

Elementary Number Theory Problems. Part XIX

Karol Pąk 
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper, we present formal solutions to twelve problems selected from Waław Sierpiński’s book *250 Problems in Elementary Number Theory*. The selected problems are: 108, 112–114, 118–119, 127, 129, 130, and 132–134 formalized in the Mizar system.

MSC: 11A41 11D72 68V20

Keywords: number theory; prime number

MML identifier: NUMBER19, version: 8.1.15 5.98.1507

INTRODUCTION

This article represents a further step in the formalization of problems from the collection *250 Problems in Elementary Number Theory* [17], [13]. In this study, we focus on twelve selected problems from Chapter 4: *Prime and Composite Numbers*.

We begin with Problem 108, which provides a method for determining whether a pair of numbers constitutes a pair of twin primes – that is, prime numbers that differ by exactly 2 [5]. The problem is stated as follows (Theorem 19): a pair of integers n and $n + 2$ are twin primes if and only if $(n - 1)!$ is not divisible by either n or $n + 2$. It should be noted that the assertion that there are infinitely many twin primes remains an open and unresolved problem in number theory [4], [7].

Next, we formalize Problems 112 and 113, which are formulated by indicating equations with only a finite number of solutions [11]. First, in Problem 112, we

consider the equation $p + 1 = n^s$ (see Theorem 22), where p is a prime number, n is a natural number, and s is a natural exponent satisfying the condition $2 \leq s \leq 10$. We demonstrate that there are precisely four solutions to this equation within this range: $\langle s, p \rangle = \langle 3, 5 \rangle, \langle 3, 7 \rangle, \langle 5, 31 \rangle$, and $\langle 7, 127 \rangle$, with $n = 2$ in all cases. The proof is carried out by analyzing all possible cases of s , given that it is straightforward to establish $n = 2$. The problem is naturally related to Mersenne primes [3], [1], since it amounts to examining primes of the form $2^n - 1$. Similarly, in Problem 113 we show (see Theorem 22) that the equation $(p - 1)! + 1 = p^m$ has no solutions when p is a prime number and m is a natural number, aside from the obvious cases of $p = 2, 3, 5$.

The expression $(p - 1)! + 1$ and its arithmetic properties are examined in Problem 114, with particular attention given to its divisibility. According to the classical Wilson's Theorem, the congruence $(p - 1)! + 1 \equiv 0 \pmod{p}$ holds if and only if p is prime. In Problem 114, we prove that there are infinitely many primes q for which there is a natural number $p < q$ such that $q | (p - 1)! + 1$. A solution originally presented in Sierpiński's book shows that the set of primes q is infinite, provided q is assumed to be prime (see Theorem 25). However, in our final formulation (see Theorem 26), we restate the result in its original version by removing the requirement that the corresponding number p must also be prime.

In Sections 6 and 7, we investigate Problems 118 and 119, which concern the construction of integers k such that either $k \cdot 2^n + 1$ or $2^n + k$ is composite for all positive integers n , respectively. In both cases, we prove that there are infinitely many such values of k . Following Sierpiński's approach, we focus on the properties of the initial Fermat numbers [6], [10], which are defined as $F_n = 2^{2^n} - 1$. In particular, we use the identity $F_0 \cdot F_1 \cdot \dots \cdot F_4 = 2^{32} - 1$ and the known factorization $F_5 = 641 \cdot 6700417$, and we consider the system of congruences

$$k \equiv 1 \pmod{(2^{32} - 1) \cdot 641}, \quad \text{and} \quad k \equiv -1 \pmod{6700417}. \quad (\text{I.1})$$

By the Chinese Remainder Theorem [15], [16], the system has infinitely many solutions k . The problem is finally solved by proving that $k \cdot 2^n$ is a composite number for every positive integer if k is greater than 6700417. Sierpiński modifies system (I.1) by adding $k \equiv 1 \pmod{2}$ to solve Problem 119, stating that the system has an infinite number of solutions $k > 6700417$, that $2^n + k$ is divisible by at least one of the six primes $F_0, F_1, \dots, F_4$ and 6700417. Although the smallest number satisfying system (I.1) and the condition $k \equiv 1 \pmod{2}$, namely

$$k = 15511380746462593381$$

is not divisible by any of those numbers (see Theorem 31), it is divisible by 641. Therefore, we modify the proposed solution to the problem by additionally taking into account the seventh prime divisor, 641.

In Problem 127, the focus is on polynomials that assign consecutive prime numbers to consecutive natural numbers. The initial segment of the problem posits the absence of a polynomial $f(x)$ with integer coefficients that satisfies the following conditions: $f(1) = 2$, $f(2) = 3$, and $f(3) = 5$. However, as demonstrated in Theorem 64, a contradiction already arises under the weaker assumption involving only two of these equalities, namely $f(1) = 2$ and $f(3) = 5$. In order to construct a polynomial $f_m(x)$ with rational coefficients satisfying the conditions $f_m(i) = p_i$ for all natural numbers $1 \leq i \leq m$, where p_i denotes the i^{th} prime number, it suffices to use the Lagrange interpolation polynomial of the form

$$f_m(x) = \sum_{i=1}^k p_i i \prod_{1 \leq j \leq k, j \neq i} \frac{x-j}{i-j}. \quad (\text{I.2})$$

Then, in Problem 129, the task is to identify a polynomial with integer coefficients such that $f_m(p_i) = p_i$ for $1 \leq i \leq m$ and f_m is a reducible polynomial, for a given natural m . We recall the definition of the reducible polynomial: namely, that it can be expressed as the product of two non-constant polynomials with integer coefficients. In accordance with Sierpiński's approach, it is demonstrated that the polynomial

$$f_m(x) = [(x - p_1)(x - p_2) \dots (x - p_m) + 1] x \quad (\text{I.3})$$

proposed by him possesses the desired properties. Problem 130 concerns the analysis of the set of prime numbers p satisfying the congruence $f(x) \equiv 0 \pmod{p}$. Here, f denotes a fixed, non-constant polynomial with integer coefficients. It is demonstrated that the set of primes for which this congruence has a solution is infinite.

The final three issues pertain to the maximum number of prime numbers that can be contained within an interval of n consecutive numbers commencing from $k + 1$, defined to be

$$\text{seg}(k, n) := \{k + 1, k + 2, k + 3, \dots, k + n\} \quad (\text{I.4})$$

The following equation is to be used: where k is any natural number, and $n = 100$ in Problems 132 and 133, while $n = 21$ is considered in Problem 134. The solution to this problem is based on calculating the total number of numbers in this interval which are not prime, with particular focus on those divisible by 2, 3, 5, 7, or 11. In the most challenging case, the proposed approach relies on the manual enumeration of divisible numbers "*it sufficient to write down all positive integers $\leq 2310 + 100$ divisible by 2, 3, 5, 7 or 11*" [17]. To avoid manual computation, we focus on the properties of intervals of a given length, which remain invariant under simultaneous translation of both endpoints. In

particular, the following equality holds:

$$\overline{\text{seq}(0, d) \cap M_{q_1} \cap M_{q_2} \cap \dots \cap M_{q_i}} = \overline{\text{seq}(n, d) \cap M_{q_1} \cap M_{q_2} \cap \dots \cap M_{q_i}} \quad (\text{I.5})$$

where n and d are natural numbers, $q_1, q_2, \dots, q_i$ are divisors of d , and M_q denotes the set of all multiples of a given number q .

We subsequently demonstrate that the set $\text{seq}(n, 100) \cap M_2 \cap M_3 \cap M_5$ comprises a minimum of 72 elements, with the value 72 exclusively manifesting for $n \equiv 9$ and $n \equiv 10 \pmod{30}$. Next, we extend the set of divisors to include 7, thereby demonstrating that $\text{seq}(n, 100) \cap M_2 \cap M_3 \cap M_5 \cap M_7$ contains at least 75 elements. This value is only attained for $n \equiv 9, 10, 99$ and $100 \pmod{210}$. Finally, we prove that $\text{seq}(n, 100) \cap M_2 \cap M_3 \cap M_5 \cap M_7 \cap M_{11}$ contains at least 76 elements. We use this to show in Problem 131 that the set $\text{seq}(n, 100)$ achieves the maximum number of prime numbers, 26, for $n = 1$ only. The value 25 (as stated in Problem 132) occurs in only six cases: $n = 0, 2, 3, 4, 9$ and 10 . Using analogous reasoning, we prove that the set $\text{seq}(n, 21)$ achieves the maximum number of prime numbers, i.e. 8, in only three cases: $n = 0, 1$ and 2 .

1. PRELIMINARIES

From now on $n, m, k, i, a, b, c, d, s$ denote natural numbers and p denotes a prime number.

