

Elementary Number Theory Problems. Part IX

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 Waław Sierpiński.

MSC: 11A41 68V20

Keywords: number theory; divisibility; primes; factorization

MML identifier: NUMBER09, version: 8.1.14 5.76.1452

INTRODUCTION

In this paper, problems 62 from Section III, 91, 125 from Section IV, 143, 146, 147, 158, 166, 178, 180, and 181 from Section V of [10] are formalized, using the Mizar formalism [1, 2, 4]. It contributes to the project for the formalization of problems defined in [7].

In the preliminary section, we provide some very technical lemmas, mainly about powers of complex numbers, which are helpful for this and future formalizations. To formulate the statement of Problem 62 the operation `ArProg` introduced in [3] is used. Some useful theorems about primeness of products of elements of finite sequences are proven.

Problem 91 is devoted to decomposing some Mersenne numbers [9] into products of primes or arbitrary integers. For justification of the primeness of `Mersenne(17)` and `Mersenne(19)` we formalized the lemma

$$\forall_{p,q \in \mathbb{P}} p \text{ is odd} \wedge q | \text{Mersenne}(p) \Rightarrow \exists_{k \in \mathbb{N}} q = 2 \cdot k \cdot p + 1.$$

The proof of Problem 143 concerning solutions of the equation $x^2 - Dy^2 = z^2$ in positive integers x, y, z for arbitrary integer D presented in the book has been split into three cases depending on the sign of the parameter D .

The proof of Problem 158 about infiniteness of the number of solutions of the equation $\frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{z} = 1$ in integers x, y, z, t relies on the infiniteness of the range of an injective function with infinite domain, where as the function we use $f : A \rightarrow \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, where A is the set of all integers greater than 1 and for every integer $n > 1$, $f(n) = [-n^2, n^2 \cdot (n^2 - 1), (n^2 - 1)^2, -n \cdot (n^2 - 1)]$.

Problem 166 about representing number $\frac{1}{2}$ as a sum of reciprocals of a finite number of squares of positive integers is formulated as just one example of such decomposition, as

$$\frac{1}{2} = \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{6^2} + \frac{1}{7^2} + \frac{1}{9^2} + \frac{1}{12^2} + \frac{1}{14^2} + \frac{1}{21^2} + \frac{1}{36^2} + \frac{1}{45^2} + \frac{1}{60^2}$$

and its proof is evident to the Mizar verifier due to built-in arithmetic processing.

Problem 180 about solutions (in positive integers) of the equation $y \cdot (y + 1) = x \cdot (x + 1) \cdot (x + 2)$ is formulated as equations $2 \cdot (2 + 1) = 1 \cdot (1 + 1) \cdot (1 + 2)$ and $14 \cdot (14 + 1) = 5 \cdot (5 + 1) \cdot (5 + 2)$ with shapes which mimic the structure of the problem. Its proof is also obvious to the Mizar verifier due to built-in arithmetic processing [8].

The proof of Problem 181 about infiniteness of the number of solutions of the equation $1 + x^2 + y^2 = z^2$ in positive integers x, y, z uses the same technique as we used in the proof of Problem 158 where $f : \mathbb{N}_+ \rightarrow \mathbb{N}_+ \times \mathbb{N}_+ \times \mathbb{N}_+$ such that for every positive integer n , $f(n) = [2 \cdot n, 2 \cdot n^2, 2 \cdot n^2 + 1]$.

1. PRELIMINARIES

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i, j denote integers, r, s denote real numbers, p, p_1, p_2, p_3 denote prime numbers, and z denotes a complex number. Now we state the propositions:

- (1) $z^{11} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$.
- (2) $z^{12} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (1).
- (3) $z^{13} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (2).
- (4) $z^{14} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (3).
- (5) $z^{15} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (4).

