FORMALIZED MATHEMATICS
Volume 31, 2023, Pages 87–100
DOI: 10.2478/forma-2023-0009
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part VIII

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper problems 25, 86, 88, 105, 111, 137–142, and 184–185 from [12] are formalized, using the Mizar formalism [3], [1], [4]. This is a continuation of the work from [5], [6], and [2] as suggested in [8]. The automatization of selected lemmas from [11] proven in this paper as proposed in [9] could be an interesting future work.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes; factorization

MML identifier: `NUMBER08`, version: `8.1.12 5.75.1447`

1. Preliminaries

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i, j denote integers, r, s denote real numbers, and p, p_1, p_2, p_3, q denote prime numbers.

Let us consider n and r. Let us observe that $n-r+r$ is natural and $n+r-r$ is natural. Now we state the propositions:

(1) Let us consider natural numbers m, n. If $m < n < m+2$, then $n = m+1$.

(2) $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$.

Let us note that $\mathbb{N}_+$ is infinite. Now we state the propositions:

(3) Let us consider finite sequences f, g. Suppose $f \frown g$ is X-valued. Then

(i) f is X-valued, and

(ii) g is X-valued.

(4) Let us consider complex-valued many sorted sets f_1, f_2, f_3 indexed by X. Suppose for every object x such that $x \in X$ holds $f_1(x) = f_2(x) \cdot f_3(x)$. Then $f_1 = f_2 \cdot f_3$.

(5) If $b \neq 0$ and $c \neq 0$, then $\frac{r \cdot b + c}{b} > r$.

(6) If $m \leqslant n$, then $m! \mid n!$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $m \leqslant \$_1$, then $m! \mid \$_1!$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(7) If $p_1 \mid p_2$, then $p_1 = p_2$.

(8) If m and n are relatively prime, then $a \cdot n + m$ and n are relatively prime.

(9) If $n \mid 27$, then $n = 1$ or $n = 3$ or $n = 9$ or $n = 27$.

2. Problem 25

Now we state the proposition:

(10) Let us consider a function f. Then support(EmptyBag $X {+\cdot} f$) = support f.

Let X be a set and f be a finite-support function.

Observe that EmptyBag $X {+\cdot} f$ is finite-support.

Let p be a prime number and n be a non zero natural number. Observe that p-count(p^n) is non zero. Now we state the propositions:

(11) Let us consider a finite-support function b.
Then $\mathrm{dom}(b \cdot (\mathrm{CFS}(\mathrm{support}\, b))) = \mathrm{dom}(\mathrm{CFS}(\mathrm{support}\, b))$.

(12) Let us consider complex-valued functions f, g. Then $\mathrm{support}(f \cdot g) \subseteq \mathrm{support}\, f$.

Let f, g be finite-support, complex-valued functions. One can verify that $f \cdot g$ is finite-support. Now we state the propositions:

(13) Let us consider complex-valued functions f, g. Suppose $\mathrm{support}\, f = \mathrm{support}\, g$. Then $\mathrm{support}(f \cdot g) = \mathrm{support}\, f$. The theorem is a consequence of (12).

(14) Let us consider finite-support, complex-valued many sorted sets b_1, b_2 indexed by X. Suppose $\mathrm{support}\, b_1 = \mathrm{support}\, b_2$. Then $\prod(b_1 \cdot b_2) = (\prod b_1) \cdot (\prod b_2)$.

PROOF: Set $b_0 = b_1 \cdot b_2$. $\mathrm{support}\, b_0 = \mathrm{support}\, b_1$. $\mathrm{support}\, b_0 = \mathrm{support}\, b_2$. Consider f_0 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_0 = \prod f_0$ and $f_0 = b_0 \cdot (\mathrm{CFS}(\mathrm{support}\, b_0))$. Consider f_1 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_1 = \prod f_1$ and $f_1 = b_1 \cdot (\mathrm{CFS}(\mathrm{support}\, b_1))$. Consider f_2 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_2 = \prod f_2$ and $f_2 =$

$b_2 \cdot$(CFS(support b_2)). dom($b_0 \cdot$(CFS(support b_0))) = dom(CFS(support b_0)). dom f_0 = dom f_1. dom f_0 = dom f_2. For every object c such that $c \in$ dom f_0 holds $f_0(c) = f_1(c) \cdot f_2(c)$. □

Let n be a non zero natural number. The functor EulerFactorization(n) yielding a function is defined by

(Def. 1) dom *it* = support PPF(n) and for every natural number p such that $p \in$ dom *it* there exists a non zero natural number c such that $c = p$-count(n) and $it(p) = p^c - p^{c-1}$.

