FORMALIZED MATHEMATICS
Vol. 33, No. 1, pp. 217–229, 2025
DOI: 10.2478/forma-2025-0017
e-ISSN: 1898–9934

Elementary Number Theory Problems. Part XVIII

Adam Grabowski
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper another seven problems from Wacław Sierpiński's book "250 Problems in Elementary Number Theory" are formalized, using the Mizar formalism, namely: 53, 61, 81, 90, 100, 156, and 167.

MSC: 11A99 68V20 68V35

Keywords: number of divisors; Fermat prime; Mersenne prime

MML identifier: `NUMBER18`, version: `8.1.15 5.98.1507`

Introduction

In this paper we continue formalizing the proofs of selected problems from Sierpiński's book "250 Problems in Elementary Number Theory" [18] using the Mizar formalism [8], [14]. The paper is a part of the project *Formalization of Elementary Number Theory in Mizar* [12].

In Sect. 1 we prove important formula on the number of natural divisors (> 0) of a number (which is equal to $\sigma_0(n)$) [4]. It is well-known that if $n = {p_1}^{k_1} \cdot \ldots \cdot {p_m}^{k_m}$, then the number of divisors of n is just $(k_1+1)\cdot\ldots\cdot(k_m+1)$ [16]. This is proven in a standard way; first, we define many sorted set `BNumberOfDivisors` of the desired form, and then we take the product of this set.

Problem 53 demonstrates that for every natural number $n > 0$, the set of all positive integers whose number of positive integer divisors is divisible by n contains an infinite arithmetic progression. It is enough to take the arithmetic progression [6] of the form $2^n t + 2^{n-1}$ (`Sierp53Seq` in Sect. 2) and use the aforementioned formula for the number of positive divisors.

Problem 81 is about the existence of primes p, q, r such that $p(p+1), q(q+1)$, and $q(q+1)$ form an increasing arithmetic progression [17]. Clearly, the numbers $127, 3697$, and 5227 satisfy this property (in [18] $q = 5527$, a typo), but Sierpiński does not claim that by getting appropriate triangular numbers with prime indices, we can obtain *all* such triplets (with a reference for a conjecture by A. Schinzel [15]).

Problem 90 asks if there exist only finitely many positive integers n such that both n and $n+1$ have only one prime divisor [7] is equivalent to the theorem asserting that there exist only finitely many prime Mersenne numbers and finitely many prime Fermat numbers [3]. Both problems (about the existence of infinitely many Fermat and Mersenne primes) are still open [9], but this equivalence can be proven using auxiliary facts from [16] (a prevailing belief, supported by the Lenstra-Pomerance-Wagstaff conjecture [2], is that there are infinitely many Mersenne primes; similarly with Fermat primes [5], [10]).

Problem 100 actually shows that all numbers of the form $2^{m!+k} - 1$ are not prime for $k = 2, 3, \ldots$, hence for $m - 1$ (i.e., for arbitrarily long subsequences) consecutive terms of the sequence $2^n - 1$ are composite Mersenne numbers.

The solution of Problem 167, on the existence of the solution of the equation

$$\frac{1}{x_1^m} + \frac{1}{x_2^m} + \ldots + \frac{1}{x_s^m} = 1$$

in positive integers $x_1, x_2, \ldots, x_s$ [11] is obtained via the construction of the Mizar functor `Expand` (Def. 11), for which was proven that if the equation is solvable for positive integer s, then it is also solvable for $s + (a^m - 1)k$, where k is an arbitrary positive integer and uses extensively Corollary 2, p. 29 from [16] (see Th. 77).

1. The Number of Natural Divisors

Let n be a natural number. The functor BNumberOfDivisors(n) yielding a many sorted set indexed by $\mathbb{P}$ is defined by

(Def. 1) support it = support PFExp(n) and for every natural number p such that $p \in$ support PFExp(n) holds $it(p) = (p\text{-count}(n)) + 1$.

Let n be a non zero natural number. One can verify that BNumberOfDivisors (n) is natural-valued and finite-support.

