositions:

(57) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $3\cdot x^{\mathbf{2}}+3\cdot x-y^{\mathbf{2}}+1=0\}$ is infinite.

Proof: Define $\mathcal{R}$(complex number, complex number) $=3\cdot\$_1^{\mathbf{2}}+3\cdot\$_1-\$_2^{\mathbf{2}}+1$. Set $A=\{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x,y)=0\}$. Set $f=\mathrm{recSeqCart}(7,13,7,4,3,12,7,6)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1)\in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. $\mathrm{rng}\, f\subseteq A$. □

(58) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $(x+1)^3-x^3=y^{\mathbf{2}}\}$ is infinite. The theorem is a consequence of (57).

15. Problem 193

Now we state the propositions:

(59) If i is even, then $i^{\mathbf{2}} \bmod 8=0$ or $i^{\mathbf{2}} \bmod 8=4$.

(60) If i is odd, then $i^{\mathbf{2}} \bmod 8=1$.

(61) (i) $i^{\mathbf{2}} \bmod 8=0$, or

(ii) $i^{\mathbf{2}} \bmod 8=1$, or

(iii) $i^{\mathbf{2}} \bmod 8=4$.

(62) If $p=4\cdot k+3$ and $p \mid i^{\mathbf{2}}+j^{\mathbf{2}}$, then $p\mid i$ and $p\mid j$.

(63) $x^2-y^3\neq 7$. The theorem is a consequence of (59) and (60).

16. Problem 194

Now we state the proposition:

(64) Let us consider an odd natural number c. Then $x^2 - y^3 \neq (2 \cdot c)^3 - 1$. The theorem is a consequence of (60) and (59).

17. Problem 197

Let f, g be positive yielding finite sequences. Let us note that $f \frown g$ is positive yielding. Let x be a positive real number. Let us note that $\langle x \rangle$ is positive yielding. Let x, y be positive real numbers. Let us note that $\langle x, y \rangle$ is positive yielding. Now we state the proposition:

(65) If $n > 0$, then there exists a positive yielding finite sequence f of elements of $\mathbb{N}$ such that $\operatorname{len} f = n$ and $\sum f = \prod f$.

18. Problem 199

Now we state the propositions:

(66) Let us consider positive natural numbers x, y. Suppose $y \cdot (3 \cdot y - 1) = x \cdot (x + 1)$. Then $\operatorname{Polygon}(3, x) = \operatorname{Polygon}(5, y)$.

(67) Let us consider positive natural numbers m, n, and a natural number s. If $\operatorname{Polygon}(s, m) = \operatorname{Polygon}(s, n)$ and $s \geqslant 2$, then $m = n$.

(68) $\{\langle x, y \rangle$, where x, y are positive natural numbers : $y \cdot (3 \cdot y - 1) - x \cdot (x + 1) = 0\}$ is infinite.

Proof: Define $\mathcal{R}(\text{complex number}, \text{complex number}) = \$_2 \cdot (3 \cdot \$_2 - 1) - \$_1 \cdot (\$_1 + 1)$. Set $A = \{\langle x, y \rangle$, where x, y are positive natural numbers : $\mathcal{R}(x, y) = 0\}$. Set $f = \operatorname{recSeqCart}(1, 1, 7, 12, 1, 4, 7, 1)$. Define $\mathcal{N}[\text{natural number}] \equiv f(\$_1) \in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a + 1]$. $\mathcal{N}[a]$. $\operatorname{rng} f \subseteq A$. □

(69) $\{n$, where n is a 3-gonal natural number : n is 5-gonal$\}$ is infinite.

Proof: Set $A = \{n$, where n is a 3-gonal natural number : n is 5-gonal$\}$. Set $B = \{\langle x, y \rangle$, where x, y are positive natural numbers : $y \cdot (3 \cdot y - 1) - x \cdot (x + 1) = 0\}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a positive natural number n such that $n = (\$_1)_{\mathbf{1}}$ and $\$_2 = \operatorname{Polygon}(3, n)$. For every object e such that $e \in B$ there exists an object u such that $\mathcal{P}[e, u]$. Consider f being a function such that $\operatorname{dom} f = B$ and for every object e such that $e \in B$ holds $\mathcal{P}[e, f(e)]$. f is one-to-one. $\operatorname{rng} f \subseteq A$. □

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] 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.

[3] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[4] Artur Korniłowicz. Elementary number theory problems. Part VIII. *Formalized Mathematics*, 31(1):87–100, 2023. doi:10.2478/forma-2023-0009.

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

[6] 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.

[7] Adam Naumowicz. Extending numeric automation for number theory formalizations in Mizar. In Catherine Dubois and Manfred Kerber, editors, *Intelligent Computer Mathematics – 16th International Conference, CICM 2023, Cambridge, UK, September 5–8, 2023, Proceedings*, volume 14101 of *Lecture Notes in Computer Science*, pages 309–314. Springer, 2023. doi:10.1007/978-3-031-42753-4_23.

[8] Marco Riccardi. Solution of cubic and quartic equations. *Formalized Mathematics*, 17(**2**):117–122, 2009. doi:10.2478/v10037-009-0012-z.

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

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

[11] Rafał Ziobro. Prime factorization of sums and differences of two like powers. *Formalized Mathematics*, 24(**3**):187–198, 2016. doi:10.1515/forma-2016-0015.

Accepted November 21, 2023