Observe that dom(EulerFactorization(n)) is finite and EulerFactorization(n) is $\mathbb{P}$-defined. Now we state the propositions:

(15) Let us consider a non zero natural number n, and an object p. Suppose $p \in$ dom(EulerFactorization(n)). Then p is a prime number.

(16) Let us consider a non zero natural number n, and a natural number p. Suppose $p \in$ dom(EulerFactorization(n)). Then there exists a non zero natural number c such that

(i) $c = p$-count(n), and

(ii) (EulerFactorization(n))(p) $= p^{c-1} \cdot (p-1)$.

Let n be a non zero natural number. Let us observe that EulerFactorization(n) is natural-valued and EulerFactorization(n) is finite-support and EulerFactorization(1) is empty. Now we state the propositions:

(17) Let us consider a non zero natural number n. Then EulerFactorization(p^n) $= p \dot{\longmapsto} (p^n - p^{n-1})$.

(18) EulerFactorization(p) $= p \dot{\longmapsto} (p-1)$. The theorem is a consequence of (17).

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

(19) support EulerFactorization(n) = dom(EulerFactorization(n)). The theorem is a consequence of (15).

(20) If $n > 1$, then support EulerFactorization(n) is not empty.

(21) If $n > 1$, then EulerFactorization(n) is not empty. The theorem is a consequence of (20).

Let us consider non zero natural numbers s, t. Now we state the propositions:

(22) If s and t are relatively prime, then dom(EulerFactorization(s)) misses dom(EulerFactorization(t)).

(23) Suppose s and t are relatively prime. Then EmptyBag $\mathbb{P}$+· EulerFactorization($s \cdot t$) = (EmptyBag $\mathbb{P}$+· EulerFactorization(s))+(EmptyBag $\mathbb{P}$+· EulerFactorization(t)).

PROOF: Set $n = s \cdot t$. Set $N = \mathrm{EulerFactorization}(n)$. Set $S = \mathrm{EulerFactorization}(s)$. Set $T = \mathrm{EulerFactorization}(t)$. For every object x such that $x \in \mathbb{P}$ holds $(B{+}{\cdot}N)(x) = (B{+}{\cdot}S)(x) + (B{+}{\cdot}T)(x)$ by [7, (25), (58)], (22). $\square$

(24) Let us consider a non zero natural number n. Then $\mathrm{Euler}\, n = \prod(\mathrm{EmptyBag}\, \mathbb{P} {+}{\cdot}\, \mathrm{EulerFactorization}(n))$.
PROOF: Set $N = \mathrm{EulerFactorization}(n)$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero natural number n such that $\mathrm{support}(B{+}{\cdot}\, \mathrm{EulerFactorization}(n)) \subseteq \mathrm{Seg}\, \$_1$ holds $\prod(B{+}{\cdot}\, \mathrm{EulerFactorization}(n)) = \mathrm{Euler}\, n$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. Set $G = B{+}{\cdot}N$. $\mathrm{support}\, G = \mathrm{support}\, N$. $\square$

Let n be a non zero natural number. The functor $\mathrm{EulerFactorization}_1(n)$ yielding a function is defined by

(Def. 2) $\mathrm{dom}\, it = \mathrm{support}\, \mathrm{PPF}(n)$ and for every natural number p such that $p \in \mathrm{dom}\, it$ there exists a non zero natural number c such that $c = p\text{-count}(n)$ and $it(p) = p^{c-1}$.

Let us observe that $\mathrm{dom}(\mathrm{EulerFactorization}_1(n))$ is finite and $\mathrm{EulerFactorization}_1(n)$ is $\mathbb{P}$-defined. Now we state the proposition:

(25) Let us consider a non zero natural number n, and an object p. Suppose $p \in \mathrm{dom}(\mathrm{EulerFactorization}_1(n))$. Then p is a prime number.

Let n be a non zero natural number. Note that $\mathrm{EulerFactorization}_1(n)$ is natural-valued and $\mathrm{EulerFactorization}_1(n)$ is finite-support. Now we state the proposition:

(26) Let us consider a non zero natural number n. Then $\mathrm{support}\, \mathrm{EulerFactorization}_1(n) = \mathrm{dom}(\mathrm{EulerFactorization}_1(n))$. The theorem is a consequence of (25).

Let n be a non zero natural number. The functor $\mathrm{EulerFactorization}_2(n)$ yielding a function is defined by

(Def. 3) $\mathrm{dom}\, it = \mathrm{support}\, \mathrm{PPF}(n)$ and for every natural number p such that $p \in \mathrm{dom}\, it$ holds $it(p) = p - 1$.

One can verify that $\mathrm{dom}(\mathrm{EulerFactorization}_2(n))$ is finite and $\mathrm{EulerFactorization}_2(n)$ is $\mathbb{P}$-defined. Now we state the proposition:

(27) Let us consider a non zero natural number n, and an object p. Suppose $p \in \mathrm{dom}(\mathrm{EulerFactorization}_2(n))$. Then p is a prime number.

