FORMALIZED MATHEMATICS
Vol. 30, No. 2, Pages 135–158, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0011
sciendo.com/journal/forma

Elementary Number Theory Problems. Part III

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Summary. In this paper problems 11, 16, 19–24, 39, 44, 46, 74, 75, 77, 82, and 176 from [10] are formalized as described in [6], using the Mizar formalism [1], [2], [4]. Problems 11 and 16 from the book are formulated as several independent theorems. Problem 46 is formulated with a given example of required properties. Problem 77 is not formulated using triangles as in the book is.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: `NUMBER03`, version: `8.1.12 5.71.1431`

1. Preliminaries

One can verify that every set which is natural is also natural-membered.

From now on a, b, i, k, m, n denote natural numbers, s, z denote non zero natural numbers, r denotes a real number, c denotes a complex number, and e_1, e_2, e_3, e_4, e_5 denote extended reals.

Now we state the propositions:

(1) If $e_1 \leqslant e_2 \leqslant e_3 \leqslant e_4$, then $e_1 \leqslant e_4$.

(2) If $e_1 \leqslant e_2 \leqslant e_3 \leqslant e_4 \leqslant e_5$, then $e_1 \leqslant e_5$. The theorem is a consequence of (1).

(3) $2^{10} + 1 = 1025$.

(4) $3^{10} + 1 = 5905 \cdot 10$.

(5) $4^{10} + 1 = 1048 \cdot 1000 + 577$.

(6) $5^{10} + 1 = 9765 \cdot 1000 + 626$.

(7) $6^{10} + 1 = 6046 \cdot 10000 + 6177$.

(8) $7^{10} + 1 = (2824 \cdot 10000 + 7525) \cdot 10$.

(9) $8^{10} + 1 = (1073 \cdot 100 + 74) \cdot 10000 + 1825$.

(10) $9^{10} + 1 = (3486 \cdot 100 + 78) \cdot 10000 + 4402$.

(11) $n \bmod (m+1) = 0$ or ... or $n \bmod (m+1) = m$.

(12) If $n \mid 8$, then $n \in \{1, 2, 4, 8\}$.

(13) If $0 < m$, then $\gcd(m, n) \leqslant m$.

(14) Let us consider integers i, j. If i and j are relatively prime, then $i \neq j$ or $i = j = 1$ or $i = j = -1$.

(15) Let us consider natural numbers i, j. If i and j are relatively prime, then $i \neq j$ or $i = j = 1$.

(16) If $a < n$ and $b < n$ and $n \mid a - b$, then $a = b$.

(17) Let us consider integers a, b, m. Suppose $a < b$. Then there exists k such that

  (i) $m < (b - a) \cdot k + 1 - a$, and

  (ii) $k = |\lceil \frac{m+a-1}{b-a} + 1 \rceil|$.

Let i be an integer. Let us observe that $(i^{\kappa})_{\kappa \in \mathbb{N}}$ is $\mathbb{Z}$-valued.

Let us consider n. Note that $(n^{\kappa})_{\kappa \in \mathbb{N}}$ is $\mathbb{N}$-valued.

Let f be a non-negative yielding, real-valued many sorted set indexed by $\mathbb{N}$. Let us observe that $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$ is non-decreasing.

Now we state the propositions:

(18) Suppose $a \neq 0$ or $b \neq 0$. Then there exist natural numbers A, B such that

  (i) $a = (\gcd(a, b)) \cdot A$, and

  (ii) $b = (\gcd(a, b)) \cdot B$, and

  (iii) A and B are relatively prime.

(19) If $n \neq 0$, then for every integers p, m such that $p \mid m$ holds $p \mid ((m^{\kappa})_{\kappa \in \mathbb{N}})(n)$.

PROOF: Set $G = (m^{\kappa})_{\kappa \in \mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \neq 0$, then $p \mid G(\$_1)$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. □

(20) $((r^{\kappa})_{\kappa \in \mathbb{N}})(a + b) = ((r^{\kappa})_{\kappa \in \mathbb{N}})(a) \cdot (r^{b})$.