Let f be a positive yielding, real-valued finite sequence. Let us observe that $\text{Rev}(f)$ is positive yielding.

Let n be a natural number. Let us note that $f|_n$ is positive yielding and $f \upharpoonright n$ is positive yielding.

Let n, m be natural numbers. Let us note that $\text{mid}(f, n, m)$ is positive yielding. Now we state the propositions:

- (1) Suppose $n \mid m$. Then the set of positive divisors of $n \subseteq$ the set of positive divisors of m .
- (2) Let us consider a non zero natural number m . If $p^n \mid m$, then $n + 1 \leq \overline{\alpha}$, where α is the set of positive divisors of m .

PROOF: Set $n_1 = n + 1$. Define $\mathcal{F}(\text{natural number}) = p^{\mathbb{N}}$. Consider f being a function such that $\text{dom } f = \mathbb{Z}_{n_1}$ and for every element d of $\mathbb{Z}_{n_1}$, $f(d) = \mathcal{F}(d)$. For every objects x_1, x_2 such that $x_1, x_2 \in \text{dom } f$ and $f(x_1) = f(x_2)$ holds $x_1 = x_2$. $\text{rng } f \subseteq \{p^k, \text{ where } k \text{ is an element of } \mathbb{N} : k \leq n\}$. $\text{rng } f \subseteq$ the set of positive divisors of $p^n \subseteq$ the set of positive divisors of m . $\square$

Let p be a prime number. Let us observe that $p - 1$ is non zero.

Now we state the propositions:

- (3) If $1 \leq k \leq m \leq n$, then $p \mid \prod \text{mid}(\text{primesFinS}(n), k, m)$ iff $k \leq 1 + \text{primeindex}(p) \leq m$.

PROOF: Set $M = \text{mid}(\text{primesFinS}(n), k, m)$. If $p \mid \prod M$, then $k \leq 1 + \text{primeindex}(p) \leq m$. $\square$

- (4) If $1 \leq k \leq m < n \leq a \leq b$, then $\prod \text{mid}(\text{primesFinS}(b), k, m)$ and $\prod \text{mid}(\text{primesFinS}(b), n, a)$ are relatively prime. The theorem is a consequence of (3).

- (5) Let us consider an integer-valued finite sequence u , a CR-sequence m , and an integer z . Suppose $z \equiv_{u(\cdot)} m(\cdot)$. If $i \in \text{dom } u$ and $u(i)$ and $m(i)$ are relatively prime, then z and $m(i)$ are relatively prime.

- (6) Let us consider an integer-valued finite sequence u , and a CR-sequence m . Suppose $\text{dom } u = \text{dom } m$. Let us consider a natural number z . Suppose $z \equiv_{u(\cdot)} m(\cdot)$ and for every i such that $i \in \text{dom } u$ holds $u(i)$ and $m(i)$ are relatively prime. Then z and $\prod m$ are relatively prime. The theorem is a consequence of (5).

Let f be a one-to-one finite sequence and n, m be natural numbers. One can check that $\text{mid}(f, n, m)$ is one-to-one.

Let us consider k, m , and n . Now we state the propositions:

- (7) If $1 \leq k \leq m \leq n$, then $\text{PrimeDivisors}(\prod \text{mid}(\text{primesFinS}(n), k, m)) = \text{rng } \text{mid}(\text{primesFinS}(n), k, m)$.

PROOF: Set $M = \text{mid}(\text{primesFinS}(n), k, m)$. $\text{PrimeDivisors}(\prod M) \subseteq \text{rng } M$. $\text{rng } M \subseteq \text{PrimeDivisors}(\prod M)$. $\square$

- (8) If $1 \leq k \leq m \leq n$, then $\overline{\text{PrimeDivisors}(\prod \text{mid}(\text{primesFinS}(n), k, m))} = m - k + 1$. The theorem is a consequence of (7).

- (9) $n < \text{pr}(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \$1 < \text{pr}(\$1)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n , $\mathcal{P}[n]$. $\square$

- (10) $\text{primeindex}(p) < p$. The theorem is a consequence of (9).

- (11) $\text{value}(n \mapsto 0, b) = 0$.

- (12) Suppose $b > 1$ and $k > 0$ and $n > 0$. Then $\text{value}(\langle \langle 1 \rangle \wedge (n -' 1 \mapsto 0) \rangle \wedge \text{digits}(k, b), b) = k \cdot b^n + 1$. The theorem is a consequence of (11).

- (13) Suppose $b > 1$ and $k > 0$ and $n > 0$. Then $\text{digits}(k \cdot b^n + 1, b) = \langle \langle 1 \rangle \wedge (n -' 1 \mapsto 0) \rangle \wedge \text{digits}(k, b)$.

PROOF: Set $N = \langle 1 \rangle \wedge (n -' 1 \mapsto 0)$. Set $D = \text{digits}(k, b)$. Set $N_1 = N \wedge D$. For every natural number i such that $i \in \text{dom } N_1$ holds $N_1(i) < b$. $\square$

- (14) Let us consider finite 0-sequences f, g , and a set X . Then $\overline{(f \wedge g)^{-1}(X)} = \overline{f^{-1}(X)} + \overline{g^{-1}(X)}$.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv \$_1$ is a natural number and for every natural number n such that $\$_1 = n$ holds $\$_2 = n + \text{len } f$. For every object x such that $x \in g^{-1}(X)$ there exists an object y such that $y \in ((f \cap g)^{-1}(X)) \setminus (\text{len } f)$ and $\mathcal{P}[x, y]$. Consider F being a function such that $\text{dom } F = g^{-1}(X)$ and $\text{rng } F \subseteq ((f \cap g)^{-1}(X)) \setminus (\text{len } f)$ and for every object x such that $x \in g^{-1}(X)$ holds $\mathcal{P}[x, F(x)]$. $((f \cap g)^{-1}(X)) \setminus (\text{len } f) \subseteq \text{rng } F$. For every objects x_1, x_2 such that $x_1, x_2 \in \text{dom } F$ and $F(x_1) = F(x_2)$ holds $x_1 = x_2$. $(f \cap g)^{-1}(X) \cap \text{len } f \subseteq f^{-1}(X)$. $f^{-1}(X) \subseteq (f \cap g)^{-1}(X) \cap \text{len } f$. $\square$

(15) If $b > 1$ and $k > 0$, then $\text{value}((n \mapsto b-1) \wedge \text{digits}(k-1, b), b) = k \cdot b^n - 1$.

(16) If $b > 1$ and $k > 0$ and $n > 0$, then $\sum \text{digits}(k \cdot b^n - 1, b) \geq n \cdot (b - 1)$.

The theorem is a consequence of (15).

2. PROBLEM 108

Let us consider an odd, natural number n . Now we state the propositions:

(17) If $n > 1$, then n is prime iff $n \nmid (n-1)!$.

PROOF: If n is prime, then $n \nmid (n-1)!$. Consider k being a natural number such that $n = 2 \cdot k + 1$. $\square$

(18) If $n > 1$, then $n + 2$ is prime iff $n + 2 \nmid (n-1)!$.

PROOF: If $n + 2$ is prime, then $n + 2 \nmid (n-1)!$. Consider k being a natural number such that $n = 2 \cdot k + 1$. $\square$

(19) If $n > 1$, then n is prime and $n + 2$ is prime iff $n \nmid (n-1)!$ and $n + 2 \nmid (n-1)!$.

3. PROBLEM 112

Now we state the propositions:

(20) If $\sum \text{CFS}(\text{the set of positive divisors of } p) = n^s$ and $2 \leq s$, then $n = 2$.

(21) Let us consider a prime number p , and natural numbers n, s . Suppose $\sum \text{CFS}(\text{the set of positive divisors of } p) = n^s$ and $2 \leq s \leq 10$. Then

(i) $s = 2$ and $p = 3$, or

(ii) $s = 3$ and $p = 7$, or

(iii) $s = 5$ and $p = 31$, or

(iv) $s = 7$ and $p = 127$.

The theorem is a consequence of (20).

4. PROBLEM 113

Now we state the proposition:

- (22) If $p > 5$, then $(p - '1)! + 1 \neq p^m$.

PROOF: Consider k being a natural number such that $p = 2 \cdot k + 1$. $(p - '1) \cdot (p - '1) \mid (p - '1)!$ by [14, (37)]. $m > 0$. Consider t being a natural number such that $p^m - '1 = (p - '1) \cdot t$ by [12, (11)]. $p - '1 \mid m$. $p^m > (p - '1)! + 1$. $\square$

5. PROBLEM 114

Now we state the propositions:

- (23) If $p > 5$, then there exists a prime number q such that $p < q$ and $q \mid (p - '1)! + 1$.