Let n be a non zero natural number. Let us note that $\mathrm{EulerFactorization}_2(n)$ is natural-valued and $\mathrm{EulerFactorization}_2(n)$ is finite-support.

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

(28) support EulerFactorization$_2(n)$ = dom(EulerFactorization$_2(n)$). The theorem is a consequence of (27).

(29) EmptyBag $\mathbb{P}$+· EulerFactorization(n) = (EmptyBag $\mathbb{P}$+· EulerFactorization$_1(n)$) · (EmptyBag $\mathbb{P}$+· EulerFactorization$_2(n)$).

PROOF: Set N = EulerFactorization(n). Set S = EulerFactorization$_1(n)$. Set T = EulerFactorization$_2(n)$. For every object x such that $x \in \mathbb{P}$ holds $(B{+}{\cdot}N)(x) = (B{+}{\cdot}S)(x) \cdot (B{+}{\cdot}T)(x)$. □

(30) Let us consider integer-valued finite sequences f_1, f_2. Suppose len f_1 = len f_2 and for every n such that $1 \leqslant n \leqslant$ len f_1 holds $f_1(n) \mid f_2(n)$. Then $\prod f_1 \mid \prod f_2$.

(31) Let us consider a non zero natural number n. Then $\prod$(EmptyBag $\mathbb{P}$+· EulerFactorization$_1(n)$) $\mid n$.

PROOF: Set b_0 = PPF(n). Set F_1 = EulerFactorization$_1(n)$. Set b_1 = $B{+}{\cdot}F_1$. Consider f_0 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_0 = \prod f_0$ and $f_0 = b_0 \cdot$ (CFS(support b_0)). Consider f_1 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_1 = \prod f_1$ and $f_1 = b_1 \cdot$ (CFS(support b_1)). support b_1 = support F_1. support F_1 = dom F_1. dom f_0 = dom(CFS(support b_0)). dom f_1 = dom(CFS(support b_1)). For every natural number x such that $1 \leqslant x \leqslant$ len f_1 holds $f_1(x) \mid f_0(x)$. $\prod f_1 \mid \prod f_0$. □

Let f be a real-valued function and r be a real number. We say that $f \leqslant r$ if and only if

(Def. 4) for every object x such that $x \in$ dom f holds $f(x) \leqslant r$.

Now we state the propositions:

(32) Let us consider a real-valued function f, and real numbers r_1, r_2. If $f \leqslant r_1 \leqslant r_2$, then $f \leqslant r_2$.

(33) Let us consider real-valued functions f, g. If rng $g \subseteq$ rng f and $f \leqslant n$, then $g \leqslant n$.

Let us consider extended real-valued finite sequences f, g. Now we state the propositions:

(34) If $f \frown g$ is increasing, then f is increasing and g is increasing.

(35) If $f \frown g$ is positive yielding, then f is positive yielding and g is positive yielding.

(36) Let us consider a natural-valued finite sequence f. If $f \leqslant n$ and f is increasing and positive yielding, then $\prod f \mid n!$. The theorem is a consequence of (3), (34), (35), and (6).

Let f be a natural-valued finite sequence. Note that sort$_{\rm a}$ f is natural-valued and sort$_{\rm d}$ f is natural-valued. Let f be an integer-valued finite sequence. One can check that $\mathrm{sort_a}\, f$ is integer-valued and $\mathrm{sort_d}\, f$ is integer-valued. Let f be a rational-valued finite sequence. One can verify that $\mathrm{sort_a}\, f$ is rational-valued and $\mathrm{sort_d}\, f$ is rational-valued. Now we state the proposition:

(37) Let us consider binary relations P, R. Suppose $\mathrm{rng}\, R \subseteq \mathrm{rng}\, P$ and P is positive yielding. Then R is positive yielding.

Let f be a positive yielding, real-valued finite sequence. Let us observe that $\mathrm{sort_a}\, f$ is positive yielding and every function which is $\mathbb{P}$-defined is also $\mathbb{N}$-defined. Now we state the propositions:

(38) Let us consider a real-valued, finite-support function f. Suppose $f \leqslant n$. Let us consider a real-valued finite sequence F. Suppose $F = (\mathrm{EmptyBag}\, \mathbb{P} +\cdot f) \cdot (\mathrm{CFS}(\mathrm{support}(\mathrm{EmptyBag}\, \mathbb{P} +\cdot f)))$. Then $F \leqslant n$.

