FORMALIZED MATHEMATICS
Vol. 32, No. 1, pp. 91–109, 2024
DOI: 10.2478/forma-2024-0007
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part XV – Diophantine Equations

Karol Pąk
Faculty of Computer Science
University of Białystok
Poland

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

Summary. This paper formalizes problems 38, 58, 160, 164, 168, 171, 188, 195, 196, and 198 from "250 Problems in Elementary Number Theory" by Wacław Sierpiński [17].

MSC: 68V20

Keywords: number theory; prime number; Diophantine equation

MML identifier: NUMBER15, version: 8.1.14 5.82.1469

Introduction

In this paper, Problems 38 from Section I, 58 from Section III, 160, 164, 168, 171, 188, 195, 196, and 198 from Section V of [17] are formalized, using the Mizar formalism [6, 5]. The paper is a part of the project *Formalization of Elementary Number Theory in Mizar* [14].

In the preliminary section, we provided some valuable facts about the monotonicity of functions.

Problem 38 concerns a comparison between the number of divisors of the form $4k + 1$ and the number of divisors of the form $4k + 3$ for a given positive integer. We demonstrate that the number of divisors of the form $4k+1$ is greater than or equal to that of the form $4k+3$. Furthermore, we show that there are an infinite number of cases where equality is observed, as well as instances where the former is greater. To prove the last two problems, we utilize the families

of numbers indicated in the book, for which we prove that they are infinite. The original proof is inductive with respect to the number of prime numbers of the form $4k+3$ in the decomposition into prime numbers in first powers. In the induction step, we encountered an obstacle. For illustrative purposes, let us consider the case of $n = 3 \cdot 3 \cdot 3$, which has $s+1 = 3$ divisors of the form $4k+3$. Then the only distribution $n = m \cdot q$ where m has s divisors of the form $4k+3$ is for $m = 3^2$, $q = 3$. We define g to be the number of divisors in the form $4k+1$ of m (3^0, 3^2), and h to be the number of divisors in the form $4k+3$ of n (3^1,3^3). Then $m \cdot q$ should have $g+h$ divisors of the form $4k+1$ but has only 2: 3^0, 3^2. We have also noticed that this property only occurs if m and q are coprime.

To solve this problem we considered our proof, which uses the idea proposed in the book. First, we prove that for any prime number p to a power other than zero n holds $(p^n)_{4k+1} \geqslant (p^n)_{4k+3}$ where $(p^n)_{4k+1}$ and $(p^n)_{4k+3}$ are the numbers of p^n divisors of the form $4k+1$ and $4k+3$, respectively. Then, we consider induction with respect to the number of distinct prime factors that appear with non-zero exponents in the prime factorization. Let $n = \prod_{i=1}^{s+1} p_i^{n_i}$ where $p_1 < p_2 < \ldots < p_{s+1}$ are primes and the n_i are positive integers. Set $m = \prod_{i=1}^{s} p_i^{n_i}$, $q = p_{s+1}^{n_{s+1}}$. From what has been proven before, we have $(q)_{4k+1} \geqslant (q)_{4k+3}$ and $(m)_{4k+1} \geqslant (m)_{4k+3}$ by induction, which gives $((m)_{4k+1} - (m)_{4k+3}) \cdot ((q)_{4k+1} - (q)_{4k+3}) \geqslant 0$ and consequently:

$$(m)_{4k+1} \cdot (q)_{4k+1} + (m)_{4k+3} \cdot (q)_{4k+3} \geqslant (m)_{4k+1} \cdot (q)_{4k+3} + (m)_{4k+3} \cdot (q)_{4k+1} \quad \text{(I.1)}$$

The proof is completed by showing that $(n)_{4k+1} = (m)_{4k+1} \cdot (q)_{4k+1} + (m)_{4k+3} \cdot (q)_{4k+3}$, $(n)_{4k+3} = (m)_{4k+1} \cdot (q)_{4k+3} + (m)_{4k+3} \cdot (q)_{4k+1}$ and that it holds since m, q are coprime.

Problem 58 asks about the existence of arbitrarily long arithmetic progression formed of different positive integers, whose terms are powers of positive integers with integer exponents greater than 1. Such terms are named `perfect_powers` [10]. The proof of the problem considers only progressions with positive lengths, while we generalized the proof to arbitrary length s, where the solution for $s = 0$ is the empty finite sequence.

It is worth mentioning that we found two errors (just misprints) in the proof of Problem 58. The formula for numbers Q_k should be

$$Q_k = k^{(a_k+1)/p_k} \prod_{\substack{n=1 \\ n \neq k}}^{s} n^{a_n/p_k}$$

that is one should consider numbers n^{a_n/p_k}, but not n^{a_k/p_k} in the $\prod$. Moreover, in the book it is written "$p_k | a_n$ if $k \neq n$, where n is a positive integer >

s", while n must be $\leqslant s$ – it is reflected in the defintion of a finite sequence `sequenceAnPk(s,k)`.

Problem 160 requires finding all solutions in positive integers x, y, z, t, with $x \leqslant y \leqslant z \leqslant t$ of the equation

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{t}=1.$$

The proof given in the book presents 14 different solutions of the equation, but one of them $x=2$, $y=4$, $z=5$, $t=24$ is incorrect $\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{5}+\frac{1}{24}=\frac{119}{120}\neq 1\right)$. It should be $x=2$, $y=4$, $z=5$, and $t=20$.

Problem 168 concerns proving that for every positive integer s, the equation

$$\frac{1}{x_1^2}+\frac{1}{x_2^2}+\cdots+\frac{1}{x_s^2}=\frac{1}{x_{s+1}^2}$$

has infinitely many solutions in positive integers $x_1, x_2, \ldots, x_s, x_{s+1}$. The original proof is splited into several cases – but the case for $s=2$ provides a wrong solution $\frac{1}{15^2}+\frac{1}{12^2}=\frac{1}{20^2}$. It should be $\frac{1}{15^2}+\frac{1}{20^2}=\frac{1}{12^2}$.

Problem 196 asks to solve the problem of A. Moessner of finding all solutions in positive integers x, y, z, t of the system of equations

$$x+y=zt, z+t=xy$$

where $x \leqslant y$ and $x \leqslant z \leqslant t$ and to prove that this system has infinitely many integer solutions x, y, z, and t. The proof in the book is divided into several cases. The case for $x>2$ is slightly imprecise. It claims that $z_1t_1+2z_1+2t_1+4 \geqslant z_1+t_1+9$, for $z_1=z-2$, and $t_1=t-2$, but we could prove only inequality $z_1t_1+2z_1+2t_1+4 \geqslant z_1+t_1+7$. Anyway, our restriction could be used to complete the proof.