- (6) $z^{16} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (5).
- (7) $z^{17} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (6).
- (8) $z^{18} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (7).
- (9) $z^{19} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (8).
- (10) $z^{20} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (9).
- (11) If $n \geq 2$, then there exists a positive natural number k such that $2^n - 1 = 4 \cdot k - 1$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \geq 2$, then there exists a positive natural number k such that $2^{\$1} - 1 = 4 \cdot k - 1$. $\mathcal{P}[2]$. For every natural number j such that $2 \leq j$ holds if $\mathcal{P}[j]$, then $\mathcal{P}[j + 1]$. For every natural number i such that $2 \leq i$ holds $\mathcal{P}[i]$. \square

2. PROBLEM 62

Let X be a set. We say that X is included in a segment if and only if

(Def. 1) there exists a natural number k such that $X \subseteq \text{Seg } k$.

Note that every set which is empty is also included in a segment.

Let n be a non zero natural number. Let us note that $\{n\}$ is included in a segment and there exists a set which is non empty and included in a segment and every set which is included in a segment is also finite and natural-membered and every finite, natural-membered set which has non empty elements is also included in a segment.

Let a, r be natural numbers. Observe that $\text{ArProg}(a, r)$ is natural-valued.

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

(Def. 2) $\{j, \text{ where } j \text{ is an integer : } i \text{ and } j \text{ are relatively prime}\}$.

Now we state the proposition:

- (12) Let us consider an included in a segment set X . If $X \subseteq \mathbb{P}$ and $p \mid \prod \text{Sgm } X$, then $p \in X$.

Let us consider natural numbers a, b and a non zero natural number m . Now we state the propositions:

- (13) Suppose a and b are relatively prime. Then $\prod \text{Sgm}\{p$, where p is a prime number : $p \mid m$ and $p \mid a\}$ and $\prod \text{Sgm}\{q$, where q is a prime number : $q \mid m$ and $q \mid b\}$ are relatively prime. The theorem is a consequence of (12).
- (14) $\prod \text{Sgm}\{p$, where p is a prime number : $p \mid m$ and $p \mid a\}$ and $\prod \text{Sgm}\{r$ where r is a prime number : $r \mid m$ and $r \nmid a$ and $r \nmid b\}$ are relatively prime. The theorem is a consequence of (12).
- (15) Suppose a and b are relatively prime. Then $\prod \text{Sgm}\{q$, where q is a prime number : $q \mid m$ and $q \mid b\}$ and $\prod \text{Sgm}\{r$, where r is a prime number : $r \mid m$ and $r \nmid a$ and $r \nmid b\}$ are relatively prime. The theorem is a consequence of (14).
- (16) Let us consider an included in a segment set X . If $a \in X$, then $a \mid \prod \text{Sgm } X$.
- (17) Let us consider non zero natural numbers a, m . Suppose a and b are relatively prime. Then $\text{rng ArProg}(b, a) \cap \text{Coprimes}(m)$ is infinite.
 PROOF: Set $P_1 = \{p$, where p is a prime number : $p \mid m$ and $p \mid a\}$. Set $R_1 = \{r$, where r is a prime number : $r \mid m$ and $r \nmid a$ and $r \nmid b\}$. Set $P = \prod \text{Sgm } P_1$. Set $R = \prod \text{Sgm } R_1$. $a \cdot P \cdot R + b$ and m are relatively prime. Set $g = \text{ArProg}(b, a)$. Set $X = \text{rng } g \cap \text{Coprimes}(m)$. For every natural number x such that $x \in X$ there exists a natural number y such that $y > x$ and $y \in X$ by [3, (7)], [5, (64)]. \square

3. PROBLEM 91

Let n be a complex number. We say that n is a product of two primes if and only if

(Def. 3) there exist prime numbers p_1, p_2 such that $n = p_1 \cdot p_2$.

We introduce the notation n is not a product of two primes as an antonym for n is a product of two primes.

One can check that every prime number is not a product of two primes. Let us consider p_1 and p_2 . One can verify that $p_1 \cdot p_2$ is a product of two primes. Now we state the propositions:

- (18) If $a \neq 1$ and $a \neq n$ and a is not prime and $a \mid n$, then n is not a product of two primes.
- (19) If n is a product of two primes, then $n \geq 4$.
- (20) If c is a product of two different primes, then c is a product of two primes.

