FORMALIZED MATHEMATICS
Vol. **32**, No. **1**, pp. 203–212, **2024**
DOI: 10.2478/forma-2024-0017
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part XVI

Karol Pąk
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper, we continue the work on formalizing problems from "250 Problems in Elementary Number Theory" by Wacław Sierpiński, using Mizar proof assistant. The formalization covers problems 63, 65, 66, 67, 68, 93, 95, 96, 102, and 103.

MSC: 11A41 11B25 68V20

Keywords: number theory; prime number; arithmetic progression

MML identifier: `NUMBER16`, version: `8.1.14 5.86.1479`

Introduction

In this paper, we continue the work on formalizing problems from "250 Problems in Elementary Number Theory" by Wacław Sierpiński [16]. The paper is a part of the project *Formalization of Elementary Number Theory in Mizar* [11] initiated in [10]. We present a detailed encoding of proofs of selected problems verified using the Mizar system [2], [3], focusing on properties of arithmetic progressions and specific characteristics related to the occurrence of prime numbers, particularly in the context of Chebyshev's theorem.

The formalization encompasses items 63, 65, 66, 67, 68 from Section III "Arithmetic Progressions" (and use formal apparatus of [5]) and 93, 95, 96, 102, and 103 from Section IV "Prime and Composite Numbers", each of them is contained in a separate section with appropriate title. Section 7 contains selected properties of product of distinct primes (see also [6]), needed mainly in

the solution of Problem 93 and 95, but also of general interest. Problem 95 refers to Chebyshev theorem, pointing out its proof in [15], and also Problem 102 asks to prove the equivalence of this theorem with another one. The existence of at least one prime number between positive n and $2n$ was conjectured by Bertrand in 1845 [4], but completely proved by Chebyshev in 1852 [17]. The formal proof of this fact, under name of of Bertrand's postulate [13] with proof based on [1], is present in the Mizar Mathematical Library, so the usefulness of this equivalence is rather low.

Problem 68 refers to [12] proving that in each arithmetic progression with positive coefficients there exist infinitely many terms with the same prime divisors. We use additionally [15] in some places (e.g., in Problem 65, as Sierpiński suggests in its solution).

1. Problem 63

From now on a, b, d, n, k, i, j, x, s denote natural numbers. Now we state the propositions:

(1) Let us consider finite 0-sequences f, g of $\mathbb{N}$. Then $\mathrm{value}(f \frown g, b) = \mathrm{value}(f, b) + (\mathrm{value}(g, b)) \cdot b^{\mathrm{len}\, f}$.

Proof: Consider f_2 being a finite 0-sequence of $\mathbb{N}$ such that $\mathrm{dom}\, f_2 = \mathrm{dom}\, f$ and for every natural number i such that $i \in \mathrm{dom}\, f_2$ holds $f_2(i) = f(i) \cdot b^i$ and $\mathrm{value}(f, b) = \sum f_2$. Consider g_1 being a finite 0-sequence of $\mathbb{N}$ such that $\mathrm{dom}\, g_1 = \mathrm{dom}\, g$ and for every natural number i such that $i \in \mathrm{dom}\, g_1$ holds $g_1(i) = g(i) \cdot b^i$ and $\mathrm{value}(g, b) = \sum g_1$. Consider f_1 being a finite 0-sequence of $\mathbb{N}$ such that $\mathrm{dom}\, f_1 = \mathrm{dom}(f \frown g)$ and for every natural number i such that $i \in \mathrm{dom}\, f_1$ holds $f_1(i) = (f \frown g)(i) \cdot b^i$ and $\mathrm{value}(f \frown g, b) = \sum f_1$. Consider F_1, G_1 being finite 0-sequences such that $\mathrm{len}\, F_1 = \mathrm{len}\, f$ and $\mathrm{len}\, G_1 = \mathrm{len}\, g$ and $f_1 = F_1 \frown G_1$. For every natural number k such that $k \in \mathrm{dom}\, f_2$ holds $f_2(k) = F_1(k)$. Set $B = b^{\mathrm{len}\, f}$. For every natural number k such that $k \in \mathrm{dom}\, g_1$ holds $(B \cdot g_1)(k) = G_1(k)$. □

(2) If $b > 1$ and $n > 0$ and $n \cdot b^k \leqslant x < (n+1) \cdot b^k$, then $\mathrm{digits}(n, b) = (\mathrm{digits}(x, b))_{\restriction k}$. The theorem is a consequence of (1).