(39) Let us consider a natural-valued, finite-support function f, and a real-valued finite sequence F.
Suppose $F = (\mathrm{EmptyBag}\, \mathbb{P} +\cdot f) \cdot (\mathrm{CFS}(\mathrm{support}(\mathrm{EmptyBag}\, \mathbb{P} +\cdot f)))$. Then F is positive yielding. The theorem is a consequence of (11).

Let us consider a natural-valued, finite-support, $\mathbb{P}$-defined function f and a real-valued finite sequence F. Now we state the propositions:

(40) Suppose f is increasing. Then suppose $F = (\mathrm{EmptyBag}\, \mathbb{P} +\cdot f) \cdot (\mathrm{CFS}(\mathrm{support}(\mathrm{EmptyBag}\, \mathbb{P} +\cdot f)))$. Then $\mathrm{sort_a}\, F$ is one-to-one. The theorem is a consequence of (10) and (11).

(41) Suppose f is increasing. Then suppose $F = (\mathrm{EmptyBag}\, \mathbb{P} +\cdot f) \cdot (\mathrm{CFS}(\mathrm{support}(\mathrm{EmptyBag}\, \mathbb{P} +\cdot f)))$. Then $\mathrm{sort_a}\, F$ is increasing. The theorem is a consequence of (11) and (10).

(42) Let us consider a natural-valued, finite-support, $\mathbb{P}$-defined function f. Suppose $f \leqslant n$ and f is increasing. Then $\prod(\mathrm{EmptyBag}\, \mathbb{P} +\cdot f) \mid n!$. The theorem is a consequence of (38), (39), (41), (33), and (36).

(43) Let us consider a non zero natural number n. Then $\mathrm{EulerFactorization}_2(n) \leqslant n - 1$. The theorem is a consequence of (27).

Let n be a non zero natural number. Let us note that $\mathrm{EulerFactorization}_2(n)$ is increasing and $\mathrm{EulerFactorization}_2(n)$ is positive yielding.

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

(44) $\prod(\mathrm{EmptyBag}\, \mathbb{P} +\cdot \mathrm{EulerFactorization}_2(n)) \mid (n-1)!$.

(45) $\mathrm{Euler}\, n \mid n!$. The theorem is a consequence of (24), (31), (43), (42), (10), (26), (28), (29), and (14).

(46) Let us consider an odd natural number n. Then $n \mid 2^{n!} - 1$. The theorem is a consequence of (45).

3. Problem 86

Now we state the proposition:

(47) Suppose p_1, p_2, p_3 are mutually different. Then

(i) $p_1 \geqslant 2$ and $p_2 \geqslant 3$ and $p_3 \geqslant 5$, or

(ii) $p_1 \geqslant 2$ and $p_2 \geqslant 5$ and $p_3 \geqslant 3$, or

(iii) $p_1 \geqslant 3$ and $p_2 \geqslant 2$ and $p_3 \geqslant 5$, or

(iv) $p_1 \geqslant 3$ and $p_2 \geqslant 5$ and $p_3 \geqslant 2$, or

(v) $p_1 \geqslant 5$ and $p_2 \geqslant 2$ and $p_3 \geqslant 3$, or

(vi) $p_1 \geqslant 5$ and $p_2 \geqslant 3$ and $p_3 \geqslant 2$.

Let n be a natural number. We say that n satisfies Sierpiński Problem 86 if and only if

(Def. 5) there exist prime numbers p_1, p_2, p_3 such that p_1, p_2, p_3 are mutually different and $n^2 - 1 = p_1 \cdot p_2 \cdot p_3$.

Now we state the propositions:

(48) If n satisfies Sierpiński Problem 86, then $n \geqslant 6$. The theorem is a consequence of (47).

(49) Let us consider prime numbers a, b, c. If $n^2 - 1 = a \cdot b \cdot c$, then $n - 1$ is prime or $n + 1$ is prime.

(50) Suppose n satisfies Sierpiński Problem 86. Then

(i) $n - 1$ is prime and there exist prime numbers x, y such that $x \neq y$ and $n + 1 = x \cdot y$, or

(ii) $n + 1$ is prime and there exist prime numbers x, y such that $x \neq y$ and $n - 1 = x \cdot y$.

The theorem is a consequence of (49).

(51) If n satisfies Sierpiński Problem 86, then n is even. The theorem is a consequence of (50) and (48).

(52) $14^2 - 1 = 3 \cdot 5 \cdot 13$.

(53) $16^2 - 1 = 3 \cdot 5 \cdot 17$.

(54) $20^2 - 1 = 3 \cdot 7 \cdot 19$.

(55) $22^2 - 1 = 3 \cdot 7 \cdot 23$.

(56) $32^2 - 1 = 3 \cdot 11 \cdot 31$.

(57) 14 satisfies Sierpiński Problem 86. The theorem is a consequence of (52).