PROOF: Set $S = (r^{\kappa})_{\kappa \in \mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv S(a + \$_1) = S(a) \cdot (r^{\$_1})$. $\mathcal{P}[0]$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. □

(21) Let us consider integers p, m. Suppose $p \mid m$.
Then $p \mid ((\sum_{\alpha=0}^{\kappa}((m^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(n) - 1$.
PROOF: Set $G = (m^{\kappa})_{\kappa\in\mathbb{N}}$. Set $P = (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv p \mid P(\$_1) - 1$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. □

(22) $((\sum_{\alpha=0}^{\kappa}((m^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(n)$ and m^{n+1} are relatively prime. The theorem is a consequence of (21).

(23) $\gcd(((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k), ((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k+i)) = \gcd(((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k), ((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k+i) - ((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k))$.

(24) $((\sum_{\alpha=0}^{\kappa}((r^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k+i+1) - ((\sum_{\alpha=0}^{\kappa}((r^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k) = r^{k+1} \cdot ((\sum_{\alpha=0}^{\kappa}((r^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(i)$.
PROOF: Set $S = (r^{\kappa})_{\kappa\in\mathbb{N}}$. Set $P = (\sum_{\alpha=0}^{\kappa} S(\alpha))_{\kappa\in\mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv P(k + \$_1 + 1) - P(k) = r^{k+1} \cdot P(\$_1)$. $\mathcal{P}[0]$. For every a such that $\mathcal{P}[a]$ holds $\mathcal{P}[a+1]$. For every k, $\mathcal{P}[k]$. □

(25) Suppose $n+1$ and $m+1$ are relatively prime.
Then $((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(n)$ and $((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(m)$ are relatively prime. The theorem is a consequence of (14).

(26) If $a \neq 0$ and $b \neq 0$ and $i \neq 0$, then $\gcd(i^a - 1, i^b - 1) = i^{\gcd(a,b)} - 1$. The theorem is a consequence of (18) and (25).

Let us consider integers a, b, k. Now we state the propositions:

(27) Suppose $a+b > 0$ and $(a \bmod k)+(b \bmod k) > 0$. Then $(a+b)^n \bmod k = ((a \bmod k) + (b \bmod k))^n \bmod k$.
PROOF: Set $a_1 = a \bmod k$. Set $b_1 = b \bmod k$. Define $\mathcal{P}$[natural number] $\equiv (a+b)^{\$_1} \bmod k = (a_1+b_1)^{\$_1} \bmod k$. $\mathcal{P}[0]$. For every natural number x such that $\mathcal{P}[x]$ holds $\mathcal{P}[x+1]$. For every natural number x, $\mathcal{P}[x]$. □

(28) $(a+b)^n \bmod k = ((a \bmod k) + (b \bmod k))^n \bmod k$.
PROOF: Set $a_1 = a \bmod k$. Set $b_1 = b \bmod k$. Define $\mathcal{P}$[natural number] $\equiv (a+b)^{\$_1} \bmod k = (a_1+b_1)^{\$_1} \bmod k$. $\mathcal{P}[0]$. For every natural number x such that $\mathcal{P}[x]$ holds $\mathcal{P}[x+1]$. For every natural number x, $\mathcal{P}[x]$. □

(29) If $1 < m$, then $m \mid a^b + 1$ iff $m \mid (a \bmod m)^b + 1$.
PROOF: Set $r = a \bmod m$. If $m \mid a^b + 1$, then $m \mid r^b + 1$ by [8, (7)], (28). □

(30) $10 \mid a^{10} + 1$ if and only if there exist natural numbers r, k such that $a = 10 \cdot k + r$ and $10 \mid r^{10} + 1$ and $r = 0$ or ... or $r = 9$.
PROOF: If $10 \mid a^{10} + 1$, then there exist natural numbers r, k such that $a = 10 \cdot k + r$ and $10 \mid r^{10} + 1$ and $r = 0$ or ... or $r = 9$ by (29), [3, (8)]. □

(31) Let us consider odd natural numbers a, b. If $a - b = 2$, then a and b are relatively prime.