PROOF: Consider k, m being natural numbers such that $(p - '1)! + 1 = m \cdot p^k$ and $p \nmid m$. $m \geq 1 + 1$. Consider q being an element of $\mathbb{N}$ such that q is prime and $q \mid m$. $q > p - '1$. $\square$

- (24) Let us consider natural numbers n, k . If $0 < n < k$, then $n! < k!$.

- (25) $\{q, \text{ where } q \text{ is a prime number : there exists a prime number } p \text{ such that } p < q \mid (p - '1)! + 1\}$ is infinite.

PROOF: Define $\mathcal{G}(\text{object}, \text{natural number}) = (\text{pr}(\$2!)) \in \mathbb{N}$. Consider f being a sequence of $\mathbb{N}$ such that $f(0) = 7$ and for every natural number k , $f(k + 1) = \mathcal{G}(k, f(k))$. Define $\mathcal{P}[\text{natural number}] \equiv f(\$1)$ is a prime number and $5 < f(\$1)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [2, (11)]. For every natural number n , $\mathcal{P}[n]$. For every natural numbers i, j such that $i \leq j$ holds $f(i) \leq f(j)$. Define $\mathcal{F}[\text{object}, \text{object}] \equiv \2 is a prime number and for every natural numbers i, j such that $\$1 = i$ and $\$2 = j$ holds j is prime and $f(i) < j \mid (f(i) - '1)! + 1$. For every object x such that $x \in \mathbb{N}$ there exists an object y such that $y \in \mathbb{N}$ and $\mathcal{F}[x, y]$. Consider F being a function such that $\text{dom } F = \mathbb{N}$ and $\text{rng } F \subseteq \mathbb{N}$ and for every object x such that $x \in \mathbb{N}$ holds $\mathcal{F}[x, F(x)]$. For every objects x_1, x_2 such that $x_1, x_2 \in \text{dom } F$ and $F(x_1) = F(x_2)$ holds $x_1 = x_2$. $\text{rng } F \subseteq \{q, \text{ where } q \text{ is a prime number : there exists a prime number } p \text{ such that } p < q \mid (p - '1)! + 1\}$. $\square$

- (26) $\{q, \text{ where } q \text{ is a prime number : there exists a natural number } n \text{ such that } n < q \text{ and } q \mid (n - '1)! + 1\}$ is infinite. The theorem is a consequence of (25).

6. PROBLEM 118

Now we state the propositions:

- (27) (i) Fermat $5 = 2^{32} + 1 = 641 \cdot 6700417$, and
 (ii) $6700417 > \text{Fermat } 4$.
- (28) $(2^{32} - 1) \cdot 641$ and 6700417 are relatively prime. The theorem is a consequence of (27).
- (29) Let us consider a natural number k . Suppose $k \equiv 1 \pmod{(2^{32} - 1) \cdot 641}$ and $k \equiv -1 \pmod{6700417}$ and $k > 6700417$. Let us consider a positive natural number n . Then
- (i) $k \cdot 2^n + 1$ is composite, and
 (ii) Fermat $0 \mid k \cdot 2^n + 1$ or ... or Fermat $4 \mid k \cdot 2^n + 1$ or $641 \mid k \cdot 2^n + 1$ or $6700417 \mid k \cdot 2^n + 1$.

The theorem is a consequence of (27).

- (30) There exists a natural number c_1 such that
- (i) $6700417 < c_1 < 2 \cdot (2^{64} - 1)$, and
 (ii) for every natural number n , $c_1 + n \cdot 2 \cdot (2^{64} - 1) \equiv 1 \pmod{(2^{32} - 1) \cdot 641}$ and $c_1 + n \cdot 2 \cdot (2^{64} - 1) \equiv -1 \pmod{6700417}$ and $c_1 + n \cdot 2 \cdot (2^{64} - 1) \equiv 1 \pmod{2}$.

PROOF: Set $P_1 = (2^{32} - 1) \cdot 641$. Set $P_2 = 6700417$. Set $P_3 = 2$. Set $P_5 = \langle P_1, P_2, P_3 \rangle$. For every natural numbers i, j such that $i, j \in \text{dom } P_5$ and $i < j$ holds $P_5(i)$ and $P_5(j)$ are relatively prime. For every natural numbers i, j such that $i, j \in \text{dom } P_5$ and $i \neq j$ holds $P_5(i)$ and $P_5(j)$ are relatively prime. $6700417 < c_1$. $\square$

- (31) $\{k, \text{ where } k \text{ is a natural number : for every positive natural number } n, k \cdot 2^n + 1 \text{ is composite}\}$ is infinite. The theorem is a consequence of (30), (27), and (29).

7. PROBLEM 119

Now we state the proposition:

- (32) Let us consider a natural number k . Suppose $k = 15 \cdot 1000000000 \cdot 1000000000 + 511380746 \cdot 1000000000 + 462593381$. Then
- (i) $k > 6700417$, and
 (ii) $k \equiv 1 \pmod{(2^{32} - 1) \cdot 641}$, and
 (iii) $k \equiv -1 \pmod{6700417}$, and

- (iv) $k \equiv 1 \pmod{2}$, and
- (v) Fermat $0 \nmid k \cdot 2^{2^5} + 1$ and ... and Fermat $4 \nmid k \cdot 2^{2^5} + 1$, and
- (vi) $6700417 \nmid k \cdot 2^{2^5} + 1$, and
- (vii) $641 \mid k \cdot 2^{2^5} + 1$.

The theorem is a consequence of (27).

Let n be a natural number. One can check that Fermat n is odd.

Now we state the propositions:

- (33) Let us consider non zero natural numbers n , m , and p . If $p^n \mid m$, then Euler $p^n \leq \text{Euler } m$.
- (34) Suppose $k \equiv 1 \pmod{(2^{32} - 1) \cdot 641}$ and $k \equiv -1 \pmod{6700417}$ and $k > 6700417$. Let us consider a positive natural number n . Then
 - (i) $k + 2^n$ is composite, and
 - (ii) Fermat $0 \mid k + 2^n$ or ... or Fermat $4 \mid k + 2^n$ or $641 \mid k + 2^n$ or $6700417 \mid k + 2^n$.

PROOF: Set $Q = (\text{Fermat } 0) \cdot (\text{Fermat } 1) \cdot (\text{Fermat } 2) \cdot (\text{Fermat } 3) \cdot (\text{Fermat } 4) \cdot (\text{Fermat } 5)$. 2 and Q are relatively prime by [8, (64)]. $2 < \text{Fermat } 5$ and $1 \leq (\text{Fermat } 0) \cdot (\text{Fermat } 1) \cdot (\text{Fermat } 2) \cdot (\text{Fermat } 3) \cdot (\text{Fermat } 4)$. Set $e = n \cdot (\text{Euler } Q - 1)$. Euler $Q > 1$. $k \cdot 2^e + 1$ is composite and Fermat $0 \mid k \cdot 2^e + 1$ or ... or Fermat $4 \mid k \cdot 2^e + 1$ or $641 \mid k \cdot 2^e + 1$ or $6700417 \mid k \cdot 2^e + 1$. Consider q being a natural number such that $q \mid k \cdot 2^e + 1$ and $q = \text{Fermat } 0$ or $q = \text{Fermat } 1$ or $q = \text{Fermat } 2$ or $q = \text{Fermat } 3$ or $q = \text{Fermat } 4$ or $q = 641$ or $q = 6700417$. $2^{\text{Euler } Q} \equiv 1 \pmod{q}$ and $k > q > 1$. $\square$

- (35) $\{k, \text{ where } k \text{ is a natural number : for every positive natural number } n, 2^n + k \text{ is composite}\}$ is infinite. The theorem is a consequence of (30), (27), and (34).

8. LAGRANGE BASIS AND INTERPOLATING POLYNOMIALS

Let us consider a non empty zero structure L and a polynomial p over L . Now we state the propositions:

- (36) If $\text{len } p = 1$, then $p = \langle p(0) \rangle$.

PROOF: For every natural number k such that $k < \text{len } p$ holds $p(k) = \langle p(0) \rangle(k)$. $\square$

- (37) If $\text{len } p = 2$, then $p = \langle p(0), p(1) \rangle$.