Let us consider p_1, p_2 , and p_3 . One can check that $p_1 \cdot p_2 \cdot p_3$ is not a product of two primes. Now we state the propositions:

(21) If n is a product of two primes, then for every a and b such that $a \neq 1$ and $b \neq 1$ and $n = a \cdot b$ holds a is prime and b is prime.

(22) If $2^n - 1$ is prime and $2^n + 1$ is prime, then $n = 2$.

Let n be a zero natural number. Note that M_n is zero. Let n be a non zero natural number. Let us note that M_n is odd. Now we state the propositions:

(23) Let us consider prime numbers p, q . Suppose p is odd and $q \mid M_p$. Then there exists a natural number k such that $q = 2 \cdot k \cdot p + 1$.

(24) M_{17} is prime. The theorem is a consequence of (23).

(25) M_{19} is prime. The theorem is a consequence of (23).

(26) $\{2^n - 1, \text{ where } n \text{ is a natural number} : 2^n - 1 \leq 10^6 \text{ and } 2^n - 1 \text{ is a product of two primes}\} = \{2^4 - 1, 2^9 - 1, 2^{11} - 1\}$.

PROOF: Set $A = \{2^n - 1 : 2^n - 1 \leq 10^6 \text{ and } 2^n - 1 \text{ is a product of two primes}\}$. Set $B = \{2^4 - 1, 2^9 - 1, 2^{11} - 1\}$. $A \subseteq B$ by [6, (7)], (9). $B \subseteq A$.

□

Let us consider n . We say that n has at least three different divisors if and only if

(Def. 4) there exist natural numbers q_1, q_2, q_3 such that q_1, q_2, q_3 are mutually different and $q_1 > 1$ and $q_2 > 1$ and $q_3 > 1$ and $q_1 \mid n$ and $q_2 \mid n$ and $q_3 \mid n$.

Observe that every natural number which has more than two different prime divisors has also at least three different divisors and every natural number which has more than two different prime divisors is also not a product of two primes.

Now we state the propositions:

(27) If n has more than two different prime divisors, then n is not a product of two different primes.

(28) If n is even and $n > 4$, then $2^n - 1$ has at least three different divisors. The theorem is a consequence of (22).

4. PROBLEM 125

Now we state the propositions:

(29) If Fermat $m =$ Fermat n , then $m = n$.

(30) If $m < n$, then Fermat $m <$ Fermat n .

(31) If $m \leq n$, then Fermat $m \leq$ Fermat n . The theorem is a consequence of (30).

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

(33) $i \cdot n \equiv n \pmod{n}$.

(34) If $a \mid m^k + 1$, then $a \mid (a \cdot n + m)^k + 1$.

- (35) $17 \mid (34 \cdot k + 2)^{2^2} + 1$. The theorem is a consequence of (34).
- (36) $17 \mid (34 \cdot k + 4)^{2^1} + 1$. The theorem is a consequence of (34).
- (37) $17 \mid (34 \cdot k + 6)^{2^3} + 1$. The theorem is a consequence of (34).
- (38) $17 \mid (34 \cdot k + 8)^{2^2} + 1$. The theorem is a consequence of (34).
- (39) $17 \mid (34 \cdot k + 10)^{2^3} + 1$. The theorem is a consequence of (34).
- (40) $17 \mid (34 \cdot k + 12)^{2^3} + 1$. The theorem is a consequence of (34).
- (41) $17 \mid (34 \cdot k + 14)^{2^3} + 1$. The theorem is a consequence of (34).
- (42) $17 \mid (34 \cdot k + 20)^{2^3} + 1$. The theorem is a consequence of (34).
- (43) $17 \mid (34 \cdot k + 22)^{2^3} + 1$. The theorem is a consequence of (34).
- (44) $17 \mid (34 \cdot k + 24)^{2^3} + 1$. The theorem is a consequence of (34).
- (45) $17 \mid (34 \cdot k + 26)^{2^2} + 1$. The theorem is a consequence of (34).
- (46) $17 \mid (34 \cdot k + 28)^{2^3} + 1$. The theorem is a consequence of (34).
- (47) $17 \mid (34 \cdot k + 30)^{2^1} + 1$. The theorem is a consequence of (34).
- (48) $17 \mid (34 \cdot k + 32)^{2^2} + 1$. The theorem is a consequence of (34).
- (49) If $1 < a \leq 100$, then there exists a positive natural number n such that $n \leq 6$ and $a^{2^n} + 1$ is composite. The theorem is a consequence of (37), (38), (39), (40), (41), (42), (43), (44), (45), (46), (47), (48), (35), and (36).