(58) 16 satisfies Sierpiński Problem 86. The theorem is a consequence of (53).

(59) 20 satisfies Sierpiński Problem 86. The theorem is a consequence of (54).

(60) 22 satisfies Sierpiński Problem 86. The theorem is a consequence of (55).

(61) 32 satisfies Sierpiński Problem 86. The theorem is a consequence of (56).

(62) If n satisfies Sierpiński Problem 86 and $n \leqslant 32$, then $n \in \{14, 16, 20, 22, 32\}$. The theorem is a consequence of (48).

4. Problem 184

Now we state the propositions:

(63) $3^{2 \cdot k} \equiv 1 \pmod 8$.

(64) $8 \nmid 3^n + 1$. The theorem is a consequence of (63).

(65) If $n \neq 0$ and $2^m - 3^n = 1$, then $m = 2$ and $n = 1$. The theorem is a consequence of (64).

5. Problem 185

Now we state the propositions:

(66) $3^{2 \cdot k} \equiv 1 \pmod 4$.

(67) If $2^n \bmod 4 = 2$, then $n = 1$.

(68) If $2^m - 2^n = 2$, then $m = 2$ and $n = 1$.

(69) If n is odd and $3^n - 2^m = 1$, then $n = m = 1$. The theorem is a consequence of (66) and (67).

(70) If n is even and $3^n - 2^m = 1$, then $n = 2$ and $m = 3$. The theorem is a consequence of (68).

(71) If $3^n - 2^m = 1$, then $n = m = 1$ or $n = 2$ and $m = 3$. The theorem is a consequence of (69) and (70).

6. Problem 88

Let us consider n. We say that n has unique prime divisor if and only if

(Def. 6) there exists a prime number p such that $p \mid n$ and for every prime number r such that $r \neq p$ holds $r \nmid n$.

Assume n has unique prime divisor. The only divisor of n yielding a prime number is defined by

(Def. 7) $it \mid n$ and for every prime number r such that $r \neq it$ holds $r \nmid n$.

Now we state the proposition:

(72) If n has unique prime divisor and $p \mid n$, then the only divisor of $n = p$.

Let us observe that every natural number which is prime has unique prime divisor. Now we state the proposition:

(73) The only divisor of $p = p$.

One can check that every natural number which is zero does not have unique prime divisor. Now we state the proposition:

(74) 1 does not have unique prime divisor.

Let p be a prime number. Let us observe that p^0 does not have unique prime divisor. Let k be a non zero natural number. One can verify that p^k has unique prime divisor. Now we state the propositions:

(75) If $p_1 \neq p_2$, then $p_1 \cdot p_2$ does not have unique prime divisor.

(76) If n has unique prime divisor, then there exists a non zero natural number k such that $n = (\text{the only divisor of } n)^k$.

(77) If $n > 7$, then there exists a natural number m and there exist prime numbers p, q such that $p \neq q$ and ($m = n$ or $m = n + 1$ or $m = n + 2$) and $p \mid m$ and $q \mid m$.

Proof: Consider k such that $n = 6 \cdot k$ or $n = 6 \cdot k + 1$ or $n = 6 \cdot k + 2$ or $n = 6 \cdot k + 3$ or $n = 6 \cdot k + 4$ or $n = 6 \cdot k + 5$. n has unique prime divisor. $n + 1$ has unique prime divisor. $n + 2$ has unique prime divisor. □

7. Problem 105

Let us consider n. We say that n has more than two different prime divisors if and only if

(Def. 8) there exist prime numbers q_1, q_2, q_3 such that q_1, q_2, q_3 are mutually different and $q_1 \mid n$ and $q_2 \mid n$ and $q_3 \mid n$.

Let n be a non zero natural number. We say that n satisfies Sierpiński Problem 105 if and only if

(Def. 9) $n - 1$ has more than two different prime divisors and $n + 1$ has more than two different prime divisors.

Now we state the proposition:

(78) If n has unique prime divisor, then n has no more than two different prime divisors.

Note that every natural number which is zero has more than two different prime divisors. Now we state the proposition:

(79) If $n > 0$ and n has more than two different prime divisors, then $n \geqslant 30$. The theorem is a consequence of (47).

Let us note that every natural number which is prime does not have more than two different prime divisors. Let us consider p_1 and p_2. Observe that $p_1 \cdot p_2$ does not have more than two different prime divisors.

Let us consider p and n. Let us note that p^n does not have more than two different prime divisors. Let us consider p, q, m and n. Note that $p^m \cdot q^n$ does not have more than two different prime divisors. Now we state the propositions:

(80) 131 satisfies Sierpiński Problem 105.

(81) There exists no prime number p such that $p \leqslant 130$ and p satisfies Sierpiński Problem 105. The theorem is a consequence of (79).