PROOF: For every natural number k such that $k < \text{len } p$ holds $p(k) = \langle p(0), p(1) \rangle(k)$. $\square$

- (38) Let us consider a ring R , an element x of R , and a polynomial p over R . Then $\text{ExtEval}(p, x) = \text{eval}(p, x)$.
- (39) Let us consider rings R, S . Suppose S is a subring of R . Let us consider a polynomial p over R , an element x of R , a polynomial q over S , and an element y of S . If $p = q$ and $x = y$, then $\text{eval}(p, x) = \text{eval}(q, y)$. The theorem is a consequence of (38).
- (40) Let us consider a field R , a polynomial p over R , and an element a of R . Suppose a is a root of p . Then $p = (p \text{ div } \text{rpoly}(1, a)) * \text{rpoly}(1, a)$.
- (41) Let us consider a non empty commutative ring R , and a ring S . Suppose S is a subring of R . Let us consider polynomials p, q over R . Suppose p is a polynomial over S . Let us consider an element a of R , and an element b of S . Suppose $a = b$ and b is left invertible and $p = q * \text{rpoly}(1, a)$. Then q is a polynomial over S .

PROOF: Reconsider $S_1 = S$ as a subring of R . Reconsider $b = c$ as an element of S_1 . Consider y_1 being an element of S_1 such that $y_1 \cdot b = 1_{S_1}$. Define $\mathcal{P}[\text{natural number}] \equiv q(\$_1) \in \text{the carrier of } S_1. \mathcal{P}[0]$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$. For every natural number i , $\mathcal{P}[i]. \text{rng } q \subseteq \text{the carrier of } S$. Reconsider $q_1 = q$ as a sequence of S . q_1 is finite-Support. $\square$

From now on L denotes a unital, add-associative, right zeroed, right complementable, distributive, non empty double loop structure.

Let us consider L . Let z be a finite sequence of elements of the carrier of L and f be a $\mathbb{N}$ -valued finite sequence. The functor $\text{rpoly}(f, z)$ yielding a finite sequence of elements of the carrier of Polynom-Ring L is defined by

- (Def. 1) $\text{len } it = \text{len } f$ and for every natural number i such that $1 \leq i \leq \text{len } f$ holds $it(i) = \text{rpoly}(f/i, z/i)$.

Now we state the propositions:

- (42) Let us consider finite sequences z_1, z_2 of elements of the carrier of L , and $\mathbb{N}$ -valued finite sequences f_1, f_2 . Suppose $\text{len } f_1 = \text{len } z_1$ and $\text{len } f_2 \leq \text{len } z_2$. Then $\text{rpoly}(f_1 \frown f_2, z_1 \frown z_2) = \text{rpoly}(f_1, z_1) \frown \text{rpoly}(f_2, z_2)$.
PROOF: For every natural number i such that $1 \leq i \leq \text{len } \text{rpoly}(f_1 \frown f_2, z_1 \frown z_2)$ holds $(\text{rpoly}(f_1 \frown f_2, z_1 \frown z_2))(i) = (\text{rpoly}(f_1, z_1) \frown \text{rpoly}(f_2, z_2))(i)$. $\square$
- (43) Let us consider an element z of the carrier of L , and an element k of $\mathbb{N}$. Then $\text{rpoly}(\langle k \rangle, \langle z \rangle) = \langle \text{rpoly}(k, z) \rangle$.
- (44) Let us consider finite sequences z_1, z_2 of elements of the carrier of L , and a $\mathbb{N}$ -valued finite sequence f . Suppose $\text{len } f \leq \text{len } z_1$ and $\text{len } f \leq \text{len } z_2$ and $z_1 \upharpoonright \text{len } f = z_2 \upharpoonright \text{len } f$. Then $\text{rpoly}(f, z_1) = \text{rpoly}(f, z_2)$.
PROOF: For every natural number i such that $1 \leq i \leq \text{len } f$ holds $(\text{rpoly}(f, z_1))(i) = (\text{rpoly}(f, z_2))(i)$. $\square$

- (45) Let us consider a finite sequence z of elements of the carrier of L , a $\mathbb{N}$ -valued finite sequence f , and a natural number n . Suppose $n < \text{len } f$. Then $\text{rpoly}(f \upharpoonright (n+1), z) = \text{rpoly}(f \upharpoonright n, z) \cap \langle \text{rpoly}(f_{/n+1}, z_{/n+1}) \rangle$.

PROOF: For every natural number i such that $1 \leq i \leq n+1$ holds $(\text{rpoly}(f \upharpoonright (n+1), z))(i) = (\text{rpoly}(f \upharpoonright n, z) \cap \langle \text{rpoly}(f_{/n+1}, z_{/n+1}) \rangle)(i)$. $\square$

- (46) Let us consider a finite sequence z of elements of the carrier of L , and a $\mathbb{N}$ -valued finite sequence f . Suppose $\text{len } f = \text{len } z$. Let us consider a permutation p of $\text{dom } f$, and a finite sequence z_3 of elements of the carrier of L . Suppose $z_3 = z \cdot p$. Then $\text{rpoly}(f \cdot p, z_3) = (\text{rpoly}(f, z)) \cdot p$.

PROOF: For every object x such that $x \in \text{dom } f$ holds $(\text{rpoly}(f \cdot p, z_3))(x) = ((\text{rpoly}(f, z)) \cdot p)(x)$. $\square$

- (47) Let us consider a commutative ring L , a finite sequence z of elements of the carrier of L , and a $\mathbb{N}$ -valued finite sequence f . Suppose $\text{len } f = \text{len } z$. Let us consider a permutation p of $\text{dom } f$, and a finite sequence z_3 of elements of the carrier of L . Suppose $z_3 = z \cdot p$. Then $\prod \text{rpoly}(f, z) = \prod \text{rpoly}(f \cdot p, z_3)$. The theorem is a consequence of (46).

- (48) Let us consider a non degenerated, integral domain-like ring L , a finite sequence z of elements of the carrier of L , and a $\mathbb{N}$ -valued finite sequence f . Then $\deg(\text{R2P}(\prod \text{rpoly}(f, z))) = \sum f$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \leq \text{len } f$, then $\text{R2P}(\prod \text{rpoly}(f \upharpoonright \$1, z)) \neq \mathbf{0}.L$ and $\deg(\text{R2P}(\prod \text{rpoly}(f \upharpoonright \$1, z))) = \sum(f \upharpoonright \$1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i , $\mathcal{P}[i]$. $\square$

- (49) Let us consider a non degenerated commutative ring L , a finite sequence z of elements of the carrier of L , a $\mathbb{N}$ -valued finite sequence f , and an element x of the carrier of L . Then there exists a finite sequence e of elements of the carrier of L such that

(i) $\text{eval}(\text{R2P}(\prod \text{rpoly}(f, z)), x) = \prod e$, and

(ii) $\text{len } e = \text{len } f$, and

(iii) for every i such that $1 \leq i \leq \text{len } e$ holds $e(i) = \text{eval}(\text{rpoly}(f_{/i}, z_{/i}), x)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \leq \text{len } f$, then there exists a finite sequence e of elements of the carrier of L such that $\text{eval}(\text{R2P}(\prod \text{rpoly}(f \upharpoonright \$1, z)), x) = \prod e$ and $\text{len } e = \$1$ and for every natural number i such that $1 \leq i \leq \text{len } e$ holds $e(i) = \text{eval}(\text{rpoly}(f_{/i}, z_{/i}), x)$. $\mathcal{P}[0]$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i , $\mathcal{P}[i]$. $\square$

- (50) Let us consider a non degenerated commutative ring L , a finite sequence z of elements of the carrier of L , a $\mathbb{N}$ -valued finite sequence f , and i . Suppose $i \in \text{dom } f$ and $f(i) \neq 0$. Then $z_{/i}$ is a root of $\text{R2P}(\prod \text{rpoly}(f, z))$.

PROOF: Consider e being a finite sequence of elements of the carrier of L such that $\text{eval}(\text{R2P}(\prod \text{rpoly}(f, z)), z_{/i}) = \prod e$ and $\text{len } e = \text{len } f$ and for every natural number j such that $1 \leq j \leq \text{len } e$ holds $e(j) = \text{eval}(\text{rpoly}(f_{/j}, z_{/j}), z_{/i})$. $\text{eval}(\text{rpoly}(f_{/i}, z_{/i}), z_{/i}) = 0_L$. $\square$

- (51) Let us consider an integral domain L , a finite sequence z of elements of the carrier of L , a $\mathbb{N}$ -valued finite sequence f , and an element x of the carrier of L . Then x is a root of $\text{R2P}(\prod \text{rpoly}(f, z))$ if and only if there exists a natural number i such that $i \in \text{dom } f$ and x is a root of $\text{rpoly}(f_{/i}, z_{/i})$.