The functor NumberOfDivisors(n) yielding a natural number is defined by the term

(Def. 2) $\prod$ BNumberOfDivisors(n).

Now we state the propositions:

(1) Let us consider a prime number p. Then $(\text{BNumberOfDivisors}(p)) \cdot \langle p \rangle = \langle 2 \rangle$.
PROOF: Set $f = \langle p \rangle$. Set $g = \text{BNumberOfDivisors}(p)$. Set $z = \langle 2 \rangle$. $\text{dom}(g \cdot f) = \{1\}$. For every object x such that $x \in \text{dom}(g \cdot f)$ holds $(g \cdot f)(x) = z(x)$. □

(2) $\text{BNumberOfDivisors}(1) = \text{EmptyBag}\,\mathbb{P}$.

(3) Let us consider a prime number p, and a non zero natural number n. If $p\text{-count}(n) = 0$, then $(\text{BNumberOfDivisors}(n))(p) = 0$.

(4) Let us consider a non zero natural number n, and a prime number p. Suppose $p\text{-count}(n) \neq 0$. Then $(\text{BNumberOfDivisors}(n))(p) = (p\text{-count}(n)) + 1$.

(5) Let us consider non zero natural numbers m, n. Suppose m and n are relatively prime. Then $\text{BNumberOfDivisors}(m \cdot n) = \text{BNumberOfDivisors}(m) + \text{BNumberOfDivisors}(n)$. The theorem is a consequence of (3) and (4).

Let n be a natural number. The functor $\text{divs}(n)$ yielding a natural number is defined by the term

(Def. 3) $\sigma_0(n)$.

Now we state the propositions:

(6) $\text{EXP}\,0 = \mathbb{N} \longmapsto 1$.
PROOF: Set $f = \text{EXP}\,0$. Set $g = \mathbb{N} \longmapsto 1$. For every element n of $\mathbb{N}$, $f(n) = g(n)$. □

(7) $\text{EXP}\,1 = \text{id}_{\mathbb{N}}$.

(8) Let us consider a natural number n. If $n = 0$, then $\text{divs}(n) = 0$.

(9) Let us consider a finite subset X of $\mathbb{N}$. Then $\sum((\mathbb{N} \longmapsto 1) \restriction X) = \overline{\overline{X}}$.

(10) Let us consider a prime number p. Then $\text{divs}(p) = 2$. The theorem is a consequence of (6) and (9).

(11) Let us consider non zero natural numbers m, n. Suppose m and n are relatively prime. Then $\text{NumberOfDivisors}(m \cdot n) = (\text{NumberOfDivisors}(m)) \cdot (\text{NumberOfDivisors}(n))$. The theorem is a consequence of (5).

(12) Let us consider a non zero natural number n. Then $\text{divs}(n) = \overline{\overline{\alpha}}$, where α is the set of positive divisors of n. The theorem is a consequence of (6) and (9).

(13) Let us consider a natural number k. Then $\overline{\overline{k \cup \{k\}}} = k + 1$.

(14) Let us consider a prime number p, and a natural number k. Then $\overline{\overline{\alpha}} = k + 1$, where α is the set of positive divisors of p^k.
PROOF: $\{l,$ where l is an element of $\mathbb{N} : l \leqslant k\} = k \cup \{k\}$. Define $\mathcal{F}(\text{element of } \mathbb{N}) = p^{\$_1}$. Set $X = \{l,$ where l is an element of $\mathbb{N} : l \leqslant k\}$. Set $Y_1 =$