(32) Let us consider odd natural numbers a, b, c. If $c - b = 2$ and $b - a = 2$, then $3 \mid a$ or $3 \mid b$ or $3 \mid c$.

(33) Let us consider odd prime numbers a, b, c. If $c - b = 2$ and $b - a = 2$, then $a = 3$ and $b = 5$ and $c = 7$. The theorem is a consequence of (32).

(34) If a^n is prime, then $n = 1$.

(35) If $1 < a$, then there exists k such that $1 < k$ and $n < a^k$.

(36) (i) $2^n \bmod 3 = 1$, or

(ii) $2^n \bmod 3 = 2$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv 2^{\$_1} \bmod 3 = 1$ or $2^{\$_1} \bmod 3 = 2$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. □

(37) $3^m \mid 2^{3^m} + 1$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv 3^{\$_1} \mid 2^{3^{\$_1}} + 1$. $\mathcal{P}[0]$. For every m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m+1]$ by [7, (2),(1)]. For every m, $\mathcal{P}[m]$. □

(38) $\mathrm{Euler}\, 0 = 0$.

Let us note that Euler 0 is zero.

Let n be a positive natural number. One can check that Euler n is positive.

2. Main Problems

Now we state the propositions:

(39) $5 \mid 2^{2 \cdot n+1} - 2^{n+1} + 1$ if and only if $n \bmod 4 = 1$ or $n \bmod 4 = 2$.

PROOF: Define $\mathcal{F}(\text{natural number}) = 2^{2 \cdot \$_1+1} - 2^{\$_1+1} + 1$. Consider k such that $n = 4 \cdot k$ or $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. If $5 \mid \mathcal{F}(n)$, then $n \bmod 4 = 1$ or $n \bmod 4 = 2$. □

(40) $5 \mid 2^{2 \cdot n+1} + 2^{n+1} + 1$ if and only if $n \bmod 4 = 0$ or $n \bmod 4 = 3$.

PROOF: Define $\mathcal{G}(\text{natural number}) = 2^{2 \cdot \$_1+1} + 2^{\$_1+1} + 1$. Consider k such that $n = 4 \cdot k$ or $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. If $5 \mid \mathcal{G}(n)$, then $n \bmod 4 = 0$ or $n \bmod 4 = 3$. □

(41) $5 \mid 2^{2 \cdot n+1} - 2^{n+1} + 1$ if and only if $5 \nmid 2^{2 \cdot n+1} + 2^{n+1} + 1$. The theorem is a consequence of (11), (39), and (40).

(42) $\{n$, where n is a natural number : $n \mid 2^n + 1\}$ is infinite.

PROOF: Set $S = \{n$, where n is a natural number : $n \mid 2^n + 1\}$. Define $\mathcal{F}(\text{natural number}) = 3^{\$_1}$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element i of $\mathbb{N}$, $f(i) = \mathcal{F}(i)$. Set $R = \operatorname{rng} f$. $R \subseteq S$. For every natural number m, there exists a natural number N such that $N \geqslant m$ and $N \in R$ by [9, (1)]. □

(43) $\{n$, where n is a natural number : $n \mid 2^n + 1$ and n is prime$\} = \{3\}$.
PROOF: Set $S = \{n$, where n is a natural number : $n \mid 2^n + 1$ and n is prime$\}$. $S \subseteq \{3\}$. $3^1 \mid 2^{3^1} + 1$. □

(44) $10 \mid a^{10} + 1$ if and only if there exists k such that $a = 10 \cdot k + 3$ or $a = 10 \cdot k + 7$.
PROOF: If $10 \mid a^{10} + 1$, then there exists k such that $a = 10 \cdot k + 3$ or $a = 10 \cdot k + 7$. □

(45) If ($a \neq 0$ or $b \neq 0$) and $n > 0$ and $a \mid b^n - 1$, then a and b are relatively prime.