PROOF: Consider e being a finite sequence of elements of the carrier of L such that $\text{eval}(\text{R2P}(\prod \text{rpoly}(f, z)), x) = \prod e$ and $\text{len } e = \text{len } f$ and for every natural number i such that $1 \leq i \leq \text{len } e$ holds $e(i) = \text{eval}(\text{rpoly}(f_{/i}, z_{/i}), x)$. If x is a root of $\text{R2P}(\prod \text{rpoly}(f, z))$, then there exists a natural number i such that $i \in \text{dom } f$ and x is a root of $\text{rpoly}(f_{/i}, z_{/i})$. $\square$

- (52) Let us consider an integral domain L , and a finite sequence z of elements of the carrier of L . Then $\text{Roots}(\text{R2P}(\prod \text{rpoly}(\text{len } z \mapsto 1, z))) = \text{rng } z$.

PROOF: $\text{Roots}(\text{R2P}(\prod \text{rpoly}(\text{len } z \mapsto 1, z))) \subseteq \text{rng } z$.

$\text{rng } z \subseteq \text{Roots}(\text{R2P}(\prod \text{rpoly}(\text{len } z \mapsto 1, z)))$. $\square$

Let F be a field, X be a finite subset of F , and x be an element of F . The functor $\text{LagBPoly}(X, x)$ yielding a polynomial over F is defined by

- (Def. 2) for every one-to-one finite sequence z of elements of the carrier of F such that $\text{rng } z = X$ holds $it = (\text{eval}(\text{R2P}(\prod \text{rpoly}(\text{len } z \mapsto 1, z)), x))^{-1} \cdot (\text{R2P}(\prod \text{rpoly}(\text{len } z \mapsto 1, z)))$.

In the sequel F denotes a field. Now we state the propositions:

- (53) Let us consider a finite subset X of F , and an element x of F . Suppose $x \notin X$. Then
- (i) $\text{Roots}(\text{LagBPoly}(X, x)) = X$, and
 - (ii) $\text{eval}(\text{LagBPoly}(X, x), x) = 1_F$, and
 - (iii) $\text{deg}(\text{LagBPoly}(X, x)) = \overline{\overline{X}}$.

The theorem is a consequence of (52) and (48).

- (54) Let us consider elements x, y of F . Then $\text{LagBPoly}(\{y\}, x) = (x - y)^{-1} \cdot (\text{rpoly}(1, y))$. The theorem is a consequence of (43).
- (55) Let us consider finite subsets X_1, X_2 of F , and an element x of F . Suppose $x \notin X_1$ and $x \notin X_2$ and X_1 misses X_2 . Then $\text{LagBPoly}(X_1, x) * \text{LagBPoly}(X_2, x) = \text{LagBPoly}(X_1 \cup X_2, x)$. The theorem is a consequence of (52) and (42).

Let F be a field and x, y be finite sequences of elements of the carrier of F . The functor $\text{LagPoly}(x, y)$ yielding a polynomial over F is defined by

(Def. 3) there exists a finite sequence L of elements of the carrier of Polynom-Ring F such that $it = \sum L$ and $\text{len } L = \text{len } x$ and for every natural number i such that $1 \leq i \leq \text{len } x$ holds $L(i) = y_{/i} \cdot (\text{LagBPoly}((\text{rng } x) \setminus \{x_{/i}\}, x_{/i}))$.

Now we state the propositions:

(56) Let us consider finite sequences x, y of elements of the carrier of F , and a natural number i . Then

- (i) if $y_{/i} \neq 0_F$, then $\text{Roots}(y_{/i} \cdot (\text{LagBPoly}((\text{rng } x) \setminus \{x_{/i}\}, x_{/i}))) = (\text{rng } x) \setminus \{x_{/i}\}$, and
- (ii) $\text{eval}(y_{/i} \cdot (\text{LagBPoly}((\text{rng } x) \setminus \{x_{/i}\}, x_{/i})), x_{/i}) = y_{/i}$, and
- (iii) if $i \in \text{dom } x$ and $y_{/i} \neq 0_F$,
then $\deg(y_{/i} \cdot (\text{LagBPoly}((\text{rng } x) \setminus \{x_{/i}\}, x_{/i}))) = \overline{\text{rng } x} - 1$.

PROOF: Set $R_2 = (\text{rng } x) \setminus \{x_{/i}\}$.

If $y_{/i} \neq 0_F$, then $\text{Roots}(y_{/i} \cdot (\text{LagBPoly}(R_2, x_{/i}))) = R_2$. $\square$

(57) Let us consider finite sequences x, y of elements of the carrier of F . Then $\deg(\text{LagPoly}(x, y)) \leq \text{len } x - 1$.

PROOF: Consider L being a finite sequence of elements of the carrier of Polynom-Ring F such that $\text{LagPoly}(x, y) = \sum L$ and $\text{len } L = \text{len } x$ and for every natural number i such that $1 \leq i \leq \text{len } x$ holds $L(i) = y_{/i} \cdot (\text{LagBPoly}((\text{rng } x) \setminus \{x_{/i}\}, x_{/i}))$.

Consider f being a sequence of Polynom-Ring F such that $\sum L = f(\text{len } L)$ and $f(0) = 0_{\text{Polynom-Ring } F}$ and for every natural number j and for every element v of Polynom-Ring F such that $j < \text{len } L$ and $v = L(j+1)$ holds $f(j+1) = f(j) + v$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 \leq \text{len } L$, then $\deg(\text{R2P}(f(\$1))) \leq \text{len } x - 1$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n , $\mathcal{P}[n]$. $\square$

(58) Let us consider finite sequences x, y of elements of the carrier of F . Suppose x is one-to-one. Let us consider a natural number i . Suppose $i \in \text{dom } x$. Then $\text{eval}(\text{LagPoly}(x, y), x_{/i}) = y_{/i}$.

PROOF: Consider L being a finite sequence of elements of the carrier of Polynom-Ring F such that $\text{LagPoly}(x, y) = \sum L$ and $\text{len } L = \text{len } x$ and for every natural number i such that $1 \leq i \leq \text{len } x$ holds $L(i) = y_{/i} \cdot (\text{LagBPoly}((\text{rng } x) \setminus \{x_{/i}\}, x_{/i}))$.

Consider f being a sequence of Polynom-Ring F such that $\sum L = f(\text{len } L)$ and $f(0) = 0_{\text{Polynom-Ring } F}$ and for every natural number j and for every element v of Polynom-Ring F such that $j < \text{len } L$ and $v = L(j+1)$ holds $f(j+1) = f(j) + v$. For every natural number n such that $n+1 \leq \text{len } x$ and $n+1 \neq i$ holds $\text{eval}(\text{R2P}(f(n)), x_{/i}) = \text{eval}(\text{R2P}(f(n+1)), x_{/i})$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 < i$, then $\text{eval}(\text{R2P}(f(\$1)), x_{/i}) = 0_F$. For every

natural number n , $\mathcal{P}[n]$. Define $\mathcal{Q}[\text{natural number}] \equiv$ if $i \leq \$1 \leq \text{len } x$, then $\text{eval}(\text{R2P}(f(\$1)), x_{/i}) = y_{/i}$. For every natural number n such that $\mathcal{Q}[n]$ holds $\mathcal{Q}[n+1]$. For every natural number n , $\mathcal{Q}[n]$. $\square$

Let F be a unital, add-associative, right zeroed, right complementable, distributive, non empty double loop structure, z be a finite sequence of elements of the carrier of F , and i be a natural number. The functor $\text{LagIPoly}(z, i)$ yielding a polynomial over F is defined by the term

(Def. 4) $\prod \text{rpoly}(\text{len } z_{\upharpoonright i} \mapsto 1, z_{\upharpoonright i})$.

Now we state the propositions:

(59) Let us consider a finite sequence z of elements of the carrier of L , and a natural number i . Suppose $i \notin \text{dom } z$.

Then $\text{LagIPoly}(z, i) = \prod \text{rpoly}(\text{len } z \mapsto 1, z)$.

(60) Let us consider a finite sequence z , and a natural number i . Suppose z is one-to-one at i . Then $\text{rng } z_{\upharpoonright i} = (\text{rng } z) \setminus \{z(i)\}$.

PROOF: $z(i) \notin \text{rng } z_{\upharpoonright i}$. $(\text{rng } z) \setminus \{z(i)\} \subseteq \text{rng } z_{\upharpoonright i}$. $\square$

(61) Let us consider a finite sequence z of elements of the carrier of F , and a natural number i . Suppose $i \in \text{dom } z$ and z is one-to-one. Then $\text{LagBPoly}((\text{rng } z) \setminus \{z(i)\}, z_{/i}) = (\text{eval}(\text{LagIPoly}(z, i), z_{/i}))^{-1} \cdot (\text{LagIPoly}(z, i))$. The theorem is a consequence of (60).