5. PROBLEM 143

Now we state the proposition:

- (50) Let us consider an integer D . Then $\{\langle x, y, z \rangle, \text{ where } x, y, z \text{ are positive natural numbers : } x^2 - D \cdot y^2 = z^2\}$ is infinite.

6. PROBLEM 146

Now we state the propositions:

- (51) (i) $n^2 \bmod 8 = 0$, or
 (ii) $n^2 \bmod 8 = 1$, or
 (iii) $n^2 \bmod 8 = 4$.
- (52) Let us consider natural numbers x, y, z . Then $x^2 - 2 \cdot y^2 + 8 \cdot z \neq 3$. The theorem is a consequence of (51).

7. PROBLEM 147

Now we state the proposition:

$$(53) \quad \{\langle x, y \rangle, \text{ where } x, y \text{ are natural numbers : } y^2 - x \cdot (x+1) \cdot (x+2) \cdot (x+3) = 1\} = \{\langle x, y \rangle, \text{ where } x, y \text{ are natural numbers : } y = x^2 + 3 \cdot x + 1\}.$$

PROOF: Set $A = \{\langle x, y \rangle, \text{ where } x, y \text{ are natural numbers : } y^2 - x \cdot (x+1) \cdot (x+2) \cdot (x+3) = 1\}$. Set $B = \{\langle x, y \rangle, \text{ where } x, y \text{ are natural numbers : } y = x^2 + 3 \cdot x + 1\}$. $A \subseteq B$. Consider x, y being natural numbers such that $a = \langle x, y \rangle$ and $y = x^2 + 3 \cdot x + 1$. \square

8. PROBLEM 158

Now we state the propositions:

$$(54) \quad \text{Let us consider positive real numbers } a, b, c, d. \text{ If } \frac{a}{b} < 1 \text{ and } \frac{c}{d} < 1, \text{ then } \frac{a}{b} \cdot \frac{c}{d} < 1.$$

$$(55) \quad \text{Let us consider positive natural numbers } x, y, z, t. \text{ Then } \frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} \neq 1. \\ \text{The theorem is a consequence of (54).}$$

Let n be a natural number. The functor $\langle n, \infty \rangle_{\mathbb{N}}$ yielding a subset of \mathbb{N} is defined by the term

$$(\text{Def. 5}) \quad \mathbb{N} \setminus (\mathbb{Z}_n).$$

Let us consider n . One can check that $\langle n, \infty \rangle_{\mathbb{N}}$ is infinite. Now we state the propositions:

$$(56) \quad k \in \langle n, \infty \rangle_{\mathbb{N}} \text{ if and only if } n \leq k.$$

PROOF: If $k \in \langle n, \infty \rangle_{\mathbb{N}}$, then $n \leq k$. \square

$$(57) \quad n + k \in \langle n, \infty \rangle_{\mathbb{N}}.$$

$$(58) \quad n \in \langle n, \infty \rangle_{\mathbb{N}}.$$

$$(59) \quad \text{If } k > 0, \text{ then } n \notin \langle n + k, \infty \rangle_{\mathbb{N}}. \text{ The theorem is a consequence of (56).}$$

Let us consider n . Let us note that every element of $\langle n, \infty \rangle_{\mathbb{N}}$ is n or greater and there exists a natural number which is n or greater. Now we state the proposition:

$$(60) \quad \text{Let us consider an } n \text{ or greater natural number } k. \text{ Then } k \in \langle n, \infty \rangle_{\mathbb{N}}.$$