The proofs for the other problems are direct formalizations of the solutions presented in the book.

1. Preliminaries

From now on a, b, k, m, n, s denote natural numbers, c, c_1, c_2, c_3 denote complex numbers, i, j, z denote integers, p denotes a prime number, and x denotes an object.

Let p be a prime number. One can check that $p(\in \mathbb{P})$ reduces to p.

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

Let us consider n. One can check that there exists a finite sequence which is positive yielding, natural-valued, and n-elements and every binary relation which is non-empty and natural-valued is also positive yielding.

Let D be a set and f be a D-valued finite 0-sequence. One can verify that XFS2FS(f) is D-valued.

Now we state the proposition:

(1) Let us consider a finite 0-sequence f. If $n \in \operatorname{dom}(\text{XFS2FS}(f))$, then $n - 1 \in \operatorname{dom} f$.

Let f be an increasing, extended real-valued finite 0-sequence. One can check that XFS2FS(f) is increasing.

Let f be a decreasing, extended real-valued finite 0-sequence. Let us observe that XFS2FS(f) is decreasing.

Let f be a non-increasing, extended real-valued finite 0-sequence. Let us note that XFS2FS(f) is non-increasing.

Let f be a non-decreasing, extended real-valued finite 0-sequence. One can check that XFS2FS(f) is non-decreasing.

Let r be a positive real number and f be a positive yielding, real-valued function. One can verify that $r \cdot f$ is positive yielding.

Let f be an increasing, real-valued function. Note that $r \cdot f$ is increasing.

Let r be a negative real number. Note that $r \cdot f$ is decreasing.

Let r be a positive real number and f be a decreasing, real-valued function. Let us observe that $r \cdot f$ is decreasing.

Let r be a negative real number. Let us observe that $r \cdot f$ is increasing.

Let r be a positive real number and f be a non-increasing, real-valued function. Note that $r \cdot f$ is non-increasing.

Let r be a negative real number. Note that $r \cdot f$ is non-decreasing.

Let r be a positive real number and f be a non-decreasing, real-valued function. Let us observe that $r \cdot f$ is non-decreasing.

Let r be a negative real number. Let us observe that $r \cdot f$ is non-increasing.

Now we state the proposition:

(2) Let us consider a finite-support function f. Then $\operatorname{rng} f \subseteq \operatorname{rng}(f \restriction \operatorname{support} f) \cup \{0\}$.

Let f be a finite-support function. Let us observe that $\operatorname{rng} f$ is finite.

Now we state the propositions:

(3) Let us consider a complex-valued finite sequence f, and a finite sequence g of elements of $\mathbb{C}_{\mathrm{F}}$. If $f = g$, then $\prod f = \prod g$.

(4) Let us consider a complex number a, and complex-valued finite sequences p, q. Suppose $\operatorname{len} p = \operatorname{len} q$ and there exists a natural number i such that $i \in \operatorname{dom} p$ and $q(i) = a \cdot p(i)$ and for every natural number j such that $j \in \operatorname{dom} p$ and $i \neq j$ holds $q(j) = p(j)$. Then $\prod q = a \cdot (\prod p)$. The theorem is a consequence of (3).

2. PROBLEM 38

Now we state the propositions:

(5) If $n \bmod 4 = 0$ or $n \bmod 4 = 2$, then $n \cdot m \bmod 4 = 0$ or $n \cdot m \bmod 4 = 2$.

(6) If $n \cdot m \bmod 4 = 1$, then $n \bmod 4 = 1$ or $n \bmod 4 = 3$. The theorem is a consequence of (5).

(7) If $n \cdot m \bmod 4 = 3$, then $n \bmod 4 = 1$ and $m \bmod 4 = 3$ or $n \bmod 4 = 3$ and $m \bmod 4 = 1$. The theorem is a consequence of (5).

(8) If $n \bmod 4 = 1$ and $m \bmod 4 = 1$ or $n \bmod 4 = 3$ and $m \bmod 4 = 3$, then $n \cdot m \bmod 4 = 1$.

(9) If $n \bmod 4 = 1$ and $m \bmod 4 = 3$ or $n \bmod 4 = 3$ and $m \bmod 4 = 1$, then $n \cdot m \bmod 4 = 3$.

(10) If p is prime and $p \bmod 4 = 1$ and $n \mid p^k$, then $n \bmod 4 = 1$.
PROOF: Consider t being an element of $\mathbb{N}$ such that $n = p^t$ and $t \leqslant k$. Define $\mathcal{P}[\text{natural number}] \equiv p^{\$_1} \bmod 4 = 1$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by (8), [12, (6)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(11) If $p \bmod 4 = 3$, then $p^{2 \cdot n} \bmod 4 = 1$ and $p^{2 \cdot n+1} \bmod 4 = 3$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv p^{2 \cdot \$_1} \bmod 4 = 1$ and $p^{2 \cdot \$_1+1} \bmod 4 = 3$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [12, (6)], (8), (9). For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

Let n, m, r be integers. The functor divisors(n, m, r) yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 1) $\{k,$ where k is a natural number : $k \bmod m = r$ and $k \mid n\}$.

Now we state the proposition:

(12) Let us consider integers n, m, r. Then $k \in \operatorname{divisors}(n, m, r)$ if and only if $k \bmod m = r$ and $k \mid n$.

Let n be a positive natural number and m, r be integers. Note that $\operatorname{divisors}(n, m, r)$ is finite.

Now we state the propositions:

(13) Let us consider integers n, m, r, p. Then $k \in \mathrm{divisors}(n, m, r) \cup \mathrm{divisors}(n, m, p)$ if and only if ($k \bmod m = r$ or $k \bmod m = p$) and $k \mid n$. The theorem is a consequence of (12).

(14) Let us consider integers n, m, r. If $k \neq i$, then $\mathrm{divisors}(n, m, k)$ misses $\mathrm{divisors}(n, m, i)$. The theorem is a consequence of (12).

(15) (i) $\mathrm{divisors}(2^n, 4, 3) = \emptyset$, and

(ii) $\mathrm{divisors}(2^n, 4, 1) = \{1\}$.