(3) If $b > 0$ and $d > 1$ and $s > 0$, then there exist natural numbers m, i such that $(\mathrm{digits}((\mathrm{ArProg}(a, b))(m), d))_{\restriction i} = \mathrm{digits}(s, d)$. The theorem is a consequence of (2).

(4) Problem 63:

If $b > 0$ and $s > 0$, then there exist natural numbers m, i such that $(\mathrm{digits}((\mathrm{ArProg}(a, b))(m), 10))_{\restriction i} = \mathrm{digits}(s, 10)$.

2. PROBLEM 67

Now we state the proposition:

(5) PROBLEM 67:

Let us consider natural numbers a, b. Suppose $a > 0$ and a and b are relatively prime. Then there exists an infinite subset N of $\mathbb{N}$ such that for every natural numbers n, m such that n, $m \in N$ and $n \neq m$ holds $(\mathrm{ArProg}(b, a))(n)$ and $(\mathrm{ArProg}(b, a))(m)$ are relatively prime.

PROOF: Define $\mathcal{X}[\mathrm{set}] \equiv \$_1$ is finite and $0 \notin \$_1$ and for every natural numbers n, m such that n, $m \in \$_1$ and $n \neq m$ holds $(\mathrm{ArProg}(b, a))(n)$ and $(\mathrm{ArProg}(b, a))(m)$ are relatively prime. Define $\mathcal{G}[\mathrm{object}, \mathrm{object}] \equiv$ for every set Y such that $Y = \$_1$ and $\mathcal{X}[Y]$ there exists a natural number k such that $k \notin Y$ and $\$_2 = Y \cup \{k\}$ and $\mathcal{X}[Y \cup \{k\}]$. For every object x such that $x \in 2^{\mathbb{N}}$ there exists an object y such that $y \in 2^{\mathbb{N}}$ and $\mathcal{G}[x, y]$ by [5, (7)], [6, (17)], [14, (4)]. Consider g being a function such that $\mathrm{dom}\, g = 2^{\mathbb{N}}$ and $\mathrm{rng}\, g \subseteq 2^{\mathbb{N}}$ and for every object x such that $x \in 2^{\mathbb{N}}$ holds $\mathcal{G}[x, g(x)]$. Define $\mathcal{G}(\mathrm{object}, \mathrm{object}) = g(\$_2)$. Consider f being a function such that $\mathrm{dom}\, f = \mathbb{N}$ and $f(0) = \emptyset$ and for every natural number n, $f(n + 1) = \mathcal{G}(n, f(n))$. Define $\mathcal{F}[\mathrm{natural\ number}] \equiv f(\$_1)$ is finite and $f(\$_1) \in 2^{\mathbb{N}}$ and $\mathcal{X}[f(\$_1)]$ and for every finite set X such that $X = f(\$_1)$ holds $\overline{\overline{X}} = \$_1$. If $\mathcal{F}[n]$, then $\mathcal{F}[n + 1]$. $\mathcal{F}[n]$. $\bigcup \mathrm{rng}\, f$ is infinite. $\bigcup \mathrm{rng}\, f \subseteq \mathbb{N}$. Reconsider $N = \bigcup \mathrm{rng}\, f$ as an infinite subset of $\mathbb{N}$. Define $\mathcal{G}[\mathrm{natural\ number}] \equiv$ for every natural number n, $f(n) \subseteq f(n + \$_1)$. For every k such that $\mathcal{G}[k]$ holds $\mathcal{G}[k + 1]$. $\mathcal{G}[n]$. Consider N being a set such that $n \in N$ and $N \in \mathrm{rng}\, f$. Consider x_4 being an object such that $x_4 \in \mathrm{dom}\, f$ and $f(x_4) = N$. Consider M being a set such that $m \in M$ and $M \in \mathrm{rng}\, f$. Consider x_3 being an object such that $x_3 \in \mathrm{dom}\, f$ and $f(x_3) = M$. $\square$

3. PROBLEM 68

Now we state the proposition:

(6) PROBLEM 68:

Suppose $a > 0$ and $b > 0$. Then there exists an infinite subset N of $\mathbb{N}$ such that for every natural numbers n, m for every prime number p such that n, $m \in N$ holds $p \mid (\mathrm{ArProg}(b, a))(n)$ iff $p \mid (\mathrm{ArProg}(b, a))(m)$.