$\{\mathcal{F}(w)$, where w is an element of $\mathbb{N} : w \in X\}$. $Y_1 = \{p^l$, where l is an element of $\mathbb{N} : l \leqslant k\}$. $Y_1 \subseteq \operatorname{Seg} p^k \cup \{p^k\}$. Set $F_1 = \{l$, where l is an element of $\mathbb{N} : l \leqslant k\}$. Define $\mathcal{F}$(element of $\mathbb{N}) = p^{\$_1} (\in \mathbb{N})$. There exists a function f from $\mathbb{N}$ into $\mathbb{N}$ such that for every element x of $\mathbb{N}$, $f(x) = \mathcal{F}(x)$. Consider f_3 being a function from $\mathbb{N}$ into $\mathbb{N}$ such that for every element x of $\mathbb{N}$, $f_3(x) = \mathcal{F}(x)$. Set $f = f_3 \restriction F_1$. $F_1 \subseteq \mathbb{N}$. $\operatorname{rng} f = Y_1$. For every objects x_1, x_2 such that x_1, $x_2 \in \operatorname{dom} f_3$ and $f_3(x_1) = f_3(x_2)$ holds $x_1 = x_2$. $\square$

The functor Divs yielding a sequence of $\mathbb{N}$ is defined by

(Def. 4) for every element n of $\mathbb{N}$, $it(n) = \operatorname{divs}(n)$.

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

(15) If m and n are relatively prime, then $\operatorname{divs}(m \cdot n) = (\operatorname{divs}(m)) \cdot (\operatorname{divs}(n))$.

(16) If m and n are relatively prime, then $\overline{\overline{\alpha}} = \overline{\overline{\beta}} \cdot \overline{\overline{\gamma}}$, where α is the set of positive divisors of $m \cdot n$, β is the set of positive divisors of m, and γ is the set of positive divisors of n. The theorem is a consequence of (15) and (12).

(17) Let us consider a natural number k. Then $\operatorname{divs}(2^k) = k+1$. The theorem is a consequence of (14) and (12).

2. Problem 53

Now we state the proposition:

(18) Let us consider a non zero natural number n, and natural numbers k, t. Suppose $k \geqslant 1$ and $n = 2^k \cdot t + 2^{k-'1}$. Then $k \mid \overline{\overline{\alpha}}$, where α is the set of positive divisors of n. The theorem is a consequence of (12), (17), and (15).

Let k be a natural number. The functor Sierp53Seq(k) yielding a sequence of $\mathbb{R}$ is defined by the term

(Def. 5) $\operatorname{ArProg}(2^{k-'1}, 2^k)$.

Let k be a positive natural number and t be a natural number. Note that (Sierp53Seq(k))(t) is non zero and natural. Now we state the proposition:

(19) Let us consider a positive natural number k, and a natural number t. Then $k \mid \overline{\overline{\alpha}}$, where α is the set of positive divisors of (Sierp53Seq(k))(t). The theorem is a consequence of (18).

3. PROBLEM 61

Now we state the proposition:

(20) 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) $\operatorname{len} f = s$, and

(ii) for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $f(i)$ is not prime.

4. PROBLEM 81

Now we state the propositions:

(21) There exist prime numbers p, q, r such that $\operatorname{Triangle} p$, $\operatorname{Triangle} q$ and $\operatorname{Triangle} r$ form an arithmetic progression.

(22) Let us consider prime numbers p, q, r. Suppose $p = 127$ and $q = 3697$ and $r = 5227$. Then $p \cdot (p+1)$, $q \cdot (q+1)$ and $r \cdot (r+1)$ form an arithmetic progression.

5. LEMMAS TO PROBLEM 90

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

(23) Suppose $m \geqslant 1$. Then suppose M_m is a prime number. Then

(i) $\overline{\overline{\operatorname{PrimeDivisors}(M_m)}} = 1$, and

(ii) $\overline{\overline{\operatorname{PrimeDivisors}(M_m + 1)}} = 1$.

(24) Suppose $m \geqslant 1$. Then suppose $\operatorname{Fermat} m$ is a prime number. Then

(i) $\overline{\overline{\operatorname{PrimeDivisors}(\operatorname{Fermat} m)}} = 1$, and

(ii) $\overline{\overline{\operatorname{PrimeDivisors}(\operatorname{Fermat} m - 1)}} = 1$.