Proof: $\mathrm{divisors}(2^n, 4, 3) = \emptyset$ by (12), [9, (5)]. $\mathrm{divisors}(2^n, 4, 1) \subseteq \{1\}$. □

Let us consider a prime number p and a natural number n. Now we state the propositions:

(16) $\overline{\overline{\{k, \text{ where } k \text{ is a natural number} : k \mid p^n\}}} = n + 1$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{\{k, \text{ where } k \text{ is a natural number} : k \mid p^{\$_1}\}}} = \$_1 + 1$. Set $X = \{k, \text{ where } k \text{ is a natural number} : k \mid p^0\}$. $X \subseteq \{1\}$ by [13, (13)]. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$ by [2, (41)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(17) Suppose $p \bmod 4 = 1$. Then

(i) $\overline{\overline{\mathrm{divisors}(p^n, 4, 1)}} = n + 1$, and

(ii) $\overline{\overline{\mathrm{divisors}(p^n, 4, 3)}} = 0$.

The theorem is a consequence of (10) and (16).

Now we state the propositions:

(18) Let us consider a prime number p, m, and n. Suppose $p \bmod 4 = 3$. Then

(i) $\mathrm{divisors}(p^n, 4, 1) \cup \mathrm{divisors}(p^n, 4, 3) = \{k, \text{ where } k \text{ is a natural number} : k \mid p^n\}$, and

(ii) if $n = 2 \cdot m$, then $\overline{\overline{\mathrm{divisors}(p^n, 4, 1)}} = m+1$ and $\overline{\overline{\mathrm{divisors}(p^n, 4, 3)}} = m$, and

(iii) if $n = 2 \cdot m+1$, then $\overline{\overline{\mathrm{divisors}(p^n, 4, 1)}} = m+1$ and $\overline{\overline{\mathrm{divisors}(p^n, 4, 3)}} = m + 1$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every m, $\mathrm{divisors}(p^{\$_1}, 4, 1) \cup \mathrm{divisors}(p^{\$_1}, 4, 3) = \{k, \text{ where } k \text{ is a natural number} : k \mid p^{\$_1}\}$ and if $\$_1 = 2 \cdot m$, then $\overline{\overline{\mathrm{divisors}(p^{\$_1}, 4, 1)}} = m+1$ and $\overline{\overline{\mathrm{divisors}(p^{\$_1}, 4, 3)}} = m$ and if $\$_1 = 2 \cdot m + 1$, then $\overline{\overline{\mathrm{divisors}(p^{\$_1}, 4, 1)}} = m + 1$ and $\overline{\overline{\mathrm{divisors}(p^{\$_1}, 4, 3)}} = m + 1$. $\mathcal{P}[0]$ by [12, (4)], [9, (5)], [13, (13)], [7, (33)]. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$ by [21, (36)], [16, (9)], (11), [12, (6)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(19) If p is prime, then $p = 2$ or $p \bmod 4 = 1$ or $p \bmod 4 = 3$.

(20) If $n > 1$, then there exists a prime number p such that $p \mid n$ and for every prime number q such that $q \mid n$ holds $q \leqslant p$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ \$1 is prime and \$1 $\mid n$. Consider k being a natural number such that $\mathcal{P}[k]$ and for every natural number n such that $\mathcal{P}[n]$ holds $n \leqslant k$ from [3, Sch. 6]. □

(21) Suppose n is positive and p is prime and $p \mid n$. Then there exist positive natural numbers k, m such that
(i) $0 < k$, and
(ii) $n = m \cdot p^k$, and
(iii) m and p are relatively prime.
PROOF: Consider u being a positive natural number such that $n \leqslant p^u$. Define $\mathcal{P}$[natural number] $\equiv p^{\$1} \mid n$. For every natural number k such that $\mathcal{P}[k]$ holds $k \leqslant u$ by [15, (93)], [9, (30)]. Consider k being a natural number such that $\mathcal{P}[k]$ and for every natural number n such that $\mathcal{P}[n]$ holds $n \leqslant k$ from [3, Sch. 6]. Consider m being a natural number such that $n = p^k \cdot m$. Consider m_1 being a natural number such that $m = p \cdot m_1$. □

(22) Let us consider a non zero natural number n. Then $\overline{\overline{\text{divisors}(n, 4, 3)}} \leqslant \overline{\overline{\text{divisors}(n, 4, 1)}}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non zero natural number n such that for every prime number p such that $p \mid n$ holds $p \leqslant$ \$1 holds $\overline{\overline{\text{divisors}(n, 4, 3)}} \leqslant \overline{\overline{\text{divisors}(n, 4, 1)}}$. For every natural number k such that for every natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [12, (4)], [13, (28)], [3, (9)], (20). For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 4]. □

(23) If m is even, then $3^m \bmod 4 = 1$.

(24) If m is odd, then $3^m \bmod 4 = 3$.

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

(25) $\text{divisors}(3^{2 \cdot n+1}, 4, 1) = \{3^m : m \text{ is even and } m \leqslant 2 \cdot n + 1\}$.
PROOF: Set $A = \text{divisors}(3^{2 \cdot n+1}, 4, 1)$. Set $B = \{3^m : m \text{ is even and } m \leqslant 2 \cdot n + 1\}$. $A \subseteq B$ by [9, (34), (41)], (24). Consider m such that $x = 3^m$ and m is even and $m \leqslant 2 \cdot n + 1$. $3^m \bmod 4 = 1$. □

(26) $\text{divisors}(3^{2 \cdot n+1}, 4, 3) = \{3^m$, where m is a natural number : m is odd and $m \leqslant 2 \cdot n + 1\}$.
PROOF: Set $A = \text{divisors}(3^{2 \cdot n+1}, 4, 3)$. Set $B = \{3^m$, where m is a natural number : m is odd and $m \leqslant 2 \cdot n + 1\}$. $A \subseteq B$ by [9, (34), (41)], (23). Consider m such that $x = 3^m$ and m is odd and $m \leqslant 2 \cdot n + 1$. $3^m \bmod 4 = 3$. □

Now we state the propositions:

(27) $\overline{\overline{\{3^m, \text{where } m \text{ is a natural number} : m \text{ is even and } m \leqslant 2 \cdot n + 1\}}} = n + 1$.