PROOF: Set $d = \gcd(a, a + b)$. Consider a_1, c being natural numbers such that $a = d \cdot a_1$ and $a + b = d \cdot c$ and a_1 and c are relatively prime. $c > 1$. For every natural number n, $a_1 \mid (c^{\mathrm{Euler}\, a_1})^{n+1} - 1$. Define $\mathcal{F}(\mathrm{natural\ number}) = c \cdot \frac{(c^{\mathrm{Euler}\, a_1})^{\$_1 + 1} - 1}{a_1} + 1$. Consider f being a function such that $\mathrm{dom}\, f = \mathbb{N}$ and

for every element x of $\mathbb{N}$, $f(x) = \mathcal{F}(x)$. $\operatorname{rng} f \subseteq \mathbb{N}$. For every objects x_1, x_2 such that $x_1, x_2 \in \operatorname{dom} f$ and $f(x_1) = f(x_2)$ holds $x_1 = x_2$. Reconsider $N = \operatorname{rng} f$ as an infinite subset of $\mathbb{N}$. For every natural number n and for every prime number p such that $n \in N$ holds $p \mid (\operatorname{ArProg}(b, a))(n)$ iff $p \mid d$ or $p \mid c$. □

4. Problem 65

Now we state the propositions:

(7) (i) $\operatorname{Fib}(6) = 8$, and

(ii) $\operatorname{Fib}(7) = 13$, and

(iii) $\operatorname{Fib}(8) = 21$, and

(iv) $\operatorname{Fib}(9) = 34$, and

(v) $\operatorname{Fib}(10) = 55$, and

(vi) $\operatorname{Fib}(11) = 89$, and

(vii) $\operatorname{Fib}(12) = 144$, and

(viii) $\operatorname{Fib}(13) = 233$, and

(ix) $\operatorname{Fib}(14) = 377$, and

(x) $\operatorname{Fib}(15) = 610$, and

(xi) $\operatorname{Fib}(16) = 987$, and

(xii) $\operatorname{Fib}(17) = 1597$, and

(xiii) $\operatorname{Fib}(18) = 2584$, and

(xiv) $\operatorname{Fib}(19) = 4181$, and

(xv) $\operatorname{Fib}(20) = 6765$, and

(xvi) $\operatorname{Fib}(21) = 10946$, and

(xvii) $\operatorname{Fib}(22) = 17711$, and

(xviii) $\operatorname{Fib}(23) = 28657$, and

(xix) $\operatorname{Fib}(24) = 46368$, and

(xx) $\operatorname{Fib}(25) = 75025$.

(8) $\operatorname{Fib}(n + 2) \geqslant n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \operatorname{Fib}(\$_1 + 2) \geqslant \$_1$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every n, $\mathcal{P}[n]$. □

(9) If $k < n \leqslant 7$, then there exists i such that $\operatorname{Fib}(i) \bmod n = k$. The theorem is a consequence of (7).

(10) Let us consider a natural number j. Suppose $0 < j \leqslant 7$. Then there exists a natural number i such that

(i) $i > 0$, and

(ii) $\mathrm{Fib}(0) \equiv \mathrm{Fib}(i) \pmod{j}$, and

(iii) $\mathrm{Fib}(1) \equiv \mathrm{Fib}(i+1) \pmod{j}$.

The theorem is a consequence of (7).