The functor MersennePrimes yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 6) $\{n$, where n is a prime number : n is Mersenne$\}$.

Let n be a natural number. We say that n is Fermat if and only if

(Def. 7) there exists a natural number k such that $n = \operatorname{Fermat} k$.

The functor FermatPrimes yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 8) $\{n$, where n is a prime number : n is Fermat$\}$.

Now we state the proposition:

(25) Let us consider a Mersenne prime number n. Then

(i) $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$, and

(ii) $\overline{\overline{\text{PrimeDivisors}(n+1)}} = 1$.

PROOF: Consider k being a natural number such that $n = M_k$. $k \geqslant 1$. $\square$

Let us observe that there exists a prime number which is Fermat. Now we state the propositions:

(26) Let us consider a Fermat prime number n. Then

(i) $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$, and

(ii) $\overline{\overline{\text{PrimeDivisors}(n-1)}} = 1$.

(27) MersennePrimes $\subseteq \mathbb{P}$.

(28) FermatPrimes $\subseteq \mathbb{P}$.

Note that every set which is Mersenne is also natural. Now we state the proposition:

(29) Let us consider an odd natural number m, and a natural number k. If $m \mid 2^k$, then $m = 1$.

Note that there exists a finite sequence of elements of $\mathbb{R}$ which is $\mathbb{Z}$-valued.

Now we state the propositions:

(30) Let us consider a $\mathbb{Z}$-valued finite sequence F of elements of $\mathbb{R}$. Suppose $\operatorname{len} F$ is odd and for every natural number i such that $i \in \operatorname{dom} F$ holds $F(i)$ is odd. Then $\sum F$ is odd.

PROOF: $F \bmod 2 = \operatorname{len} F \mapsto 1$. $\square$

(31) Let us consider natural numbers n, k, m. If $n > 1$ and $m > 1$, then $M_n \neq k^m$.

PROOF: $k \neq 0$. k is odd. m is odd by [20, (74)], [1, (16),(17),(18)]. $k \neq 1$. Consider i being a natural number such that $m = 2 \cdot i + 1$. Set $R = k^m + 1 \operatorname{div}(k+1)$. Set $m_1 = m -' 1$. Set $S_1 = (k, -1)\,\text{Subnomial}\, m_1$. For every natural number i such that $i \in \operatorname{dom} S_1$ holds $S_1(i)$ is odd. R is odd. $R = 1$. $\square$

(32) $\overline{\overline{\text{PrimeDivisors}(1)}} = 0$.

(33) Let us consider natural numbers k, l. If $2^k - 2^l = 2$ and $k \geqslant 2$ and $l \geqslant 1$, then $k = 2$ and $l = 1$.

(34) 3 is a Fermat prime number.

(35) 3 is a Mersenne prime number.

Let us observe that there exists an integer which is odd and natural.

Now we state the proposition:

(36) PrimeDivisors$(0) = \mathbb{P}$.

One can check that $\overline{\overline{\mathbb{P}}}$ is non zero. Now we state the propositions:

(37) Let us consider an odd, natural integer n, and a natural number k. If $n \mid 2^k$, then $n = 1$.

(38) Let us consider natural numbers a, b. If $a \mid b$, then PrimeDivisors$(a) \subseteq$ PrimeDivisors(b).

(39) Let us consider natural numbers m, n. Suppose PrimeDivisors$(n) = \{m\}$. Then

(i) m-count$(n) \geqslant 1$, and

(ii) $n = m^{m\text{-count}(n)}$.

The theorem is a consequence of (36).

(40) Let us consider an even natural number n. Suppose $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$. Then there exists a natural number k such that

(i) $k \geqslant 1$, and

(ii) $n = 2^k$.

The theorem is a consequence of (36).

(41) Let us consider an odd natural number n. Suppose $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$. Then there exists a natural number k and there exists a prime number p such that $n = p^k$. The theorem is a consequence of (39).

(42) Let us consider an even natural number n. Suppose $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$. Then there exists a natural number k such that $n = 2^k$. The theorem is a consequence of (36) and (39).