PROOF: Define $\mathcal{F}(\text{natural number}) = 3^{\$_1}$. Define $\mathcal{A}(\text{natural number}) = \{\mathcal{F}(m), \text{where } m \text{ is a natural number} : m \text{ is even and } m \leqslant 2 \cdot \$_1 + 1\}$. Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{\mathcal{A}(\$_1)}} = \$_1 + 1$. $\mathcal{P}[0]$ by [3, (25)], [1, (30)]. If $\mathcal{P}[a]$, then $\mathcal{P}[a+1]$ by [3, (16)], [9, (30)], [3, (13), (62)]. $\mathcal{P}[a]$ from [3, Sch. 2]. □

(28) $\overline{\overline{\{3^m, \text{where } m \text{ is a natural number} : m \text{ is odd and } m \leqslant 2 \cdot n + 1\}}} = n + 1$.

PROOF: Define $\mathcal{F}(\text{natural number}) = 3^{\$_1}$. Define $\mathcal{A}(\text{natural number}) = \{\mathcal{F}(m), \text{where } m \text{ is a natural number} : m \text{ is odd and } m \leqslant 2 \cdot \$_1 + 1\}$. Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{\mathcal{A}(\$_1)}} = \$_1 + 1$. $\mathcal{P}[0]$ by [3, (25)], [1, (30)]. If $\mathcal{P}[a]$, then $\mathcal{P}[a+1]$ by [3, (16)], [9, (30)], [3, (13), (62)]. $\mathcal{P}[a]$ from [3, Sch. 2]. □

(29) $\overline{\overline{\text{divisors}(3^{2 \cdot n+1}, 4, 1)}} = n + 1$. The theorem is a consequence of (25) and (27).

(30) $\overline{\overline{\text{divisors}(3^{2 \cdot n+1}, 4, 3)}} = n + 1$. The theorem is a consequence of (26) and (28).

(31) $\overline{\overline{\text{divisors}(3^{2 \cdot n+1}, 4, 1)}} = \overline{\overline{\text{divisors}(3^{2 \cdot n+1}, 4, 3)}}$. The theorem is a consequence of (25), (26), (27), and (28).

(32) $\{n, \text{where } n \text{ is a natural number} : \overline{\overline{\text{divisors}(3^{2 \cdot n+1}, 4, 1)}} = \overline{\overline{\text{divisors}(3^{2 \cdot n+1}, 4, 3)}}\}$ is infinite.

PROOF: Define $\mathcal{A}(\text{natural number}) = \text{divisors}(3^{2 \cdot \$_1 + 1}, 4, 1)$. Define $\mathcal{B}(\text{natural number}) = \text{divisors}(3^{2 \cdot \$_1 + 1}, 4, 3)$. Set $X = \{n, \text{where } n \text{ is a natural number} : \overline{\overline{\mathcal{A}(n)}} = \overline{\overline{\mathcal{B}(n)}}\}$. $\overline{\overline{\mathcal{A}(0)}} = \overline{\overline{\mathcal{B}(0)}}$. X is natural-membered. For every a such that $a \in X$ there exists a natural number b such that $b > a$ and $b \in X$ by [3, (16)], (31). □

(33) $\{n, \text{where } n \text{ is a natural number} : \overline{\overline{\text{divisors}(n, 4, 1)}} = \overline{\overline{\text{divisors}(n, 4, 3)}}\}$ is infinite.

PROOF: Define $\mathcal{A}(\text{natural number}) = \text{divisors}(\$_1, 4, 1)$. Define $\mathcal{B}(\text{natural number}) = \text{divisors}(\$_1, 4, 3)$. Set $X = \{n, \text{where } n \text{ is a natural number} : \overline{\overline{\mathcal{A}(n)}} = \overline{\overline{\mathcal{B}(n)}}\}$. Set $n = 3^{2 \cdot 0 + 1}$. $\overline{\overline{\mathcal{A}(n)}} = 1$. $\overline{\overline{\mathcal{B}(n)}} = 1$. X is natural-membered. For every a such that $a \in X$ there exists a natural number b such that $b > a$ and $b \in X$ by [12, (86)], (29), (30). □

(34) If $k \mid 5^n$, then $k \bmod 4 = 1$.

(35) There exists no k such that $k \bmod 4 = 3$ and $k \mid 5^n$.

(36) $\{k, \text{where } k \text{ is a natural number} : k \mid 5^n\} = \text{divisors}(5^n, 4, 1)$. The the-

orem is a consequence of (34).

(37) $\overline{\overline{\{k,\text{ where } k \text{ is a natural number} : k \mid 5^n\}}} = n+1$.

PROOF: Define $\mathcal{F}(\text{natural number}) = 5^{\$_1}$. Define $\mathcal{A}(\text{natural number}) = \{m, \text{where } m \text{ is a natural number} : m \mid \mathcal{F}(\$_1)\}$. Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{\mathcal{A}(\$_1)}} = \$_1 + 1$. $\mathcal{P}[0]$ by (34), [3, (25)], [1, (30)]. If $\mathcal{P}[a]$, then $\mathcal{P}[a+1]$ by [3, (16)], [9, (66), (34), (59)]. $\mathcal{P}[a]$ from [3, Sch. 2]. □

(38) $\text{divisors}(5^n, 4, 3) = \emptyset$. The theorem is a consequence of (34).

(39) $\{n, \text{where } n \text{ is a natural number} : \overline{\overline{\text{divisors}(5^n, 4, 1)}} > \overline{\overline{\text{divisors}(5^n, 4, 3)}}\}$ is infinite.

PROOF: Define $\mathcal{A}(\text{natural number}) = \text{divisors}(5^{\$_1}, 4, 1)$. Define $\mathcal{B}(\text{natural number}) = \text{divisors}(5^{\$_1}, 4, 3)$. Set $X = \{n, \text{where } n \text{ is a natural number} : \overline{\overline{\mathcal{A}(n)}} > \overline{\overline{\mathcal{B}(n)}}\}$. $\{k, \text{where } k \text{ is a natural number} : k \mid 5^0\} = \mathcal{A}(0)$. $\overline{\overline{\mathcal{A}(0)}} = 0+1$. $\overline{\overline{\mathcal{A}(0)}} > \overline{\overline{\mathcal{B}(0)}}$. X is natural-membered. For every a such that $a \in X$ there exists a natural number b such that $b > a$ and $b \in X$ by [3, (16)], (37), (36), (38). □

(40) $\{n, \text{where } n \text{ is a positive natural number} : \overline{\overline{\text{divisors}(n, 4, 1)}} > \overline{\overline{\text{divisors}(n, 4, 3)}}\}$ is infinite.