(46) There exists no natural number n such that $1 < n$ and $n \mid 2^n - 1$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv 1 < \$_1$ and $\$_1 \mid 2^{\$_1} - 1$. Consider N being a natural number such that $\mathcal{P}[N]$ and for every natural number n such that $\mathcal{P}[n]$ holds $N \leqslant n$. Set $E = \operatorname{Euler} N$. Set $d = \gcd(N, E)$. 2 and N are relatively prime. $\gcd(2^N - 1, 2^E - 1) = 2^d - 1$. $d \leqslant E$. □

(47) $\{n$, where n is an odd natural number : $n \mid 3^n + 1\} = \{1\}$.
PROOF: Set $A = \{n$, where n is an odd natural number : $n \mid 3^n + 1\}$. $A \subseteq \{1\}$. □

(48) $\{n$, where n is a positive natural number : $3 \mid n \cdot (2^n) + 1\}$ = the set of all $6 \cdot k + 1$ where k is a natural number $\cup$ the set of all $6 \cdot k + 2$ where k is a natural number.
PROOF: Set $A = \{n$, where n is a positive natural number : $3 \mid n \cdot (2^n) + 1\}$. Set B = the set of all $6 \cdot k + 1$ where k is a natural number. Set C = the set of all $6 \cdot k + 2$ where k is a natural number. $A \subseteq B \cup C$ by [5, (26)]. □

Let us consider an odd prime number p. Now we state the propositions:

(49) If $n = (p - 1) \cdot (k \cdot p + 1)$, then $2^n \bmod p = 1$.

(50) If $n = (p - 1) \cdot (k \cdot p + 1)$, then $p \mid$ the Cullen number of n. The theorem is a consequence of (49).

(51) $\{n$, where n is a natural number : $p \mid$ the Cullen number of $n\}$ is infinite.
PROOF: Set $S = \{n$, where n is a natural number : $p \mid$ the Cullen number of $n\}$. Define $\mathcal{F}$(natural number) $= (p - 1) \cdot (\$_1 \cdot p + 1)$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element i of $\mathbb{N}$, $f(i) = \mathcal{F}(i)$. Set $R = \operatorname{rng} f$. $R \subseteq S$. For every natural number m, there exists a natural number N such that $N \geqslant m$ and $N \in R$. □

(52) There exist natural numbers x, y such that

(i) $x > n$, and

(ii) $x \nmid y$, and

(iii) $x^x \mid y^y$.

The theorem is a consequence of (35) and (34).

(53) Let us consider integers a, b, c, n. Suppose $3 < n$. Then there exists an integer k such that

(i) $n \nmid k + a$, and

(ii) $n \nmid k + b$, and

(iii) $n \nmid k + c$.

(54) Let us consider integers a, b. Suppose $a \neq b$. Then $\{n$, where n is a natural number : $a + n$ and $b + n$ are relatively prime$\}$ is infinite.

Let a, b, c be integers. We say that a, b, c are mutually coprime if and only if

(Def. 1) a and b are relatively prime and a and c are relatively prime and b and c are relatively prime.

Let d be an integer. We say that a, b, c, d are mutually coprime if and only if

(Def. 2) a and b are relatively prime and a and c are relatively prime and a and d are relatively prime and b and c are relatively prime and b and d are relatively prime and c and d are relatively prime.

Now we state the propositions:

(55) Let us consider prime numbers a, b, c. If a, b, c are mutually different, then a, b, c are mutually coprime.

(56) Let us consider prime numbers a, b, c, d. If a, b, c, d are mutually different, then a, b, c, d are mutually coprime.

(57) (i) 1, 2, 3, 4 are mutually different, and

(ii) there exists no positive natural number n such that $1+n$, $2+n$, $3+n$, $4 + n$ are mutually coprime.