8. Problem 111

Now we state the propositions:

(82) $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$.

(83) $m \mid p^4$ if and only if $m \in \{1, p, p^2, p^3, p^4\}$.

(84) $1 + p + p^2 + p^3 + p^4$ is a square if and only if $p = 3$.

(85) The set of positive divisors of $p^4 = \{1, p, p^2, p^3, p^4\}$. The theorem is a consequence of (83).

(86) $\{p$, where p is a prime number : $1 + p + p^2 + p^3 + p^4$ is a square$\} = \{3\}$. The theorem is a consequence of (84).

9. Problem 137

Let D be a non empty set. Let us observe that every sequence of D is total. Let f be a $(\mathbb{C} \times D)$-valued many sorted set indexed by $\mathbb{N}$ and n be a natural number. Note that $(f(n))_{\mathbf{1}}$ is complex. Let f be a $(D \times \mathbb{C})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is complex.

Let f be an $(\mathbb{R} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is real. Let f be a $(D \times \mathbb{R})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is real. Let f be a $(\mathbb{Q} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is rational. Let f be a $(D \times \mathbb{Q})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is rational.

Let f be a $(\mathbb{Z} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is integer. Let f be a $(D \times \mathbb{Z})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is integer. Let f be an $(\mathbb{N} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is natural. Let f be a $(D \times \mathbb{N})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is natural.

Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be complex numbers. The functor recSeqCart(a, $b, x_1, x_2, x_3, y_1, y_2, y_3$) yielding a $(\mathbb{C} \times \mathbb{C})$-valued many sorted set indexed by $\mathbb{N}$ is defined by

(Def. 10) $it(0) = \langle a, b \rangle$ and for every natural number n, $it(n+1) = \langle x_1 \cdot ((it(n))_{\mathbf{1}}) + x_2 \cdot ((it(n))_{\mathbf{2}}) + x_3, y_1 \cdot ((it(n))_{\mathbf{1}}) + y_2 \cdot ((it(n))_{\mathbf{2}}) + y_3 \rangle$.

Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be real numbers. Let us observe that recSeqCart $(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{R} \times \mathbb{R})$-valued. Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be rational numbers. Let us observe that recSeqCart$(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{Q} \times \mathbb{Q})$-valued.

Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be integers. Let us observe that recSeqCart$(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{Z} \times \mathbb{Z})$-valued. Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be natural numbers. Let us observe that recSeqCart$(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{N} \times \mathbb{N})$-valued. Let us consider real numbers a, b, a_1, a_2, a_3, b_1, b_2, b_3 and a natural number n. Now we state the propositions:

(87) Suppose $a > 0$ and $b > 0$ and $a_3 \geqslant 0$ and $b_3 \geqslant 0$ and ($a_1 > 0$ and $a_2 \geqslant 0$ or $a_1 \geqslant 0$ and $a_2 > 0$) and ($b_1 > 0$ and $b_2 \geqslant 0$ or $b_1 \geqslant 0$ and $b_2 > 0$). Then

(i) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{1}} > 0$, and

(ii) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{2}} > 0$.

PROOF: Set $f = \text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$. Define $\mathcal{P}$[natural number] $\equiv (f(\$_1))_{\mathbf{1}} > 0$ and $(f(\$_1))_{\mathbf{2}} > 0$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(88) Suppose $a \geqslant 0$ and $b \geqslant 0$ and $a_1 \geqslant 0$ and $a_2 \geqslant 0$ and $a_3 \geqslant 0$ and $b_1 \geqslant 0$ and $b_2 \geqslant 0$ and $b_3 \geqslant 0$. Then

(i) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{1}} \geqslant 0$, and

(ii) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{2}} \geqslant 0$.

PROOF: Set $f = \text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$. Define $\mathcal{P}$[natural number] $\equiv (f(\$_1))_{\mathbf{1}} \geqslant 0$ and $(f(\$_1))_{\mathbf{2}} \geqslant 0$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(89) Let us consider real numbers a, b, a_1, a_2, a_3, b_1, b_2, b_3. Suppose $a > 0$ and $b > 0$ and $a_1 \geqslant 1$ and $a_2 > 0$ and $a_3 \geqslant 0$ and $b_1 > 0$ and $b_2 \geqslant 1$ and $b_3 \geqslant 0$. Let us consider natural numbers m, n. Suppose $m > n$. Then

(i) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(m))_{\mathbf{1}} > ((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{1}}$, and

(ii) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(m))_{\mathbf{2}} > ((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{2}}$.