(62) Let us consider natural numbers n, k . Suppose $1 \leq k \leq n$. Let us consider a finite sequence z of elements of $\mathbb{Z}^R$. Suppose $z = \text{idseq}(n)$. Then

(i) $\text{eval}(\text{LagIPoly}(z, k), k(\in \mathbb{Z}^R)) = (-1)^{n-k} \cdot (n-k)! \cdot (k-1)!$, and

(ii) for every natural number i such that $1 \leq i \leq n$ and $i \neq k$ holds $i(\in \mathbb{Z}^R)$ is a root of $\text{LagIPoly}(z, k)$.

PROOF: Set $D = z_{\upharpoonright k}$. Consider e being a finite sequence of elements of the carrier of $\mathbb{Z}^R$ such that $\text{eval}(\text{LagIPoly}(z, k), k(\in \mathbb{Z}^R)) = \prod e$ and $\text{len } e = \text{len}(\text{len } D \mapsto 1)$ and for every natural number i such that $1 \leq i \leq \text{len } e$ holds $e(i) = \text{eval}(\text{rpoly}((\text{len } D \mapsto 1)_{/i}, D_{/i}), k(\in \mathbb{Z}^R))$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 < k$, then $\prod(e \upharpoonright \$1) = \frac{(k-1)!}{(k-1-\$1)!}$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i , $\mathcal{P}[i]$. Define $\mathcal{H}[\text{natural number}] \equiv$ if $k \leq \$1 < n$, then $\prod(e \upharpoonright \$1) = (-1)^{\$1+1-k} \cdot (\$1+1-k)! \cdot (k-1)!$. For every natural number i such that $\mathcal{H}[i]$ holds $\mathcal{H}[i+1]$. For every natural number i , $\mathcal{H}[i]$. $\text{eval}(\text{LagIPoly}(z, k), k(\in \mathbb{Z}^R)) = (-1)^{n-k} \cdot (n-k)! \cdot (k-1)!$. $\square$

(63) Let us consider a natural number n , and an n -element finite sequence y of elements of $\mathbb{Z}$. Then there exists a polynomial p over $\mathbb{Z}^R$ such that for every natural number k such that $1 \leq k \leq n$ holds $\text{eval}(p, k(\in \mathbb{Z}^R)) = 1 + (k-1)! \cdot (n-k)! \cdot y(k)$.

PROOF: Reconsider $z = \text{idseq}(n)$ as a finite sequence of elements of $\mathbb{Z}^{\mathbb{R}}$. Define $\mathcal{L}(\text{natural number}) = (-1)^{n-\$1} \cdot y(\$1)(\in \mathbb{Z}^{\mathbb{R}}) \cdot (\text{LagIPoly}(z, \$1))$. Consider L being a finite sequence such that $\text{len } L = n$ and for every natural number k such that $k \in \text{dom } L$ holds $L(k) = \mathcal{L}(k)$. $\text{rng } L \subseteq$ the carrier of $\text{Polynom-Ring } \mathbb{Z}^{\mathbb{R}}$. Consider f being a sequence of $\text{Polynom-Ring } \mathbb{Z}^{\mathbb{R}}$ such that $\sum L = f(\text{len } L)$ and $f(0) = 0_{\text{Polynom-Ring } \mathbb{Z}^{\mathbb{R}}}$ and for every natural number j and for every element v of $\text{Polynom-Ring } \mathbb{Z}^{\mathbb{R}}$ such that $j < \text{len } L$ and $v = L(j+1)$ holds $f(j+1) = f(j) + v$. For every natural number w such that $w+1 \leq \text{len } z$ and $w+1 \neq k$ holds $\text{eval}(\text{R2P}(f(w)), z_{/k}) = \text{eval}(\text{R2P}(f(w+1)), z_{/k})$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 < k$, then $\text{eval}(\text{R2P}(f(\$1)), z_{/k}) = 0_{\mathbb{Z}^{\mathbb{R}}}$. For every natural number i , $\mathcal{P}[i]$. Define $\mathcal{Q}[\text{natural number}] \equiv$ if $k \leq \$1 \leq \text{len } z$, then $\text{eval}(\text{R2P}(f(\$1)), z_{/k}) = (n -' k)! \cdot (k -' 1)! \cdot y(k)$. For every natural number i such that $\mathcal{Q}[i]$ holds $\mathcal{Q}[i+1]$. For every natural number n , $\mathcal{Q}[n]$. $\square$

Let i be a rational number. Let us note that $i(\in \mathbb{F}_{\mathbb{Q}})$ reduces to i .

9. PROBLEM 127

Now we state the propositions:

- (64) There exists no polynomial p over $\mathbb{Z}^{\mathbb{R}}$ such that $\text{eval}(p, 1(\in \mathbb{Z}^{\mathbb{R}})) = 2$ and $\text{eval}(p, 3(\in \mathbb{Z}^{\mathbb{R}})) = 5$. The theorem is a consequence of (39), (40), and (41).
- (65) Let us consider a natural number n , and finite sequences i, z of elements of the carrier of $\mathbb{F}_{\mathbb{Q}}$. Suppose $i = \text{idseq}(n)$ and $z = \text{primesFinS}(n)$. Let us consider a natural number k . Suppose $k < n$. Then $\text{eval}(\text{LagPoly}(i, z), (k+1)(\in \mathbb{F}_{\mathbb{Q}})) = \text{pr}(k)$. The theorem is a consequence of (58).

10. PROBLEM 129

Now we state the proposition:

- (66) Let us consider a natural number n . Then there exist polynomials p, q over $\mathbb{Z}^{\mathbb{R}}$ such that
- (i) $\text{degree}(p) > 0$, and
 - (ii) $\text{degree}(q) > 0$, and
 - (iii) for every natural number i such that $i \leq n$ holds $\text{eval}(p * q, (\text{pr}(i))(\in \mathbb{Z}^{\mathbb{R}})) = \text{pr}(i)$.

The theorem is a consequence of (48) and (50).

11. PROBLEM 130

Now we state the propositions:

- (67) Let us consider a unital, well unital, non degenerated, non empty multiplicative loop with zero structure L . Suppose L is integral domain-like. Let us consider an element x of L , and a natural number i . If $\text{power}_L(x, i) = 0_L$, then $x = 0_L$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\text{power}_L(x, \$1) = 0_L$, then $x = 0_L$. For every i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$. For every i , $\mathcal{P}[i]$. $\square$

- (68) Let us consider an integral domain-like, commutative, non degenerated, associative, add-associative, right zeroed, right complementable, distributive, Abelian, well unital, unital, non empty double loop structure L , and a polynomial p over L . Suppose $p(0) \neq 0_L$. Then there exists a polynomial q over L such that

- (i) $\text{len } p = \text{len } q$, and
- (ii) $q(0) = 1_L$, and
- (iii) for every element i of $\mathbb{N}$ such that $0 < i$ holds
 $q(i) = p(i) \cdot \text{power}_L(p(0), i -' 1)$, and
- (iv) for every element x of L , $\text{eval}(p, p(0) \cdot x) = p(0) \cdot (\text{eval}(q, x))$.

PROOF: Define $\mathcal{Q}[\text{element of } \mathbb{N}, \text{object}] \equiv$ if $\$1 = 0$, then $\$2 = 1_L$ and if $\$1 > 0$, then $\$2 = p(\$1) \cdot \text{power}_L(p(0), \$1 -' 1)$. For every element x of $\mathbb{N}$, there exists an element y of L such that $\mathcal{Q}[x, y]$. Consider q being a sequence of L such that for every element n of $\mathbb{N}$, $\mathcal{Q}[n, q(n)]$. For every natural number m such that the length of q is at most m holds $\text{len } p \leq m$. Consider P being a finite sequence of elements of the carrier of L such that $\text{eval}(p, p(0) \cdot x) = \sum P$ and $\text{len } P = \text{len } p$ and for every element n of $\mathbb{N}$ such that $n \in \text{dom } P$ holds $P(n) = p(n -' 1) \cdot \text{power}_L(p(0) \cdot x, n -' 1)$. Consider Q being a finite sequence of elements of the carrier of L such that $\text{eval}(q, x) = \sum Q$ and $\text{len } Q = \text{len } q$ and for every element n of $\mathbb{N}$ such that $n \in \text{dom } Q$ holds $Q(n) = q(n -' 1) \cdot \text{power}_L(x, n -' 1)$. For every natural number k such that $k \in \text{dom } P$ holds $P(k) = (p(0) \cdot Q)(k)$. $\square$

- (69) Let us consider a unital, well unital, Abelian, add-associative, right zeroed, right complementable, left distributive, associative, non empty double loop structure L , a polynomial p over L , and an element x of L . Then there exists an element d of L such that $\text{eval}(p, x) = d \cdot x + p(0)$.