(11) Suppose $\mathrm{Fib}(n) \equiv \mathrm{Fib}(n+i) \pmod{j}$ and $\mathrm{Fib}(n+1) \equiv \mathrm{Fib}(n+i+1) \pmod{j}$. Let us consider natural numbers x, y. Suppose $x \equiv y \pmod{i}$. Then $\mathrm{Fib}(x) \equiv \mathrm{Fib}(y) \pmod{j}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathrm{Fib}(\$_1) \equiv \mathrm{Fib}(\$_1 + i) \pmod{j}$ and $\mathrm{Fib}(\$_1+1) \equiv \mathrm{Fib}(\$_1+i+1) \pmod{j}$. Define $\mathcal{Q}$[natural number] $\equiv \mathcal{P}[n+\$_1]$. For every natural number k such that $\mathcal{Q}[k]$ holds $\mathcal{Q}[k+1]$. For every natural number k, $\mathcal{Q}[k]$. Define $\mathcal{R}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then for every natural number i such that $i = n - \$_1$ holds $\mathcal{P}[i]$. For every natural number k such that $\mathcal{R}[k]$ holds $\mathcal{R}[k+1]$. For every natural number k, $\mathcal{R}[k]$. For every natural number k, $\mathrm{Fib}(k) \equiv \mathrm{Fib}(k+i) \pmod{j}$. □

(12) Let us consider natural numbers i, j, k. Suppose $0 < j$ and $k < i$ and for every natural numbers x, y such that $x \equiv y \pmod{j}$ holds $\mathrm{Fib}(x) \equiv \mathrm{Fib}(y) \pmod{i}$ and for every natural number x such that $x < j$ holds $\mathrm{Fib}(x) \bmod i \neq k$. Let us consider a natural number m. Then $(\mathrm{ArProg}(k,i))(m)$ is not Fibonacci.

(13) (i) $\mathrm{Fib}(0) \equiv \mathrm{Fib}(12) \pmod{8}$, and

(ii) $\mathrm{Fib}(1) \equiv \mathrm{Fib}(12+1) \pmod{8}$, and

(iii) for every natural number x such that $x < 12$ holds $\mathrm{Fib}(x) \bmod 8 \neq 4$ and $\mathrm{Fib}(x) \bmod 8 \neq 6$.

The theorem is a consequence of (7).

(14) PROBLEM 65:

(i) for every i and j such that $0 < i \leqslant 7$ there exists k such that $(\mathrm{ArProg}(j,i))(k)$ is Fibonacci, and

(ii) for every k, $(\mathrm{ArProg}(4,8))(k)$ is not Fibonacci.

PROOF: For every i and j such that $0 < i \leqslant 7$ there exists k such that $(\mathrm{ArProg}(j,i))(k)$ is Fibonacci by (10), (9), [7, (5)]. $\mathrm{Fib}(0) \equiv \mathrm{Fib}(0+12) \pmod{8}$ and $\mathrm{Fib}(0+1) \equiv \mathrm{Fib}(0+12+1) \pmod{8}$. For every natural numbers x, y such that $x \equiv y \pmod{12}$ holds $\mathrm{Fib}(x) \equiv \mathrm{Fib}(y) \pmod{8}$. For every natural number x such that $x < 12$ holds $\mathrm{Fib}(x) \bmod 8 \neq 4$. □

5. Problem 66

Now we state the proposition:

(15) Problem 66:

(i) 4 and 11 are relatively prime, and

(ii) for every natural number m, $(\mathrm{ArProg}(4,11))(m)$ is not Fibonacci.

Proof: $\mathrm{Fib}(0) \equiv \mathrm{Fib}(0+10) \pmod{11}$ and $\mathrm{Fib}(0+1) \equiv \mathrm{Fib}(0+10+1) \pmod{11}$. For every natural numbers x, y such that $x \equiv y \pmod{10}$ holds $\mathrm{Fib}(x) \equiv \mathrm{Fib}(y) \pmod{11}$. For every natural number x such that $x < 10$ holds $\mathrm{Fib}(x) \bmod 11 \neq 4$ by [8, (16)], (7). □

6. Problem 96

Now we state the propositions:

(16) $\mathrm{value}(\langle 1\rangle \frown (n \longmapsto 3), 10) = \frac{10^{n+1}-7}{3}$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv 3 \cdot (\mathrm{value}(\langle 1\rangle \frown (\$_1 \longmapsto 3), 10)) = 10^{\$_1+1} - 7$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

(17) There exists a natural number k such that $17 \mid k = \frac{10^{16\cdot n+9}-7}{3}$. The theorem is a consequence of (16).

(18) 33331 is prime.

(19) 333331 is prime.