Proof: Set $f = \operatorname{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 > n$, then $(f(\$_1))_{\mathbf{1}} > (f(n))_{\mathbf{1}}$ and $(f(\$_1))_{\mathbf{2}} > (f(n))_{\mathbf{2}}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(90) Let us consider real numbers a, b, a_1, a_2, a_3, b_1, b_2, b_3. Suppose $a > 0$ and $b > 0$ and $a_1 \geqslant 1$ and $a_2 > 0$ and $a_3 \geqslant 0$ and $b_1 > 0$ and $b_2 \geqslant 1$ and $b_3 \geqslant 0$. Then $\operatorname{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$ is one-to-one. The theorem is a consequence of (89).

(91) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $3 \cdot x^{\mathbf{2}} - 7 \cdot y^{\mathbf{2}} + 1 = 0\}$ is infinite.
Proof: Define $\mathcal{R}(\text{complex number}, \text{complex number}) = 3 \cdot \$_1^{\mathbf{2}} - 7 \cdot \$_2^{\mathbf{2}} + 1$. Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x, y) = 0\}$. Define $\mathcal{G}(\text{real number}, \text{real number}) = 55 \cdot \$_1 + 84 \cdot \$_2 + 0$. Define $\mathcal{H}(\text{real number}, \text{real number}) = 36 \cdot \$_1 + 55 \cdot \$_2 + 0$. Define $\mathcal{P}$[object, element of $\mathbb{N} \times \mathbb{N}$, element of $\mathbb{N} \times \mathbb{N}$] $\equiv \$_3 = \langle \mathcal{G}((\$_2)_{\mathbf{1}}, (\$_2)_{\mathbf{2}}), \mathcal{H}((\$_2)_{\mathbf{1}}, (\$_2)_{\mathbf{2}})\rangle$. Set $f = \operatorname{recSeqCart}(3, 2, 55, 84, 0, 36, 55, 0)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1) \in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. $\operatorname{rng} f \subseteq A$. f is one-to-one. $\square$

10. Problem 138

One can check that there exists a set which is infinite and natural-membered. Now we state the propositions:

(92) If $i \mid p$, then $i = 1$ or $i = -1$ or $i = p$ or $i = -p$.

(93) $\{\langle x, y\rangle$, where x, y are integers : $2 \cdot x^3 + x \cdot y - 7 = 0\} = \{\langle 1, 5\rangle, \langle 7, -97\rangle, \langle -1, -9\rangle, \langle -7, -99\rangle\}$.
Proof: Set $A = \{\langle x, y\rangle$, where x, y are integers : $2 \cdot x^3 + x \cdot y - 7 = 0\}$. Set $B = \{\langle 1, 5\rangle, \langle 7, -97\rangle, \langle -1, -9\rangle, \langle -7, -99\rangle\}$. $A \subseteq B$ by [10, (2)], (92). $\square$

(94) Let us consider a complex number r. If $r \neq 0$, then $2 \cdot (\frac{7}{r})^3 + \frac{7}{r} \cdot (r - \frac{98}{r^{\mathbf{2}}}) - 7 = 0$.

(95) If $n^3 \leqslant 98$, then $n \leqslant 4$.

(96) $\{\langle x, y\rangle$, where x, y are positive rational numbers : $2 \cdot x^3 + x \cdot y - 7 = 0\}$ is infinite.
Proof: Define $\mathcal{R}(\text{rational number}, \text{rational number}) = 2 \cdot {\$_1}^3 + \$_1 \cdot \$_2 - 7$. Set $A = \{\langle x, y\rangle$, where x, y are positive rational numbers : $\mathcal{R}(x, y) = 0\}$. Define $\mathcal{G}(\text{natural number}) = \frac{7}{\$_1}$. Define $\mathcal{H}(\text{natural number}) = \$_1 - \frac{98}{\$_1^{\mathbf{2}}}$. Define $\mathcal{F}(\text{natural number}) = \langle \mathcal{G}(\$_1), \mathcal{H}(\$_1)\rangle$. Set $D = \mathbb{N} \setminus \{0, 1, 2, 3, 4\}$. Consider f being a many sorted set indexed by D such that for every element d of D, $f(d) = \mathcal{F}(d)$. $\operatorname{rng} f \subseteq A$. f is one-to-one. $\square$

11. PROBLEM 139

Now we state the proposition:

(97) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $(x-1)^{\mathbf{2}}+(x+1)^{\mathbf{2}} = y^{\mathbf{2}}+1\}$ is infinite.