PROOF: Define $\mathcal{A}(\text{positive natural number}) = \text{divisors}(\$_1, 4, 1)$. Define $\mathcal{B}(\text{positive natural number}) = \text{divisors}(\$_1, 4, 3)$. Set $X = \{n, \text{where } n \text{ is a positive natural number} : \overline{\overline{\mathcal{A}(n)}} > \overline{\overline{\mathcal{B}(n)}}\}$. Set $n = 5^0$. $\{k, \text{where } k \text{ is a natural number} : k \mid n\} = \mathcal{A}(n)$. $\overline{\overline{\mathcal{A}(n)}} = 0+1$. $\overline{\overline{\mathcal{B}(n)}} = 0$. X is natural-membered. For every a such that $a \in X$ there exists a natural number b such that $b > a$ and $b \in X$ by [12, (86)], (38), [1, (27)], (36). □

3. PROBLEM 58

Let X be a set. We say that X is positive-membered if and only if

(Def. 2) for every extended real x such that $x \in X$ holds $x > 0$.

Let n be a non zero natural number. Let us note that $\{n\}$ is positive-membered.

Let m be a non zero natural number. Let us observe that $\{m, n\}$ is positive-membered and $\mathbb{N} \setminus \{0\}$ is positive-membered and there exists a set which is non empty, finite, and positive-membered and there exists a set which is infinite and positive-membered.

Now we state the proposition:

(41) Let us consider a positive-membered set A, and a set B. If $B \subseteq A$, then B is positive-membered.

Let A be a positive-membered set. Note that every subset of A is positive-membered.

Let X be a positive-membered set. Observe that every binary relation which is X-valued is also positive yielding.

Let n be a natural number. Observe that $\operatorname{Seg} n$ is positive-membered.

Let X be a positive-membered set. Let us observe that id_X is positive yielding.

Let n be a natural number. One can check that $\operatorname{idseq}(n)$ is positive yielding and $\operatorname{idseq}(n)$ is increasing and $\mathbb{P}$ is positive-membered.

Let s be a natural number. The functor PrimeNumbersS(s) yielding a sequence of $\mathbb{P}$ is defined by

(Def. 3) for every natural number n, $it(n) = \operatorname{pr}(n)$.

Let us note that PrimeNumbersS(s) is increasing and PrimeNumbersS(s) is onto and PrimeNumbersS(s)$\restriction s$ is increasing.

The functor PrimeNumbersFS(s) yielding a finite sequence of elements of $\mathbb{P}$ is defined by the term

(Def. 4) XFS2FS(PrimeNumbersS(s)$\restriction s$).

Now we state the propositions:

(42) Let us consider a natural number s. Then len PrimeNumbersFS(s) $= s$.

(43) Let us consider natural numbers n, s. If $n < s$, then (PrimeNumbersFS(s))($n+1$) $= \operatorname{pr}(n)$.

(44) Let us consider a non zero natural number n, and a natural number s. If $n \leqslant s$, then (PrimeNumbersFS(s))(n) $= \operatorname{pr}(n-1)$. The theorem is a consequence of (43).

Let s be a natural number. Observe that PrimeNumbersFS(s) is increasing and PrimeNumbersFS(s) is positive yielding.

Let s be a non zero natural number. One can verify that PrimeNumbersFS(s) is non empty and PrimeNumbersFS(s) is Chinese remainder.

Now we state the proposition:

(45) Let us consider natural numbers k, s. Suppose $k < s$. Then $\frac{\prod \text{PrimeNumbersFS}(s)}{\operatorname{pr}(k)}$ is a natural number. The theorem is a consequence of (43).

Let s be a natural number. The functor sequenceA(s) yielding a finite sequence of elements of $\mathbb{N}$ is defined by

(Def. 5) $\operatorname{len} it = s$ and for every non zero natural number k such that $k \leqslant s$ for every natural number e such that $e = \frac{\prod \text{PrimeNumbersFS}(s)}{\operatorname{pr}(k-1)}$ holds $it(k) = \operatorname{CRT}(0, e, -1, \operatorname{pr}(k-1)) + \prod \text{PrimeNumbersFS}(s)$.

Let us observe that sequenceA(s) is s-elements and sequenceA(s) is positive yielding.

Now we state the propositions:

(46) Let us consider non zero natural numbers k, s. If $k \leqslant s$, then $\mathrm{pr}(k-1) \mid (\mathrm{sequenceA}(s))(k)+1$. The theorem is a consequence of (45), (42), and (44).

(47) Let us consider non zero natural numbers k, n. Suppose $k \neq n$ and $n \leqslant s$ and $k \leqslant s$. Then $\mathrm{pr}(k-1) \mid (\mathrm{sequenceA}(s))(n)$. The theorem is a consequence of (42), (44), and (45).

Let f, g be real-valued functions. The functor f^g yielding a function is defined by

(Def. 6) $\mathrm{dom}\, it = \mathrm{dom}\, f \cap \mathrm{dom}\, g$ and for every object x such that $x \in \mathrm{dom}\, it$ holds $it(x) = f(x)^{g(x)}$.

Let f, g be real-valued finite sequences. One can verify that f^g is finite sequence-like.

Let n be a natural number and f, g be n-elements, real-valued finite sequences. One can verify that f^g is n-elements.

Let f, g be real-valued functions. Let us note that f^g is $\mathbb{R}$-valued.

Let f be a rational-valued function and g be an integer-valued function. One can check that f^g is $\mathbb{Q}$-valued.

Let f be an integer-valued function and g be a natural-valued function. Let us observe that f^g is $\mathbb{Z}$-valued.

Let f, g be natural-valued functions. One can check that f^g is $\mathbb{N}$-valued.

Let f, g be positive yielding, real-valued functions. Let us observe that f^g is positive yielding.

Let s be a natural number. The functor numberQ(s) yielding a natural number is defined by the term

(Def. 7) $\prod (\mathrm{idseq}(s))^{\mathrm{sequenceA}(s)}$.

Note that numberQ(s) is positive.

The functor Problem58Solution(s) yielding a finite sequence of elements of $\mathbb{N}$ is defined by the term

(Def. 8) $\mathrm{numberQ}(s) \cdot \mathrm{idseq}(s)$.

Observe that Problem58Solution(s) is s-elements.