PROOF: Consider F being a finite sequence of elements of the carrier of L such that $\text{eval}(p, x) = \sum F$ and $\text{len } F = \text{len } p$ and for every element n of $\mathbb{N}$ such that $n \in \text{dom } F$ holds $F(n) = p(n -' 1) \cdot \text{power}_L(x, n -' 1)$. Define

$\mathcal{P}[\text{natural number}] \equiv$ if $1 \leq \$_1 \leq \text{len } p$, then there exists an element d of L such that $\sum(F|\$_1) = d \cdot x + p(0)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i , $\mathcal{P}[i]$. $\square$

- (70) Let us consider a polynomial p over $\mathbb{C}_F$. Suppose $\text{len } p \geq 2$. Let us consider a real number r . Then there exists a real number e such that for every element z of $\mathbb{C}_F$ such that $e < |z|$ holds $|\text{eval}(p, z)| > r$. The theorem is a consequence of (37).
- (71) Let us consider a polynomial f over $\mathbb{Z}^R$. Suppose $\text{degree}(f) > 0$. Then $\{p, \text{ where } p \text{ is a prime number} : \text{there exists an element } x \text{ of } \mathbb{Z}^R \text{ such that } \text{eval}(f, x) \equiv 0 \pmod{p}\}$ is infinite. The theorem is a consequence of (68), (70), (39), and (69).

12. PRELIMINARIES TO PROBLEMS 132–134

Now we state the propositions:

- (72) $k \in \text{seq}(n, m)$ if and only if $n < k \leq n + m$.
 PROOF: If $k \in \text{seq}(n, m)$, then $n < k \leq n + m$. $\square$
- (73) $k \in \text{PrimeNumbers}(n, m)$ if and only if $n < k \leq n + m$ and k is prime.
 The theorem is a consequence of (72).

Let us consider natural numbers n_1, m_1, n_2, m_2 . Now we state the propositions:

- (74) If $n_1 + m_1 \leq n_2$, then $\text{seq}(n_1, m_1)$ misses $\text{seq}(n_2, m_2)$. The theorem is a consequence of (72).
- (75) If $n_1 + m_1 \leq n_2$,
 then $\text{PrimeNumbers}(n_1, m_1)$ misses $\text{PrimeNumbers}(n_2, m_2)$. The theorem is a consequence of (74).

Now we state the propositions:

- (76) $\text{seq}(n, m) \cup \text{seq}(n + m, k) = \text{seq}(n, m + k)$.
 PROOF: $\text{seq}(n, m) \subseteq \text{seq}(n, m + k)$. $\text{seq}(n + m, k) \subseteq \text{seq}(n, m + k)$. $\text{seq}(n, m + k) \subseteq \text{seq}(n, m) \cup \text{seq}(n + m, k)$. $\square$
- (77) $\text{PrimeNumbers}(n, m) \cup \text{PrimeNumbers}(n + m, k) = \text{PrimeNumbers}(n, m + k)$. The theorem is a consequence of (76).
- (78) $\overline{\text{PrimeNumbers}(n, m + k)} = \overline{\text{PrimeNumbers}(n, m)} + \overline{\text{PrimeNumbers}(n + m, k)}$. The theorem is a consequence of (75) and (77).
- (79) (i) if $n + 1$ is prime, then $\text{PrimeNumbers}(n, 1) = \{n + 1\}$, and
 (ii) if $n + 1$ is not prime, then $\text{PrimeNumbers}(n, 1) = \emptyset$.
 The theorem is a consequence of (73).

(80) (i) if $n + 1$ is prime, then $\overline{\overline{\text{PrimeNumbers}(n, 1)}} = 1$, and

(ii) if $n + 1$ is not prime, then $\overline{\overline{\text{PrimeNumbers}(n, 1)}} = 0$.

The theorem is a consequence of (79).

Let us consider n and k . Now we state the propositions:

(81) Suppose $k > 0$ and ($n + 1$ is prime and $n + k + 1$ is prime or $n + 1$ is not prime and $n + k + 1$ is not prime). Then $\overline{\overline{\text{PrimeNumbers}(n + 1, k)}} = \overline{\overline{\text{PrimeNumbers}(n, k)}}$. The theorem is a consequence of (78) and (80).

(82) Suppose $k > 0$ and $n + 1$ is not prime and $n + k + 1$ is prime. Then $\overline{\overline{\text{PrimeNumbers}(n + 1, k)}} = \overline{\overline{\text{PrimeNumbers}(n, k)}} + 1$. The theorem is a consequence of (78) and (80).

(83) Suppose $k > 0$ and $n + 1$ is prime and $n + k + 1$ is not prime. Then $\overline{\overline{\text{PrimeNumbers}(n + 1, k)}} = \overline{\overline{\text{PrimeNumbers}(n, k)}} - 1$. The theorem is a consequence of (78) and (80).

(84) (i) $\overline{\overline{\text{PrimeNumbers}(1, 100)}} = 26$, and

(ii) for every natural number k such that $k = 0$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 9$ or $k = 10$ holds $\overline{\overline{\text{PrimeNumbers}(k, 100)}} = 25$, and

(iii) for every natural number k such that $k = 5$ or $k = 6$ or $k = 7$ or $k = 8$ holds $\overline{\overline{\text{PrimeNumbers}(k, 100)}} < 25$.

The theorem is a consequence of (82), (83), and (81).

(85) Let us consider integers n, k, p . If $p \mid k$, then $n \in \text{multiples}(p)$ iff $n + k \in \text{multiples}(p)$.

PROOF: If $n \in \text{multiples}(p)$, then $n + k \in \text{multiples}(p)$ by [9, (62)]. $\square$

(86) $s \in \text{seq}(n, k)$ if and only if $s + d \in \text{seq}(n + d, k)$. The theorem is a consequence of (72).

Let us consider integers p, q, r, s, t . Now we state the propositions:

(87) Suppose $p \mid d$ and $q \mid d$ and $r \mid d$ and $s \mid d$ and $t \mid d$. Then $\overline{\overline{\text{seq}(n, k) \cap (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t)}}} = \overline{\overline{\text{seq}(n + d, k) \cap (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t)}}}$.

PROOF: Set $S = \text{seq}(n, k)$. Set $S_2 = \text{seq}(n + d, k)$. Set $M_8 = \text{multiples}(p)$. Set $M_9 = \text{multiples}(q)$. Set $M_{10} = \text{multiples}(r)$. Set $M_{11} = \text{multiples}(s)$. Set $M_{12} = \text{multiples}(t)$. Set $M = (((M_8 \cup M_9) \cup M_{10}) \cup M_{11}) \cup M_{12}$. Reconsider $D = d$ as an element of $\mathbb{N}$. Define $\mathcal{F}(\text{element of } \mathbb{N}) = \$_1 + D$. Consider f being a function from $\mathbb{N}$ into $\mathbb{N}$ such that for every element x of $\mathbb{N}$, $f(x) = \mathcal{F}(x)$. $f^\circ(S \cap M) \subseteq S_2 \cap M$. $S_2 \cap M \subseteq f^\circ(S \cap M)$. f is one-to-one. $\square$

(88) Suppose $p \mid d$ and $q \mid d$ and $r \mid d$ and $s \mid d$ and $t \mid d$. Then $\overline{\overline{\text{seq}(n, d) \cap (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t))}} = \overline{\overline{\text{seq}(n + k, d) \cap (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t))}}$. The theorem is a consequence of (74), (76), and (87).

(89) Suppose $p \mid d$ and $q \mid d$ and $r \mid d$ and $s \mid d$ and $t \mid d$. Then $\overline{\overline{\text{seq}(n, k \cdot d) \cap (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t))}} = \overline{\overline{k \cdot \text{seq}(0, d) \cap (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t))}}$.

PROOF: Set $M = (((\text{multiples}(p) \cup \text{multiples}(q)) \cup \text{multiples}(r)) \cup \text{multiples}(s)) \cup \text{multiples}(t)$. Define $\mathcal{P}[\text{natural number}] \equiv \$1 \cdot \overline{\overline{\text{seq}(0, d) \cap M}} = \overline{\overline{\text{seq}(n, \$1 \cdot d) \cap M}}$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i , $\mathcal{P}[i]$. $\square$

(90) (i) $4 = \overline{\overline{\text{seq}(6 \cdot n, 6) \cap (\text{multiples}(2) \cup \text{multiples}(3))}}$, and

(ii) $\{6 \cdot n + 1, 6 \cdot n + 5\} = (\text{seq}(6 \cdot n, 6)) \setminus (\text{multiples}(2) \cup \text{multiples}(3))$.