(58) Let us consider an even natural number n. Suppose $n > 6$. Then there exist prime numbers p, q such that

(i) $n - p$ and $n - q$ are relatively prime, and

(ii) $p = 3$, and

(iii) $q = 5$.

The theorem is a consequence of (31).

(59) $\{p$, where p is a prime number : there exist prime numbers a, b such that $p = a + b$ and there exist prime numbers c, d such that $p = c - d\} = \{5\}$.
PROOF: Set $A = \{p$, where p is a prime number : there exist prime numbers a, b such that $p = a + b$ and there exist prime numbers c, d such that $p = c - d\}$. $A \subseteq \{5\}$. $\square$

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

(60) A corollary from the Fermat Theorem:
If $p = 4 \cdot k + 1$, then there exist positive natural numbers a, b such that $a > b$ and $p = a^{\mathbf{2}} + b^{\mathbf{2}}$.

(61) If $p = 4 \cdot k + 1$, then there exist positive natural numbers a, b such that $p^{\mathbf{2}} = a^{\mathbf{2}} + b^{\mathbf{2}}$. The theorem is a consequence of (60).

(62) (i) $5 \mid n + 1$, or
(ii) $5 \mid n + 7$, or
(iii) $5 \mid n + 9$, or
(iv) $5 \mid n + 13$, or
(v) $5 \mid n + 15$.

(63) $\{n$, where n is a natural number : $n+1$ is prime and $n+3$ is prime and $n+7$ is prime and $n+9$ is prime and $n+13$ is prime and $n+15$ is prime$\} = \{4\}$.
Proof: Set $A = \{n$, where n is a natural number : $n+1$ is prime and $n+3$ is prime and $n+7$ is prime and $n+9$ is prime and $n+13$ is prime and $n+15$ is prime$\}$. $A \subseteq \{4\}$. $\square$

(64) $r^3 + (r + 1)^3 + (r + 2)^3 = (r + 3)^3$ if and only if $r = 3$.
Proof: If $r^3 + (r + 1)^3 + (r + 2)^3 = (r + 3)^3$, then $r = 3$. $\square$

3. Tools for Computing Prime Numbers

In the sequel p denotes a prime number. Now we state the propositions:

(65) If $p < 3$, then $p = 2$.

(66) If $k < 9$ and $p \cdot p \leqslant k$, then $p = 2$. The theorem is a consequence of (65).

(67) If $p < 5$, then $p = 2$ or $p = 3$. The theorem is a consequence of (65).

(68) If $k < 25$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$. The theorem is a consequence of (67).

(69) If $p < 7$, then $p = 2$ or $p = 3$ or $p = 5$. The theorem is a consequence of (67).

(70) If $k < 49$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$. The theorem is a consequence of (69).

(71) If $p < 11$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$. The theorem is a consequence of (69).

(72) If $k < 121$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$. The theorem is a consequence of (71).

(73) If $p < 13$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$. The theorem is a consequence of (71).

(74) If $k < 169$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$. The theorem is a consequence of (73).

(75) If $p < 17$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$. The theorem is a consequence of (73).

(76) If $k < 289$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$. The theorem is a consequence of (75).

(77) If $p < 19$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$. The theorem is a consequence of (75).

(78) If $k < 361$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$. The theorem is a consequence of (77).

(79) If $p < 23$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$. The theorem is a consequence of (77).

(80) If $k < 529$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$. The theorem is a consequence of (79).

(81) If $p < 29$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$. The theorem is a consequence of (79).

(82) If $k < 841$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$. The theorem is a consequence of (81).

(83) If $p < 31$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$. The theorem is a consequence of (81).

(84) If $k < 961$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$. The theorem is a consequence of (83).

(85) If $p < 37$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$. The theorem is a consequence of (83).

(86) If $k < 1369$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$. The theorem is a consequence of (85).

(87) If $p < 41$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$. The theorem is a consequence of (85).