(20) Problem 96:

(i) for every non zero natural number n such that $n < 6$ holds $\mathrm{value}(\langle 1\rangle \frown (n \longmapsto 3), 10)$ is prime, and

(ii) $\mathrm{value}(\langle 1\rangle \frown (8 \longmapsto 3), 10)$ is not prime, and

(iii) $\{\mathrm{value}(\langle 1\rangle \frown (n \longmapsto 3), 10)$, where n is a natural number : $\mathrm{value}(\langle 1\rangle \frown (n \longmapsto 3), 10)$ is non prime$\}$ is infinite.

Proof: Consider v being a natural number such that $17 \mid v = \frac{10^{16\cdot 0+9}-7}{3}$. $\mathrm{value}(\langle 1\rangle \frown (8 \longmapsto 3), 10) = \frac{10^{8+1}-7}{3}$. Set $V = \{\mathrm{value}(\langle 1\rangle \frown (n \longmapsto 3), 10)$, where n is a natural number : $\mathrm{value}(\langle 1\rangle \frown (n \longmapsto 3), 10)$ is not prime $\}$. Define $\mathcal{F}(\text{natural number}) = \frac{10^{16\cdot \$_1+9}-7}{3}$. Consider f being a function such that $\mathrm{dom}\, f = \mathbb{N}$ and for every element d of $\mathbb{N}$, $f(d) = \mathcal{F}(d)$. For every objects x_1, x_2 such that $x_1, x_2 \in \mathrm{dom}\, f$ and $f(x_1) = f(x_2)$ holds $x_1 = x_2$. $\mathrm{rng}\, f \subseteq V$. □

7. Selected Properties of Product of Different Primes

Now we state the proposition:

(21) Let us consider a non zero natural number n, and a prime number p. Suppose support $\mathrm{PFExp}(n) = \{p\}$. Then $n = p^{(\mathrm{PFExp}(n))(p)}$.

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

(22) $\mathrm{rng}\,\mathrm{PFExp}(n) \subseteq \{0,1\}$ and $\overline{\overline{\mathrm{support}\,\mathrm{PFExp}(n)}} = 1$ if and only if n is prime.
PROOF: $\mathrm{rng}\,\mathrm{PFExp}(n) \subseteq \{0,1\}$. □

(23) $0 \in \mathrm{rng}\,\mathrm{PFExp}(n)$.

(24) Let us consider non zero natural numbers n, m. Suppose n and m are relatively prime. Then $\mathrm{rng}\,\mathrm{PFExp}(n \cdot m) = \mathrm{rng}\,\mathrm{PFExp}(n) \cup \mathrm{rng}\,\mathrm{PFExp}(m)$.
PROOF: $\mathrm{rng}\,\mathrm{PFExp}(n \cdot m) \subseteq \mathrm{rng}\,\mathrm{PFExp}(n) \cup \mathrm{rng}\,\mathrm{PFExp}(m)$. $\mathrm{rng}\,\mathrm{PFExp}(n) \subseteq \mathrm{rng}\,\mathrm{PFExp}(n \cdot m)$. $\mathrm{rng}\,\mathrm{PFExp}(m) \subseteq \mathrm{rng}\,\mathrm{PFExp}(n \cdot m)$. □

(25) $\prod \mathrm{primesFinS}((n+1)) = (\prod \mathrm{primesFinS}(n)) \cdot (\mathrm{pr}(n))$.

(26) Let us consider a natural number k. Then $2^k \leqslant \prod \mathrm{primesFinS}(k)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv 2^{\$_1} \leqslant \prod \mathrm{primesFinS}(\$_1)$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(27) If $2 \leqslant n$, then there exists a non zero natural number k such that $\prod \mathrm{primesFinS}(k) \leqslant n < \prod \mathrm{primesFinS}((k+1))$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv n < \prod \mathrm{primesFinS}((\$_1 + 1))$. Consider k being a natural number such that $2^k \leqslant n < 2^{k+1}$. $2^{k+1} \leqslant \prod \mathrm{primesFinS}((k+1))$. Consider m being a natural number such that $\mathcal{P}[m]$ and for every natural number w such that $\mathcal{P}[w]$ holds $m \leqslant w$. $\prod \mathrm{primesFinS}(m) \leqslant n$. □