Let us consider n . Let k be a non zero natural number. Observe that $k \cdot n$ is n or greater. Let k be an n or greater natural number. One can verify that $k - n$ is natural. Now we state the proposition:

$$(61) \quad \{\langle x, y, z, t \rangle, \text{ where } x, y, z, t \text{ are integers : } \frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} = 1\} \text{ is infinite.}$$

PROOF: Set $G_2 = \langle 2, \infty \rangle_{\mathbb{N}}$. Set $A = \{\langle x, y, z, t \rangle, \text{ where } x, y, z, t \text{ are integers : } \frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} = 1\}$. Define $\mathcal{V}(\text{natural number}) = -\1^2 . Define $\mathcal{Y}(\text{natural$

number) = $\$1^2 \cdot (\$1^2 - 1)$. Define $\mathcal{Z}(\text{natural number}) = (\$1^2 - 1)^2$. Define $\mathcal{T}(\text{natural number}) = -\$1 \cdot (\$1^2 - 1)$. Define $\mathcal{F}(\text{element of } G_2) = \langle \mathcal{V}(\$1), \mathcal{Y}(\$1), \mathcal{Z}(\$1), \mathcal{T}(\$1) \rangle$. Consider f being a many sorted set indexed by G_2 such that for every element d of G_2 , $f(d) = \mathcal{F}(d)$. $\text{rng } f \subseteq A$. f is one-to-one. \square

9. PROBLEM 166

Now we state the proposition:

$$(62) \quad \frac{1}{2} = \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{6^2} + \frac{1}{7^2} + \frac{1}{9^2} + \frac{1}{12^2} + \frac{1}{14^2} + \frac{1}{21^2} + \frac{1}{36^2} + \frac{1}{45^2} + \frac{1}{60^2}.$$

10. PROBLEM 178

Now we state the proposition:

$$(63) \quad (n+1)^3 + (n+2)^3 + (n+3)^3 + (n+4)^3 \neq (n+5)^3.$$

11. PROBLEM 180

Now we state the proposition:

$$(64) \quad \begin{aligned} \text{(i)} \quad & 2 \cdot (2+1) = 1 \cdot (1+1) \cdot (1+2), \text{ and} \\ \text{(ii)} \quad & 14 \cdot (14+1) = 5 \cdot (5+1) \cdot (5+2). \end{aligned}$$

12. PROBLEM 181

Now we state the proposition:

$$(65) \quad \{ \langle x, y, z \rangle, \text{ where } x, y, z \text{ are positive natural numbers : } 1 + x^2 + y^2 = z^2 \}$$

is infinite.

PROOF: Set $A = \{ \langle x, y, z \rangle, \text{ where } x, y, z \text{ are positive natural numbers : } 1 + x^2 + y^2 = z^2 \}$. Define $\mathcal{V}(\text{natural number}) = 2 \cdot \1 . Define $\mathcal{Y}(\text{natural number}) = 2 \cdot \1^2 . Define $\mathcal{Z}(\text{natural number}) = 2 \cdot \$1^2 + 1$. Define $\mathcal{F}(\text{natural number}) = \langle \mathcal{V}(\$1), \mathcal{Y}(\$1), \mathcal{Z}(\$1) \rangle$. Consider f being a many sorted set indexed by \mathbb{N}_+ such that for every element d of \mathbb{N}_+ , $f(d) = \mathcal{F}(d)$. $\text{rng } f \subseteq A$. f is one-to-one. \square

REFERENCES

- [1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, 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 Kornilowicz, 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] Adam Grabowski. Elementary number theory problems. Part VI. *Formalized Mathematics*, 30(3):235–244, 2022. doi:10.2478/forma-2022-0019.
- [4] Artur Kornilowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.
- [5] Artur Kornilowicz. Elementary number theory problems. Part IV. *Formalized Mathematics*, 30(3):223–228, 2022. doi:10.2478/forma-2022-0017.
- [6] Artur Kornilowicz and Dariusz Surowik. Elementary number theory problems. Part II. *Formalized Mathematics*, 29(1):63–68, 2021. doi:10.2478/forma-2021-0006.
- [7] 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.
- [8] 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.
- [9] Waclaw Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.
- [10] Waclaw Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

Accepted November 21, 2023