PROOF: Define $\mathcal{R}$(natural number, natural number) $= (\$_1-1)^{\mathbf{2}}+(\$_1+1)^{\mathbf{2}}-(\$_2^{\mathbf{2}}+1)$. Set $A=\{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x,y)=0\}$. Define $\mathcal{G}$(natural number, natural number) $=3\cdot\$_1+2\cdot\$_2+0$. Define $\mathcal{H}$(natural number, natural number) $=4\cdot\$_1+3\cdot\$_2+0$. Define $\mathcal{P}$[object, element of $\mathbb{N}\times\mathbb{N}$, element of $\mathbb{N}\times\mathbb{N}$] $\equiv \$_3=\langle\mathcal{G}((\$_2)_{\mathbf{1}},(\$_2)_{\mathbf{2}}), \mathcal{H}((\$_2)_{\mathbf{1}},(\$_2)_{\mathbf{2}})\rangle$. Set $f=\mathrm{recSeqCart}(2,3,3,2,0,4,3,0)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1)\in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. $\mathrm{rng}\, f\subseteq A$. f is one-to-one. Define $\mathcal{R}$[natural number, natural number] $\equiv (\$_1-1)^{\mathbf{2}}+(\$_1+1)^{\mathbf{2}} = \$_2^{\mathbf{2}}+1$. Set $B=\{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}[x,y]\}$. $A=B$. □

12. PROBLEM 140

Let a be a rational number and n be a natural number. Let us observe that a^n is rational. Let i be an integer. One can verify that a^i is rational. Now we state the propositions:

(98) If $n>1$, then $3^n-3^{1-n}-2>0$.

(99) If $n>1$, then $3^n+3^{1-n}-4>0$.

(100) Let us consider complex numbers x, y. Suppose $x=\frac{3^n-3^{1-n}-2}{4}$ and $y=\frac{3^n+3^{1-n}-4}{8}$. Then $x\cdot(x+1)=4\cdot y\cdot(y+1)$.

(101) If $m<n$, then $3^m-3^{1-m}<3^n-3^{1-n}$.

(102) There exist no positive natural numbers x, y such that $x\cdot(x+1) = 4\cdot y\cdot(y+1)$.

(103) $\{\langle x, y\rangle$, where x, y are positive rational numbers : $x\cdot(x+1)=4\cdot y\cdot(y+1)\}$ is infinite.

PROOF: Define $\mathcal{R}$(complex number, complex number) $=\$_1\cdot(\$_1+1)-4\cdot\$_2\cdot(\$_2+1)$. Set $A=\{\langle x, y\rangle$, where x, y are positive rational numbers : $\mathcal{R}(x,y)=0\}$. Define $\mathcal{G}$(natural number) $=\frac{3^{\$_1}-3^{1-\$_1}-2}{4}$. Define $\mathcal{H}$(natural number) $=\frac{3^{\$_1}+3^{1-\$_1}-4}{8}$. Define $\mathcal{F}$(natural number) $=\langle\mathcal{G}(\$_1), \mathcal{H}(\$_1)\rangle$. Set $D=\mathbb{N}\setminus\{0,1\}$. Consider f being a many sorted set indexed by D such that for every element d of D, $f(d)=\mathcal{F}(d)$. $\mathrm{rng}\, f\subseteq A$. f is one-to-one. Define $\mathcal{R}$[complex number, complex number] $\equiv \$_1\cdot(\$_1+1)=4\cdot\$_2\cdot(\$_2+1)$. Set $B=\{\langle x, y\rangle$, where x, y are positive rational numbers : $\mathcal{R}[x,y]\}$. $A=B$. □

13. Problem 141

Now we state the propositions:

(104) If $m \neq 0$ and $p^m \mid a \cdot b$, then $p \mid a$ or $p \mid b$.

(105) If a and b are relatively prime and $p^n \mid a \cdot b$, then $p^n \mid a$ or $p^n \mid b$.

(106) If $n \neq 0$, then there exist no positive natural numbers x, y such that $x \cdot (x+1) = p^{2 \cdot n} \cdot y \cdot (y+1)$. The theorem is a consequence of (105).

14. Problem 142

Now we state the proposition:

(107) Let us consider natural numbers k, x, y. Suppose $x^{\mathbf{2}} - 2 \cdot y^{\mathbf{2}} = k$. Let us consider natural numbers t, u. If $t = x - 2 \cdot y$ and $u = x - y$, then $t^{\mathbf{2}} - 2 \cdot u^{\mathbf{2}} = -k$.

References

[1] 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.

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

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[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. Elementary number theory problems. Part IV. *Formalized Mathematics*, 30(**3**):223–228, 2022. doi:10.2478/forma-2022-0017.

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

[7] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[8] 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.

[9] Adam Naumowicz. Extending numeric automation for number theory formalizations in Mizar. In Catherine Dubois and Manfred Kerber, editors, *Intelligent Computer Mathematics – 16th International Conference, CICM 2023, Cambridge, UK, September 5–8, 2023, Proceedings*, volume 14101 of *Lecture Notes in Computer Science*, pages 309–314. Springer, 2023. doi:10.1007/978-3-031-42753-4_23.

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

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

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

Accepted June 30, 2023