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

(28) (i) p-count$(\prod \mathrm{primesFinS}(k)) = 1$ iff $\mathrm{primeindex}(p) < k$, and
(ii) p-count$(\prod \mathrm{primesFinS}(k)) = 0$ iff $\mathrm{primeindex}(p) \geqslant k$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every prime number p, (p-count$(\prod \mathrm{primesFinS}(\$_1)) = 1$ iff $\mathrm{primeindex}(p) < \$_1$) and ($p$-count$(\prod \mathrm{primesFinS}(\$_1)) = 0$ iff $\mathrm{primeindex}(p) \geqslant \$_1$). $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(29) $p \mid \prod \mathrm{primesFinS}(k)$ if and only if $\mathrm{primeindex}(p) < k$.
PROOF: If $p \mid \prod \mathrm{primesFinS}(k)$, then $\mathrm{primeindex}(p) < k$. p-count$(\prod \mathrm{primesFinS}(k)) = 1$. □

(30) If $k \leqslant \mathrm{primeindex}(p)$, then p and $\prod \mathrm{primesFinS}(k)$ are relatively prime.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant k$, then p and $\prod \mathrm{primesFinS}(\$_1)$ are relatively prime. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(31) (i) $\operatorname{rng}\operatorname{PrimeExponents}(\prod \operatorname{primesFinS}(n)) \subseteq \{0,1\}$, and

(ii) $\overline{\overline{\operatorname{support}\operatorname{PrimeExponents}(\prod \operatorname{primesFinS}(n))}} = n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{\operatorname{support}\operatorname{PrimeExponents}(\prod \operatorname{primesFinS}(\$_1))}} = \$_1$ and $\operatorname{rng}\operatorname{PrimeExponents}(\prod \operatorname{primesFinS}(\$_1)) \subseteq \{0,1\}$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

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

(32) If for every natural number k such that $k < m$ holds $\operatorname{pr}(k) \mid n$, then $\prod \operatorname{primesFinS}(m) \mid n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \text{if } \$_1 \leqslant m$, then $\prod \operatorname{primesFinS}(\$_1) \mid n$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i, $\mathcal{P}[i]$. □

(33) $n < m$ if and only if $\prod \operatorname{primesFinS}(n) < \prod \operatorname{primesFinS}(m)$.

PROOF: If $n < m$, then $\prod \operatorname{primesFinS}(n) < \prod \operatorname{primesFinS}(m)$. □

8. PROBLEM 93

Now we state the proposition:

(34) PROBLEM 93:

Let us consider a sequence r of real numbers. Suppose for every non zero natural number n, there exists a prime number q such that $r(n) = \frac{q}{n}$ and $q \nmid n$ and for every prime number p such that $p \nmid n$ holds $q \leqslant p$. Then

(i) r is convergent, and

(ii) $\lim r = 0$.

PROOF: For every real number p such that $0 < p$ there exists a natural number n such that for every natural number m such that $n \leqslant m$ holds $|r(m) - 0| < p$. □

9. PROBLEM 95

Now we state the proposition:

(35) PROBLEM 95:

Let us consider a non zero natural number s, and a natural number n. Suppose $n > \prod \operatorname{primesFinS}(s)$. Then there exists a natural number p such that

(i) $n < p < 2 \cdot n$, and

(ii) $\operatorname{rng}\operatorname{PrimeExponents}(p) \subseteq \{0,1\}$, and

(iii) $\overline{\overline{\operatorname{support}\operatorname{PrimeExponents}(p)}} = s$.

PROOF: Reconsider $s_1 = s-1$ as a natural number. Set $P_1 = \prod \operatorname{primesFinS}(s_1)$. Set $k = n \operatorname{div} P_1$. Set $r = n \bmod P_1$. $k \cdot P_1 + r > P_1 \cdot (\operatorname{pr}(s_1))$. Consider p being a prime number such that $k < p \leqslant 2 \cdot k$. $p \neq 2 \cdot k$. $s_1 < \operatorname{primeindex}(p)$ by [9, (12)]. $\operatorname{support}\operatorname{PFExp}(p)$ misses $\operatorname{support}\operatorname{PFExp}(P_1)$. $\operatorname{rng}\operatorname{PFExp}(p \cdot P_1) = \operatorname{rng}\operatorname{PFExp}(p) \cup \operatorname{rng}\operatorname{PFExp}(P_1)$. $\operatorname{rng}\operatorname{PFExp}(p) \subseteq \{0,1\}$. $\operatorname{rng}\operatorname{PFExp}(P_1) \subseteq \{0,1\}$. $\overline{\overline{\operatorname{support}\operatorname{PFExp}(p)}} = 1$. □

10. PROBLEM 102

Now we state the propositions:

(36) Let us consider a natural number n, and a prime number p. If $p \leqslant n$ and $p^2 \mid n!$, then $2 \cdot p \leqslant n$.