Now we state the proposition:

(48) If $1 \leqslant k \leqslant s$, then $(\mathrm{Problem58Solution}(s))(k) = k \cdot (\mathrm{numberQ}(s))$.

Let s be a natural number. One can verify that Problem58Solution(s) is increasing and positive yielding.

The functor sequenceAk1Pk(s) yielding a finite sequence of elements of $\mathbb{N}$ is defined by

(Def. 9) len $it = s$ and for every non zero natural number k such that $k \leqslant s$ holds $it(k) = \frac{(\text{sequenceA}(s))(k)+1}{\text{pr}(k-1)}$.

Let us observe that sequenceAk1Pk(s) is s-elements.

Let k be a non zero natural number. Assume $k \leqslant s$. The functor sequenceAnPk(s, k) yielding a finite sequence of elements of $\mathbb{N}$ is defined by

(Def. 10) len $it = s$ and for every non zero natural number n such that $n \leqslant s$ holds if $n \neq k$, then $it(n) = \frac{(\text{sequenceA}(s))(n)}{\text{pr}(k-1)}$ and if $n = k$, then $it(n) = 0$.

The functor sequenceQk(s) yielding a finite sequence of elements of $\mathbb{N}$ is defined by

(Def. 11) len $it = s$ and for every non zero natural number k such that $k \leqslant s$ holds $it(k) = k^{(\text{sequenceAk1Pk}(s))(k)} \cdot (\prod(\text{idseq}(s))^{\text{sequenceAnPk}(s,k)})$.

Let us note that sequenceQk(s) is s-elements.

Now we state the propositions:

(49) Let us consider non zero natural numbers k, w. Suppose $k \leqslant s$ and $w \leqslant s$ and $w \neq k$. Then $((\text{idseq}(s))^{\text{sequenceA}(s)})(w) = ((\text{idseq}(s))^{\text{sequenceAnPk}(s,k)})^{\text{pr}(k-1)}(w)$.

(50) Let us consider a non zero natural number k. Suppose $k \leqslant s$. Then $(\text{Problem58Solution}(s))(k) = (\text{sequenceQk}(s))(k)^{\text{pr}(k-1)}$.

PROOF: Set $p = \text{pr}(k-1)$. Set $A_3 = \text{sequenceAnPk}(s, k)$. Set $I = \text{idseq}(s)$. Set $A = \text{sequenceA}(s)$. Set $F = I^{A_3}$. For every natural number j such that $j \in \text{dom } F^p$ and $k \neq j$ holds $(I^A)(j) = F^p(j)$ by [19, (25)], (49). $\prod I^A = k^{A(k)} \cdot (\prod F)^p$. □

Note that there exists a finite sequence of elements of $\mathbb{N}$ which is finite arithmetic progression-like, increasing, and positive yielding.

Let s be a natural number. One can check that Problem58Solution(s) is finite arithmetic progression-like.

Now we state the proposition:

(51) Let us consider a natural number s. Then there exists a finite arithmetic progression-like, increasing, positive yielding finite sequence f of elements of $\mathbb{N}$ such that

(i) len $f = s$, and

(ii) for every natural number i such that $1 \leqslant i \leqslant \text{len } f$ holds $f(i)$ is perfect power.

The theorem is a consequence of (50).

4. PROBLEM 160

Now we state the proposition:

(52) Let us consider positive natural numbers x, y, z, t. Suppose $x \leqslant y \leqslant z \leqslant t$. Then $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{t} = 1$ if and only if $x = 2$ and $y = 3$ and $z = 7$ and $t = 42$ or $x = 2$ and $y = 3$ and $z = 8$ and $t = 24$ or $x = 2$ and $y = 3$ and $z = 9$ and $t = 18$ or $x = 2$ and $y = 3$ and $z = 10$ and $t = 15$ or $x = 2$ and $y = 3$ and $z = 12$ and $t = 12$ or $x = 2$ and $y = 4$ and $z = 5$ and $t = 20$ or $x = 2$ and $y = 4$ and $z = 6$ and $t = 12$ or $x = 2$ and $y = 4$ and $z = 8$ and $t = 8$ or $x = 2$ and $y = 5$ and $z = 5$ and $t = 10$ or $x = 2$ and $y = 6$ and $z = 6$ and $t = 6$ or $x = 3$ and $y = 3$ and $z = 4$ and $t = 12$ or $x = 3$ and $y = 3$ and $z = 6$ and $t = 6$ or $x = 3$ and $y = 4$ and $z = 4$ and $t = 6$ or $x = 4$ and $y = 4$ and $z = 4$ and $t = 4$.

PROOF: If $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{t} = 1$, then $x = 2$ and $y = 3$ and $z = 7$ and $t = 42$ or $x = 2$ and $y = 3$ and $z = 8$ and $t = 24$ or $x = 2$ and $y = 3$ and $z = 9$ and $t = 18$ or $x = 2$ and $y = 3$ and $z = 10$ and $t = 15$ or $x = 2$ and $y = 3$ and $z = 12$ and $t = 12$ or $x = 2$ and $y = 4$ and $z = 5$ and $t = 20$ or $x = 2$ and $y = 4$ and $z = 6$ and $t = 12$ or $x = 2$ and $y = 4$ and $z = 8$ and $t = 8$ or $x = 2$ and $y = 5$ and $z = 5$ and $t = 10$ or $x = 2$ and $y = 6$ and $z = 6$ and $t = 6$ or $x = 3$ and $y = 3$ and $z = 4$ and $t = 12$ or $x = 3$ and $y = 3$ and $z = 6$ and $t = 6$ or $x = 3$ and $y = 4$ and $z = 4$ and $t = 6$ or $x = 4$ and $y = 4$ and $z = 4$ and $t = 4$ by [3, (23), (13)], [11, (37)]. □

5. PROBLEM 164

Now we state the proposition:

(53) Let us consider positive integers x, y, z, t. Then $\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{t^2} = 1$ if and only if $x = 2$ and $y = 2$ and $z = 2$ and $t = 2$.

PROOF: If $\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{t^2} = 1$, then $x = 2$ and $y = 2$ and $z = 2$ and $t = 2$ by [3, (23)]. □

6. PROBLEM 168

In the sequel f, g denote complex-valued finite sequences.

Now we state the propositions:

(54) $\operatorname{len} f^2 = \operatorname{len} f$.

(55) $\operatorname{len} f^{-1} = \operatorname{len} f$.

(56) $(c \cdot f)\restriction n = c \cdot (f\restriction n)$.