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

(43) If $n > 1$, then $a^n + 1$ is odd iff a is even.

(44) If $a > 1$ and $n > 1$ and $a^n + 1$ is a prime number, then n is even.
PROOF: $a + 1 \neq a^n + 1$. □

(45) If $a > 1$ and $n > 1$ and $a^n + 1$ is a prime number, then a is even and there exists a non zero natural number k such that $n = 2^k$.
PROOF: If n is even, then there exists a natural number s such that $n = 2^s$ by [13, (2)]. n is even by [19, (51)]. Consider s being a natural number such that $n = 2^s$. $s \neq 0$. a is even. □

Let n be a natural number. One can verify that M_n is Mersenne and Fermat n is Fermat.

6. Problem 90

Now we state the propositions:

(46) Suppose $\overline{\overline{\text{PrimeDivisors}(0)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(0+1)}} = 1$. Then

(i) 0 is a Mersenne prime number, or

(ii) $0+1$ is a Fermat prime number.

The theorem is a consequence of (32).

(47) Suppose $\overline{\overline{\text{PrimeDivisors}(1)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(1+1)}} = 1$. Then

(i) 1 is a Mersenne prime number, or

(ii) $1+1$ is a Fermat prime number.

The theorem is a consequence of (32).

(48) Suppose $\overline{\overline{\text{PrimeDivisors}(2)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(2+1)}} = 1$. Then

(i) 2 is a Mersenne prime number, or

(ii) $2+1$ is a Fermat prime number.

(49) Suppose $\overline{\overline{\text{PrimeDivisors}(3)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(3+1)}} = 1$. Then

(i) 3 is a Mersenne prime number, or

(ii) $3+1$ is a Fermat prime number.

(50) Suppose $\overline{\overline{\text{PrimeDivisors}(4)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(4+1)}} = 1$. Then

(i) 4 is a Mersenne prime number, or

(ii) $4+1$ is a Fermat prime number.

(51) Suppose $\overline{\overline{\text{PrimeDivisors}(5)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(5+1)}} = 1$. Then

(i) 5 is a Mersenne prime number, or

(ii) $5+1$ is a Fermat prime number.

(52) Suppose $\overline{\overline{\text{PrimeDivisors}(6)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(6+1)}} = 1$. Then

(i) 6 is a Mersenne prime number, or

(ii) $6+1$ is a Fermat prime number.

(53) Suppose $\overline{\overline{\text{PrimeDivisors}(7)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(7+1)}} = 1$. Then

(i) 7 is a Mersenne prime number, or

(ii) $7+1$ is a Fermat prime number.

(54) If $\overline{\overline{\text{PrimeDivisors}(8)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(8+1)}} = 1$, then 8 is a Mersenne prime number or $8+1$ is a Fermat prime number.

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

(55) Suppose $n < 8$ and $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(n+1)}} = 1$. Then

(i) n is a Mersenne prime number, or

(ii) $n+1$ is a Fermat prime number.

The theorem is a consequence of (46), (47), (48), (49), (50), (51), (52), and (53).

(56) Suppose $n > 8$ and $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(n+1)}} = 1$. Then

(i) n is a Mersenne prime number, or

(ii) $n+1$ is a Fermat prime number.

The theorem is a consequence of (42), (41), (32), (31), (34), (45), (30), (37), and (33).

(57) Let us consider a prime number p, and a natural number k. Suppose $k \geqslant 1$. Then $\overline{\overline{\text{PrimeDivisors}(p^k)}} = 1$.

One can check that MersennePrimes is non empty and natural-membered.

Now we state the propositions:

(58) Suppose $\{n$, where n is a natural number : $n > 8$ and $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(n+1)}} = 1\}$ is infinite.
Then MersennePrimes $\cup$ FermatPrimes is infinite.
PROOF: Set $M_1 =$ MersennePrimes $\cup$ FermatPrimes. For every natural number m, there exists a natural number n such that $n \geqslant m$ and $n \in M_1$. □

(59) Suppose MersennePrimes $\cup$ FermatPrimes is finite. Then $\{n$, where n is a natural number : $n > 8$ and $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(n+1)}} = 1\}$ is finite.