(88) If $k < 1681$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$. The theorem is a consequence of (87).

(89) If $p < 43$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or

$p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$. The theorem is a consequence of (87).

(90) If $k < 1849$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$. The theorem is a consequence of (89).

(91) If $p < 47$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$ or $p = 43$. The theorem is a consequence of (89).

(92) Suppose $k < 2209$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$.

The theorem is a consequence of (91).

(93) If $p < 53$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$ or $p = 43$ or $p = 47$. The theorem is a consequence of (91).

(94) Suppose $k < 2809$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$.

The theorem is a consequence of (93).

(95) Suppose $p < 59$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$.

The theorem is a consequence of (93).

(96) Suppose $k < 3481$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$.

The theorem is a consequence of (95).

(97) Suppose $p < 61$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$.

The theorem is a consequence of (95).

(98) Suppose $k < 3721$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$.

The theorem is a consequence of (97).

(99) Suppose $p < 67$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$.

The theorem is a consequence of (97).

(100) Suppose $k < 4489$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$.

The theorem is a consequence of (99).

(101) Suppose $p < 71$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$.

The theorem is a consequence of (99).

(102) Suppose $k < 5041$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$.

The theorem is a consequence of (101).

(103) Suppose $p < 73$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$.

The theorem is a consequence of (101).

(104) Suppose $k < 5329$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$.

The theorem is a consequence of (103).

(105) Suppose $p < 79$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$.

The theorem is a consequence of (103).

(106) Suppose $k < 6241$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$.

The theorem is a consequence of (105).

(107) Suppose $p < 83$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$, or
(xviii) $p = 61$, or
(xix) $p = 67$, or
(xx) $p = 71$, or
(xxi) $p = 73$, or
(xxii) $p = 79$.

The theorem is a consequence of (105).

(108) Suppose $k < 6889$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$.

The theorem is a consequence of (107).

(109) Suppose $p < 89$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$.

The theorem is a consequence of (107).

(110) Suppose $k < 7921$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$.

The theorem is a consequence of (109).

(111) Suppose $p < 97$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$, or
(xviii) $p = 61$, or
(xix) $p = 67$, or
(xx) $p = 71$, or
(xxi) $p = 73$, or
(xxii) $p = 79$, or
(xxiii) $p = 83$, or
(xxiv) $p = 89$.

The theorem is a consequence of (109).

(112) Suppose $k < 9409$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or

(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$, or
(xviii) $p = 61$, or
(xix) $p = 67$, or
(xx) $p = 71$, or
(xxi) $p = 73$, or
(xxii) $p = 79$, or
(xxiii) $p = 83$, or
(xxiv) $p = 89$.

The theorem is a consequence of (111).

(113) Suppose $p < 101$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or

(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$, or
(xviii) $p = 61$, or
(xix) $p = 67$, or
(xx) $p = 71$, or
(xxi) $p = 73$, or
(xxii) $p = 79$, or
(xxiii) $p = 83$, or
(xxiv) $p = 89$, or
(xxv) $p = 97$.

The theorem is a consequence of (111).

(114) Suppose $k < 10201$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$, or

(xxiv) $p = 89$, or

(xxv) $p = 97$.

The theorem is a consequence of (113).

References

[1] 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.

[2] 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.

[3] Adam Grabowski. Polygonal numbers. *Formalized Mathematics*, 21(**2**):103–113, 2013. doi:10.2478/forma-2013-0012.

[4] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

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

[6] 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.

[7] Marco Riccardi. Solution of cubic and quartic equations. *Formalized Mathematics*, 17(**2**): 117–122, 2009. doi:10.2478/v10037-009-0012-z.

[8] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**): 247–252, 2008. doi:10.2478/v10037-008-0029-8.

[9] Christoph Schwarzweller. Proth numbers. *Formalized Mathematics*, 22(**2**):111–118, 2014. doi:10.2478/forma-2014-0013.

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

Accepted July 23, 2022