PROOF: Set $S = \text{seq}(6 \cdot n, 6)$. Set $M_2 = \text{multiples}(2)$. Set $M_3 = \text{multiples}(3)$. $6 \cdot n + 1 \in S$. $6 \cdot n + 5 \in S$. $S \setminus (M_2 \cup M_3) \subseteq \{6 \cdot n + 1, 6 \cdot n + 5\}$. $\square$

(91) $22 = \overline{\overline{\text{seq}(0, 30) \cap ((\text{multiples}(2) \cup \text{multiples}(3)) \cup \text{multiples}(5))}}$.

PROOF: Set $M_i = \text{multiples}(i)$ for $i = 2, 3, 5$ respectively, and $M_{2,3} = M_2 \cup M_3$. Set $S = \text{seq}(0, 30)$. $\overline{S \cap M_{2,3}} = 20$. $S \cap M_5 \setminus M_{2,3} = \{5, 25\}$. $\square$

(92) Suppose $c = \overline{\overline{\text{seq}(n, 100) \cap ((\text{multiples}(2) \cup \text{multiples}(3)) \cup \text{multiples}(5))}}$. Then

(i) $c \geq 72$, and

(ii) if $c = 72$, then $n \bmod 30 = 9$ or $n \bmod 30 = 10$.

The theorem is a consequence of (87).

(93) Suppose $c = \overline{\overline{\text{seq}(n, 100) \cap (((\text{multiples}(2) \cup \text{multiples}(3)) \cup \text{multiples}(5)) \cup \text{multiples}(7))}}$. Then

(i) $c \geq 75$, and

(ii) if $c = 75$, then $n \bmod 210 = 9$ or $n \bmod 210 = 10$ or $n \bmod 210 = 99$ or $n \bmod 210 = 100$.

The theorem is a consequence of (87).

(94) Suppose $0 \leq n < 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Then $76 \leq \overline{\overline{\text{seq}(n, 100) \cap (((\text{multiples}(2) \cup \text{multiples}(3)) \cup \text{multiples}(5)) \cup \text{multiples}(7)) \cup \text{multiples}(11))}}$.

PROOF: Set $S = \text{seq}(n, 100)$. Set $M_i = \text{multiples}(i)$ for $i = 2, 3, 5, 7$ respectively, and $M_{2,3,5,7} = M_2 \cup M_3 \cup M_5 \cup M_7$. Set $M_{11} = \text{multiples}(11)$.

$\overline{\overline{S \cap M_{2,3,5,7}}} \geq 75$. $n \bmod 210 = 9$ or $n \bmod 210 = 10$ or $n \bmod 210 = 99$ or $n \bmod 210 = 100$. Consider t being a natural number such that $n = 210 \cdot t + 9$ and $9 < 210$ or $n = 210 \cdot t + 10$ and $10 < 210$ or $n = 210 \cdot t + 99$ and $99 < 210$ or $n = 210 \cdot t + 100$ and $100 < 210$. $t < 10 + 1$. For every natural numbers i, k such that $i + 1 < k \leq i + 100$ and $k \in M_{11} \setminus M_{2,3,5,7}$ holds $i \neq n$ and $i + 1 \neq n$. $\square$

(95) If $11 \leq n$, then $\overline{\overline{\text{PrimeNumbers}(n, 100)}} \leq 24$.

PROOF: Set $M_i = \text{multiples}(i)$ for $i = 2, 3, 5, 7, 11$ respectively, and $M_{2,3,5,7} = M_2 \cup M_3 \cup M_5 \cup M_7$. Set $M = M_{2,3,5,7} \cup M_{11}$. Set $S = \text{seq}(n, 100)$.

$\overline{\overline{\text{PrimeNumbers}(n, 100)}}$ misses $S \cap M$. Set $n_4 = n \bmod 2310$. $\overline{\overline{S \cap M}} = \overline{\overline{\text{seq}(n_4, 100) \cap M}}$. $\overline{\overline{S \cap M}} \geq 76$. $\square$

(96) Suppose $0 \leq n < 2 \cdot 3 \cdot 5$.

Then $14 \leq \overline{\overline{\text{seq}(n, 21) \cap ((\text{multiples}(2) \cup \text{multiples}(3)) \cup \text{multiples}(5))}}$.

PROOF: Set $M_2 = \text{multiples}(2)$. Set $M_3 = \text{multiples}(3)$. Set $M_5 = \text{multiples}(5)$. Set $M_{2,3} = M_2 \cup M_3$. Set $S = \text{seq}(n, 21)$. $\overline{\overline{S \cap M_{2,3}}} \geq 13$. For every natural number i , $i \in S \cap M_5 \setminus M_{2,3}$ iff $n < i \leq n + 21$ and $5 \mid i$ and $2 \nmid i$ and $3 \nmid i$. $S \cap M_5 \setminus M_{2,3}$ is not empty. $\square$

(97) If $5 \leq n$, then $\overline{\overline{\text{PrimeNumbers}(n, 21)}} \leq 7$. The theorem is a consequence of (73), (87), and (96).

13. PROBLEM 132

Now we state the proposition:

- (98) (i) $\overline{\overline{\text{PrimeNumbers}(1, 100)}} = 26$, and
 (ii) for every natural number n such that $n \neq 1$ holds
 $\overline{\overline{\text{PrimeNumbers}(n, 100)}} < 26$.

The theorem is a consequence of (84) and (95).

14. PROBLEM 133

Now we state the proposition:

- (99) $\{n, \text{ where } n \text{ is a natural number} : \overline{\overline{\text{PrimeNumbers}(n, 100)}} = 25\} = \{0, 2, 3, 4, 9, 10\}$.

PROOF: $\{n, \text{ where } n \text{ is a natural number} : \overline{\overline{\text{PrimeNumbers}(n, 100)}} = 25\} \subseteq \{0, 2, 3, 4, 9, 10\}$. $\{0, 2, 3, 4, 9, 10\} \subseteq \{n, \text{ where } n \text{ is a natural number} : \overline{\overline{\text{PrimeNumbers}(n, 100)}} = 25\}$. $\square$

15. PROBLEM 134

Now we state the proposition:

$$(100) \quad \{n, \text{ where } n \text{ is a natural number : } \overline{\overline{\text{PrimeNumbers}(n, 21)} = 8}\} = \{0, 1, 2\}.$$

PROOF: $\overline{\overline{\text{PrimeNumbers}(0 + 1, 21)}} = 8$. $\overline{\overline{\text{PrimeNumbers}(1 + 1, 21)}} = 8$.

$\overline{\overline{\text{PrimeNumbers}(2 + 1, 21)}} = 8 - 1$. $\{n, \text{ where } n \text{ is a natural number :}$

$\overline{\overline{\text{PrimeNumbers}(n, 21)} = 8}\} \subseteq \{0, 1, 2\}$. $\{0, 1, 2\} \subseteq \{n, \text{ where } n \text{ is a natural number : } \overline{\overline{\text{PrimeNumbers}(n, 21)} = 8}\}$. $\square$

REFERENCES

- [1] 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.
- [2] Mario Carneiro. The divergence of the sum of prime reciprocals. *Formalized Mathematics*, 30(3):209–210, 2022. doi:10.2478/forma-2022-0015.
- [3] John Horton Conway and R.K. Guy. *The Book of Numbers*. Springer-Verlag, 1996.
- [4] G. Di Pietro. New estimations for numerical analysis approach to twin primes conjecture. *Notes on Number Theory and Discrete Mathematics*, 30(3):580–586, 2024. doi:10.7546/nntdm.2024.30.3.580-586.
- [5] Leonard Eugene Dickson. *History of Theory of Numbers*. New York, 1952.
- [6] Harvey Dubner and Wilfrid Keller. Factors of generalized Fermat numbers. *Mathematics of Computation*, 64(209):397–405, 1995. doi:10.2307/2153343.
- [7] Richard K. Guy. *Unsolved Problems in Number Theory*. Problem Books in Mathematics. Springer, third edition, 2004. doi:10.1007/978-0-387-26677-0.
- [8] Artur Kornilowicz. Elementary number theory problems. Part IV. *Formalized Mathematics*, 30(3):223–228, 2022. doi:10.2478/forma-2022-0017.
- [9] Artur Kornilowicz. Elementary number theory problems. Part XIV – Diophantine equations. *Formalized Mathematics*, 32(1):47–63, 2024. doi:10.2478/forma-2024-0004.
- [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. Elementary number theory problems. Part I. *Formalized Mathematics*, 28(1):115–120, 2020. doi:10.2478/forma-2020-0010.
- [13] 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.
- [14] Karol Pąk. Elementary number theory problems. Part XVI. *Formalized Mathematics*, 32(1):203–212, 2024. doi:10.2478/forma-2024-0017.
- [15] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.
- [16] Wacław Sierpiński. *Teoria liczb*. Instytut Matematyczny Polskiej Akademii Nauk, 1950. In Polish.
- [17] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

Received December 17, 2025, Accepted December 21, 2025