PROOF: Consider o being a natural number such that $p \cdot p \cdot o = n!$. Set $I = \operatorname{idseq}(n)$. For every real number r such that $r \in \operatorname{rng} I$ holds $0 < r$. Consider i being a natural number such that $i \in \operatorname{dom}((I\restriction(p -' 1)) \frown I_{\lfloor p})$ and $p \mid ((I\restriction(p -' 1)) \frown I_{\lfloor p})(i)$. □

(37) If $0 < a < b \leqslant n$, then $a \cdot b \mid n!$.

PROOF: For every object x such that $x \in \operatorname{dom}\langle a, b\rangle$ holds $\langle a, b\rangle(x) \leqslant n$. For every natural number i such that $i \in \operatorname{dom}\langle a\rangle$ holds $\langle a\rangle(i) < b$. □

(38) Let us consider a prime number p. Suppose $2 < n$ and $n \operatorname{div} 2 < p \leqslant 2 \cdot (n \operatorname{div} 2)$. Then $p\text{-count}(n!) = 1$. The theorem is a consequence of (36).

(39) PROBLEM 102:
for every natural number n such that $n > 1$ there exists a prime number p such that $n < p < 2 \cdot n$ if and only if for every natural number n such that $n > 1$ there exists a prime number p such that $p\text{-count}(n!) = 1$.

PROOF: Consider p being a prime number such that $p\text{-count}(2 \cdot n!) = 1$. $n < p$. □

11. PROBLEM 103

Now we state the proposition:

(40) Suppose for every natural number n such that $n > 5$ there exist prime numbers p, q such that $n < p < q < 2 \cdot n$. Let us consider a natural number n. Suppose $n > 10$. Then there exist prime numbers p, q such that

(i) $p < q$, and

(ii) p-count$(n!) = 1$, and

(iii) q-count$(n!) = 1$.

The theorem is a consequence of (36) and (38).

References

[1] Martin Aigner and Günter M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.

[2] 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.

[3] 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.

[4] Joseph Bertrand. Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. *Journal de l'École Royale Polytechnique*, 18 (30):123–140, 1845.

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

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

[7] Artur Korniłowicz and Adam Naumowicz. Niven's theorem. *Formalized Mathematics*, 24 (**4**):301–308, 2016. doi:10.1515/forma-2016-0026.

[8] Artur Korniłowicz and Dariusz Surowik. Elementary number theory problems. Part II. *Formalized Mathematics*, 29(**1**):63–68, 2021. doi:10.2478/forma-2021-0006.

[9] Artur Korniłowicz and Rafał Ziobro. Elementary number theory problems. Part XIII. *Formalized Mathematics*, 32(1):1–8, 2024. doi:10.2478/forma-2024-0001.

[10] Adam Naumowicz. Elementary number theory problems. Part I. *Formalized Mathematics*, 28(**1**):115–120, 2020. doi:10.2478/forma-2020-0010.

[11] 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.

[12] Georg Pòlya. Zur arithmetischen Untersuchung der Polynome. *Mathematische Zeitschrift*, 1(1):142–148, 1918.

[13] Marco Riccardi. Pocklington's theorem and Bertrand's postulate. *Formalized Mathematics*, 14(**2**):47–52, 2006. doi:10.2478/v10037-006-0007-y.

[14] Marco Riccardi. Ramsey's theorem. *Formalized Mathematics*, 16(**2**):203–205, 2008. doi:10.2478/v10037-008-0026-y.

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

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

[17] Pafnuty Tchebychev. Mémoire sur les nombres premiers. *Journal de mathématiques pures et appliquées*, 1:366–390, 1852.

Accepted December 14, 2024