Let us consider a complex-valued function f. Now we state the propositions:

(57) $(f^{-1})^{\mathbf{2}} = f^{\mathbf{2}-1}$.

(58) $(c \cdot f)^{-1} = c^{-1} \cdot f^{-1}$.

Now we state the propositions:

(59) $(f \frown g)^{\mathbf{2}} = f^{\mathbf{2}} \frown g^{\mathbf{2}}$. The theorem is a consequence of (54).

(60) $(f \frown g)^{-1} = f^{-1} \frown g^{-1}$. The theorem is a consequence of (55).

(61) $(f \restriction n)^{-1} = f^{-1} \restriction n$. The theorem is a consequence of (55).

(62) $(f \restriction n)^{\mathbf{2}} = f^{\mathbf{2}} \restriction n$. The theorem is a consequence of (54).

(63) $\langle c \rangle^{-1} = \langle c^{-1} \rangle$. The theorem is a consequence of (55).

(64) $\langle c_1, c_2 \rangle^{-1} = \langle {c_1}^{-1}, {c_2}^{-1} \rangle$. The theorem is a consequence of (63) and (60).

(65) $\langle c_1, c_2, c_3 \rangle^{-1} = \langle {c_1}^{-1}, {c_2}^{-1}, {c_3}^{-1} \rangle$. The theorem is a consequence of (64), (63), and (60).

Let s be a natural number and f be an $(s+1)$-elements, complex-valued finite sequence. We say that f is solution of Sierp168 if and only if

(Def. 12) $\sum((f \restriction s)^{-1})^{\mathbf{2}} = \frac{1}{f(s+1)^{\mathbf{2}}}$.

Let a be an object. One can verify that $\langle a \rangle$ is $(0+1)$-elements.

Let a, b be objects. One can verify that $\langle a, b \rangle$ is $(1+1)$-elements.

Let a, b, c be objects. One can verify that $\langle a, b, c \rangle$ is $(2+1)$-elements.

Now we state the propositions:

(66) $\langle 0 \rangle$ is solution of Sierp168.

(67) $\langle 1, 1 \rangle$ is solution of Sierp168.

PROOF: Set $f = \langle 1, 1 \rangle$. Set $h = f \restriction 1$. Set $g = (h^{-1})^{\mathbf{2}}$. $g = \langle 1 \rangle$ by [19, (29)]. □

(68) $\langle 15, 20, 12 \rangle$ is solution of Sierp168.

PROOF: Set $f = \langle 15, 20, 12 \rangle$. Set $h = f \restriction 2$. Set $g = (h^{-1})^{\mathbf{2}}$. $g = \langle \frac{1}{15^{\mathbf{2}}}, \frac{1}{20^{\mathbf{2}}} \rangle$ by [19, (29)], [4, (45), (59), (44)]. □

(69) Let us consider natural numbers s, n, and an $(s+1)$-elements, complex-valued finite sequence f. If f is solution of Sierp168, then $n \cdot f$ is solution of Sierp168. The theorem is a consequence of (57), (58), and (56).

Let s be a positive natural number and f be an $(s+1)$-elements, complex-valued finite sequence. The functor SierpProblem168FS(f) yielding a finite sequence is defined by the term

(Def. 13) $(12 \cdot (f \restriction (s-1))) \frown \langle 15 \cdot f(s), 20 \cdot f(s), 12 \cdot f(s+1) \rangle$.

One can check that SierpProblem168FS(f) is $(s+1+1)$-elements and SierpProblem168F is complex-valued.

Let f be an $(s+1)$-elements, real-valued finite sequence. Let us observe that SierpProblem168FS(f) is real-valued.

Let f be an $(s+1)$-elements, integer-valued finite sequence. One can verify that SierpProblem168FS(f) is integer-valued.

Let f be an $(s+1)$-elements, natural-valued finite sequence. One can check that SierpProblem168FS(f) is natural-valued.

Let c be a non zero complex number. Note that $\langle c \rangle$ is non-empty.

Let f be a non-empty, complex-valued finite sequence. One can check that $c \cdot f$ is non-empty.

Let f be a non-empty finite sequence and n be a natural number. Note that $f \restriction n$ is non-empty.

Let s be a positive natural number and f be an $(s+1)$-elements, non-empty, real-valued finite sequence. Observe that SierpProblem168FS(f) is non-empty.

Now we state the proposition:

(70) Let us consider a positive natural number s. Then there exists an $(s+1)$-elements, non-empty, natural-valued finite sequence f such that f is solution of Sierp168.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ there exists a $(\$_1+1)$-elements, non-empty, natural-valued finite sequence f such that f is solution of Sierp168. $\mathcal{P}[1]$. For every non zero natural number s such that $\mathcal{P}[s]$ holds $\mathcal{P}[s+1]$ by (56), [4, (44)], [8, (3)], [4, (59), (22), (45)]. For every non zero natural number k, $\mathcal{P}[k]$ from [3, Sch. 10]. □

Let s be a positive natural number.

A Solution of Sierp168 of s is an $(s+1)$-elements, positive yielding, natural-valued finite sequence defined by

(Def. 14) *it* is solution of Sierp168.

Let us note that every Solution of Sierp168 of s is solution of Sierp168.

Let s, n be positive natural numbers and f be a Solution of Sierp168 of s. Note that $n \cdot f$ is solution of Sierp168.

Now we state the proposition:

(71) Let us consider positive natural numbers s, n, and a Solution of Sierp168 f of s. Then $n \cdot f$ is a Solution of Sierp168 of s.

Let s be a positive natural number and f be an $(s+1)$-elements, positive yielding, natural-valued finite sequence. The functor Solutions-of-Sierp168(f) yielding a many sorted set indexed by $\mathbb{N}_+$ is defined by

(Def. 15) for every non zero natural number n, $it(n) = n \cdot f$.

Let us note that Solutions-of-Sierp168(f) is one-to-one.

Now we state the propositions:

(72) Let us consider a positive natural number s, and a Solution of Sierp168 f of s. Then rng Solutions-of-Sierp168(f) $\subseteq$ the set of all g where g is a Solution of Sierp168 of s.

(73) Let us consider a positive natural number S. Then the set of all f where f is a Solution of Sierp168 of S is infinite. The theorem is a consequence of (72).