(60) Let us consider an infinite subset X of $\mathbb{N}$, and a natural number a. Then there exists a natural number b such that

(i) $b > a$, and

(ii) $b \in X$.

PROOF: $X \subseteq \text{Seg}\, a \cup \{0\}$. □

(61) Suppose $\{n$, where n is a natural number : $\overline{\overline{\text{PrimeDivisors}(n)}} = 1$ and $\overline{\overline{\text{PrimeDivisors}(n+1)}} = 1\}$ is finite. Then MersennePrimes $\cup$ FermatPrimes is finite. The theorem is a consequence of (60), (25), and (26).

7. Problem 100

The functor MersenneSeq yielding a sequence of $\mathbb{N}$ is defined by

(Def. 9) for every element n of $\mathbb{N}$, $it(n) = M_n$.

Now we state the propositions:

(62) Let us consider natural numbers m, k. If $m \geqslant k \geqslant 2$, then $2^{m!+k} - 1$ is not a prime number.
PROOF: $2^k \neq 2^{m!+k}$. □

(63) Let us consider a natural number m. Then rng(MersenneSeq $\restriction$ Seg$(m! + 2, m! + m)$) misses $\mathbb{P}$. The theorem is a consequence of (62).

8. Problem 156

Now we state the propositions:

(64) There exist no positive natural numbers x, y, z such that $x^3 + y^3 + z^3 = x \cdot y \cdot z$.

(65) There exist no positive natural numbers x, y, z such that $x^3 + y^3 + z^3 = 2 \cdot x \cdot y \cdot z$.

(66) Let us consider positive natural numbers x, y, z. If $x^3+y^3+z^3 = 3 \cdot x \cdot y \cdot z$, then $x = y$ and $y = z$.

9. Lemmas to Problem 167

Now we state the propositions:

(67) Let us consider non zero natural numbers a, b. Suppose a and b are relatively prime. Then there exist natural numbers u, v such that $a \cdot u - b \cdot v = 1$.

(68) Let us consider real numbers a, b. If $a - b > 1$, then there exists an integer t such that $a > t > b$.

(69) Let us consider non zero natural numbers a, b. Suppose a and b are relatively prime. Let us consider a natural number n. Suppose $n > a \cdot b$. Then there exist non zero natural numbers x, y such that $n = a \cdot x + b \cdot y$. The theorem is a consequence of (67) and (68).

(70) Let us consider a non zero natural number m. Then $2^m - 1$ and $(2^m - 1)^m - 1$ are relatively prime.

(71) Let us consider non zero natural numbers m, n. Suppose $n > (2^m - 1) \cdot ((2^m - 1)^m - 1)$. Then there exist non zero natural numbers k, l such that $n = (2^m - 1) \cdot k + ((2^m - 1)^m - 1) \cdot l$. The theorem is a consequence of (70) and (69).

10. PROBLEM 167

Let s be a natural number. One can verify that there exists a finite sequence which is s-element, positive yielding, and natural-valued. Let f be an s-element, natural-valued finite sequence. Let us note that $f\restriction s$ is s-element. Let f be an s-element, positive yielding, natural-valued finite sequence. Let us note that $(f\restriction s)^{-1}$ is s-element. Let s, m be natural numbers. We say that f is m-solution of 167th Sierpiński problem if and only if

(Def. 10) $\sum (f^{-1})^m = 1$.