7. Problem 171

Now we state the propositions:

(74) Let us consider a positive integer n. Then $n \leqslant 7$ or $n \in \{9, 10, 12, 15\}$ if and only if there exist no positive integers x, y such that $3 \cdot x + 5 \cdot y = n$. Proof: If $n \leqslant 7$ or $n \in \{9, 10, 12, 15\}$, then there exist no positive integers x, y such that $3 \cdot x + 5 \cdot y = n$ by [3, (13)], [20, (1)], [13, (30)], [9, (4)]. Consider k being a natural number such that $n = 3 \cdot k$ or $n = 3 \cdot k + 1$ or $n = 3 \cdot k + 2$. □

(75) Let us consider positive integers m, n. Suppose $n > 40 \cdot m$. Let us consider a finite set A. Suppose $A = \{\langle x, y\rangle$, where x, y are positive integers : $3 \cdot x + 5 \cdot y = n\}$. Then $\overline{\overline{A}} > m$. The theorem is a consequence of (74).

8. Problem 188

Now we state the propositions:

(76) If $m \neq 0$, then $i \operatorname{div}(\gcd(i, m))$ and $m \operatorname{div}(\gcd(i, m))$ are relatively prime.

(77) There exist no positive natural numbers x, y, z, t such that $x^{\mathbf{2}} + 2 \cdot y^{\mathbf{2}} = z^{\mathbf{2}}$ and $2 \cdot x^{\mathbf{2}} + y^{\mathbf{2}} = t^{\mathbf{2}}$. The theorem is a consequence of (76).

9. Problem 195

Now we state the propositions:

(78) If n is even, then $n \bmod 4 = 0$ or $n \bmod 4 = 2$.

(79) If n is even, then $n \equiv 0 \pmod 4$ or $n \equiv 2 \pmod 4$. The theorem is a consequence of (78).

(80) If n is odd, then $n \bmod 4 = 1$ or $n \bmod 4 = 3$. The theorem is a consequence of (78).

(81) If n is odd, then $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$. The theorem is a consequence of (80).

(82) If i is even, then $i^3 \bmod 8 = 0$.

(83) Let us consider a non zero natural number k. Then there exist no positive natural numbers x, y such that $x^2 + 2^{2 \cdot k} + 1 = y^3$. The theorem is a consequence of (82) and (81).

10. PROBLEM 196

Now we state the proposition:

(84) Let us consider positive natural numbers x, y, z, t. Suppose $x \leqslant y$ and $x \leqslant z \leqslant t$. Then $x + y = z \cdot t$ and $z + t = x \cdot y$ if and only if $x = 1$ and $y = 5$ and $z = 2$ and $t = 3$ or $x = 2$ and $y = 2$ and $z = 2$ and $t = 2$.

PROOF: If $x + y = z \cdot t$ and $z + t = x \cdot y$, then $x = 1$ and $y = 5$ and $z = 2$ and $t = 3$ or $x = 2$ and $y = 2$ and $z = 2$ and $t = 2$ by [3, (13)], [18, (5)], [3, (10)]. □

The functor exampleSierpinski196 yielding a function from $\mathbb{N}$ into $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is defined by

(Def. 16) for every natural number n, $it(n) = \langle -1, n, 1 - n, -1 \rangle$.

One can check that exampleSierpinski196 is one-to-one.

Now we state the propositions:

(85) $\operatorname{rng} \text{exampleSierpinski196} \subseteq \{\langle x, y, z, t \rangle$, where x, y, z, t are integers : $x + y = z \cdot t$ and $z + t = x \cdot y\}$.

(86) $\{\langle x, y, z, t \rangle$, where x, y, z, t are integers : $x + y = z \cdot t$ and $z + t = x \cdot y\}$ is infinite. The theorem is a consequence of (85).

11. PROBLEM 198

From now on a, b, x, y denote real numbers.

Let r be a non negative real number. One can check that $\lceil r \rceil$ is natural.

Let f be a non empty, positive yielding, real-valued finite sequence. Observe that $\sum f$ is positive.

Let a, b be positive real numbers and n be a natural number. Let us observe that $(a, b)\,\text{Subnomial}\, n$ is positive yielding.

Let r be a non positive real number. Note that $\langle r \rangle$ is non positive yielding.

Now we state the propositions:

(87) Let us consider positive natural numbers n, x, y. Suppose $a > 0$ and $2 \leqslant n$ and $x^n - y^n = a$. Then

(i) $x < \operatorname{root}_{n-1}(a)$, and

(ii) $y < \operatorname{root}_{n-1}(a)$.

(88) Let us consider positive natural numbers k, x, y. Suppose $a > 0$ and $x^{2 \cdot k} - y^{2 \cdot k} = a$. Then

(i) $x < \operatorname{root}_k(a)$, and

(ii) $y < \operatorname{root}_k(a)$.

(89) Let us consider complex numbers a, x, y. Then $x^1 - y^1 = a$ if and only if $x = a + y$.

The scheme *FinitePairs* deals with natural numbers $\mathcal{M}$, $\mathcal{N}$ and a binary predicate $\mathcal{P}$ and states that

(Sch. 1) $\{\langle m, n\rangle$, where m, n are natural numbers : $m < \mathcal{M}$ and $n < \mathcal{N}$ and $\mathcal{P}[m, n]\}$ is finite.

Now we state the proposition:

(90) Let us consider positive natural numbers a, n. Suppose $2 \leqslant n$. Then $\{\langle x, y\rangle$, where x, y are positive natural numbers : $x^n - y^n = a\}$ is finite.

PROOF: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $x^n - y^n = a\}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ not contradiction. Set $M = \text{root}_{n-1}(a)$. Set $M_1 = \lceil M \rceil$. Set $B = \{\langle x, y\rangle$, where x, y are natural numbers : $x < M_1$ and $y < M_1$ and $\mathcal{P}[x, y]\}$. B is finite from *FinitePairs*. $A \subseteq B$. □

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] 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.

[6] 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.

[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[8] Wenpai Chang, Hiroshi Yamazaki, and Yatsuka Nakamura. The inner product and conjugate of finite sequences of complex numbers. *Formalized Mathematics*, 13(**3**):367–373, 2005.

[9] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[10] Adam Grabowski. Elementary number theory problems. Part VI. *Formalized Mathematics*, 30(**3**):235–244, 2022. doi:10.2478/forma-2022-0019.

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

[12] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[13] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[14] 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.

[15] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[16] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

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

[18] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[19] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[20] 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.

[21] 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 8, 2024