Now we state the proposition:

(72) Let us consider natural numbers s, m, and an s-element, positive yielding, natural-valued finite sequence f. Suppose $s = 2^m$ and $f = s \mapsto 2$. Then f is m-solution of 167th Sierpiński problem.
PROOF: For every object x such that $x \in \operatorname{dom}((f\restriction s)^{-1})^m$ holds $((f\restriction s)^{-1})^m(x) = (s \mapsto 2^{m-1})(x)$. □

Let s, m, a be non zero natural numbers and f be an s-element, positive yielding, natural-valued finite sequence. The functor Expand(f, m, a) yielding an $(s + a^m - 1)$-element, natural-valued finite sequence is defined by the term

(Def. 11) $(f\restriction (s -' 1)) \frown (a^m \mapsto a \cdot f(s))$.

Let n be a non zero natural number and a be a positive real number. Let us note that $n \mapsto a$ is positive yielding. Let s, a be non zero natural numbers. Let us note that $s \mapsto a$ is positive yielding. Let s, m, a be non zero natural numbers and f be an s-element, positive yielding, natural-valued finite sequence. Let us note that Expand(f, m, a) is positive yielding. Now we state the propositions:

(73) Let us consider real-valued finite sequences f, g, and a non zero natural number m. Then $(f \frown g)^m = f^m \frown g^m$.
PROOF: Set $f_3 = (f \frown g)^m$. Set $g_1 = f^m \frown g^m$. For every natural number k such that $k \in \operatorname{dom} f_3$ holds $f_3(k) = g_1(k)$. □

(74) Let us consider a real number a, and a non zero natural number m. Then $\langle a\rangle^m = \langle a^m\rangle$.
PROOF: Set $f = \langle a\rangle^m$. Set $g = \langle a^m\rangle$. For every natural number k such that $k \in \operatorname{dom} f$ holds $f(k) = g(k)$. □

(75) Let us consider non zero natural numbers s, m, a, a positive yielding, s-element, natural-valued finite sequence f, and a positive yielding, $(s+a^m-1)$-element, natural-valued finite sequence g. Suppose $g = \text{Expand}(f, m, a)$. Then $\sum (f^{-1})^m = \sum (g^{-1})^m$.
PROOF: Set $t = s -' 1$. $(f^{-1})^m = ((f\restriction t)^{-1})^m \frown (\langle f(s)\rangle^{-1})^m$. Set $h = a^m \mapsto a \cdot f(s)$. $\sum ((h\restriction a^m)^{-1})^m = (\frac{1}{f(s)})^m$. Set $f_3 = f\restriction t$. Set $g_1 = a^m \mapsto a \cdot f(s)$. $((f_3 \frown g_1)^{-1})^m = ({f_3}^{-1})^m \frown ({g_1}^{-1})^m$. $\langle (f(s)^{-1})^m\rangle = (\langle f(s)\rangle^{-1})^m$. □

(76) Let us consider non zero natural numbers s, m, a, and a positive yielding, s-element, natural-valued finite sequence f. Suppose f is m-solution of 167th Sierpiński problem. Then Expand(f, m, a) is m-solution of 167th Sierpiński problem.

PROOF: Set $t = s -' 1$. $(f^{-1})^m = ((f\restriction t)^{-1})^m \frown (\langle f(s)\rangle^{-1})^m$. Set $h = a^m \mapsto a \cdot f(s)$. $\sum ((h\restriction a^m)^{-1})^m = (\frac{1}{f(s)})^m$. Set $f_3 = f\restriction t$. Set $g_1 = a^m \mapsto a \cdot f(s)$. $((f_3 \frown g_1)^{-1})^m = (f_3{}^{-1})^m \frown (g_1{}^{-1})^m$. $\langle (f(s)^{-1})^m\rangle = (\langle f(s)\rangle^{-1})^m$. □

(77) Let us consider non zero natural numbers m, s, k, l, a, b. Suppose there exists a positive yielding, s-element, natural-valued finite sequence f such that f is m-solution of 167th Sierpiński problem. Then there exists a positive yielding, $(s + (a^m - 1) \cdot k + (b^m - 1) \cdot l)$-element, natural-valued finite sequence f such that f is m-solution of 167th Sierpiński problem.

PROOF: Consider f being a positive yielding, s-element, natural-valued finite sequence such that f is m-solution of 167th Sierpiński problem. Define $\mathcal{P}$[non zero natural number] ≡ there exists a positive yielding, $(s + (a^m - 1) \cdot \$_1)$-element, natural-valued finite sequence f such that f is m-solution of 167th Sierpiński problem. $\mathcal{P}[1]$. For every non zero natural number l such that $\mathcal{P}[l]$ holds $\mathcal{P}[l + 1]$.

For every non zero natural number n, $\mathcal{P}[n]$. Consider f being a positive yielding, $(s + (a^m - 1) \cdot k)$-element, natural-valued finite sequence such that f is m-solution of 167th Sierpiński problem.

Define $\mathcal{Q}$[non zero natural number] ≡ there exists a positive yielding, $(s + (a^m - 1) \cdot k + (b^m - 1) \cdot \$_1)$-element, natural-valued finite sequence f such that f is m-solution of 167th Sierpiński problem. $\mathcal{Q}[1]$. For every non zero natural number l such that $\mathcal{Q}[l]$ holds $\mathcal{Q}[l + 1]$. For every non zero natural number n, $\mathcal{Q}[n]$. □

(78) Let us consider a non zero natural number m. Then there exists a natural number N such that for every non zero natural number n such that $n > N$ there exists a positive yielding, n-element, natural-valued finite sequence f such that f is m-solution of 167th Sierpiński problem. The theorem is a consequence of (72), (71), and (77).

ACKNOWLEDGEMENT: The Mizar processing has been performed using the infrastructure of the University of Bialystok High Performance Computing Center.

REFERENCES

[1] Kenichi Arai and Hiroyuki Okazaki. Properties of primes and multiplicative group of a field. *Formalized Mathematics*, 17(**2**):151–155, 2009. doi:10.2478/v10037-009-0017-7.

[2] P.T. Bateman, J.L. Selfridge, and S.S. Wagstaff Jr. The editor's corner: The new Mersenne conjecture. *The American Mathematical Monthly*, 96(2):125–128, 1989. doi:10.1080/00029890.1989.11972155.

[3] John Horton Conway and R.K. Guy. *The Book of Numbers*. Springer-Verlag, 1996.

[4] Leonard Eugene Dickson. *History of Theory of Numbers*. New York, 1952.

[5] Harvey Dubner and Wilfrid Keller. Factors of generalized Fermat numbers. *Mathematics of Computation*, 64(209):397–405, 1995. doi:10.2307/2153343.

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

[7] 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.

[8] 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.

[9] Richard K. Guy. *Unsolved Problems in Number Theory*. Problem Books in Mathematics. Springer, third edition, 2004. doi:10.1007/978-0-387-26677-0.

[10] Michal Křížek, Florian Luca, and Lawrence Somer. Factors of Fermat numbers. In *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, pages 70–79. Springer New York, 2001. doi:10.1007/978-0-387-21850-2_7.

[11] Louis J. Mordell. *Diophantine Equations*. Academic Press, 1969.

[12] 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.

[13] Marco Riccardi. The perfect number theorem and Wilson's theorem. *Formalized Mathematics*, 17(**2**):123–128, 2009. doi:10.2478/v10037-009-0013-y.

[14] Colin Rothgang, Artur Korniłowicz, and Florian Rabe. A new export of the Mizar Mathematical Library. In Fairouz Kamareddine and Claudio Sacerdoti Coen, editors, *Intelligent Computer Mathematics*, pages 205–210, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-81097-9_17.

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

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

[17] Wacław Sierpiński. *Teoria liczb*. Instytut Matematyczny Polskiej Akademii Nauk, 1950. In Polish.

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

[19] Rafał Ziobro. On subnomials. *Formalized Mathematics*, 24(**4**):261–273, 2016. doi:10.1515/forma-2016-0022.

[20] Rafał Ziobro. Application of complex classes to number theory. *Formalized Mathematics*, 33(1):207–216, 2025. doi:10.2478/forma-2025-0016.

Received June 12, 2025, Accepted December 21, 2025