FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 223–228, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0017

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part IV

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Summary. In this paper problems 17, 18, 26, 27, 28, and 98 from [9] are formalized, using the Mizar formalism [8], [2], [3], [6].

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: `NUMBER04`, version: `8.1.12 5.71.1431`

1. Preliminaries

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i denotes an integer, r denotes a real number, and p denotes a prime number.

Let p be a prime number. One can verify that 1 mod p reduces to 1.

Let us consider n. One can verify that $\varepsilon_{\mathbb{N}}$ mod n reduces to $\varepsilon_{\mathbb{N}}$ and $\varepsilon_{\mathbb{Z}}$ mod n reduces to $\varepsilon_{\mathbb{Z}}$. Now we state the proposition:

(1) Let us consider a non empty, natural-membered set X. Suppose for every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$. Then X is infinite.

Let us note that $\mathbb{N}_{\rm even}$ is infinite and $\mathbb{N}_{\rm odd}$ is infinite and every element of $\mathbb{N}_{\rm even}$ is even and every element of $\mathbb{N}_{\rm odd}$ is odd. Now we state the propositions:

(2) $n \bmod (k+1) = 0$ or ... or $n \bmod (k+1) = k$.

(3) Let us consider integers a, b, c. If $a \cdot b \mid c$, then $a \mid c$ and $b \mid c$.

(4) Let us consider integers a, b, m. If $a \equiv b \pmod m$, then $m \nmid a$ or $m \mid b$.

(5) If k is odd, then $(-1)^k \equiv -1 \pmod{n}$.

(6) Let us consider integers a, b. Suppose $k \neq 0$ and $a \equiv b \pmod{n^k}$. Then $a \equiv b \pmod{n}$.

(7) $2^{4 \cdot n} \equiv 1 \pmod{5}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv 2^{4 \cdot \$_1} \equiv 1 \pmod{5}$. $\mathcal{P}[0]$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(8) $2^{12 \cdot n} \equiv 1 \pmod{13}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv 2^{12 \cdot \$_1} \equiv 1 \pmod{13}$. $\mathcal{P}[0]$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(9) $\langle i \rangle \bmod n = \langle i \bmod n \rangle$.

(10) If $n \neq 0$, then for every integer-valued finite sequence f, $\sum f \equiv \sum (f \bmod n) \pmod{n}$.

PROOF: Define $\mathcal{P}[\text{finite sequence of elements of } \mathbb{Z}] \equiv \sum \$_1 \equiv \sum (\$_1 \bmod n) \pmod{n}$. For every finite sequence p of elements of $\mathbb{Z}$ and for every element x of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$. For every finite sequence p of elements of $\mathbb{Z}$, $\mathcal{P}[p]$. □

(11) If ($a \neq 0$ or $b \neq 0$) and $c \neq 0$ and a, b, c are mutually coprime, then $a \cdot b$ and c are relatively prime.

(12) If ($a \neq 0$ or $b \neq 0$) and $c \neq 0$ and a, b, c are mutually coprime and $a \mid n$ and $b \mid n$ and $c \mid n$, then $a \cdot b \cdot c \mid n$.

(13) If k is odd, then $a^n + 1 \mid a^{n \cdot k} + 1$.

(14) Let us consider an even natural number n. Suppose $n \mid 2^n + 2$. Then there exists a non zero, odd natural number k such that $2^n + 2 = n \cdot k$.

2. Main Problems

Now we state the propositions:

(15) Let us consider an even natural number n. Suppose $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1$. Let us consider a natural number n_1. If $n_1 = 2^n + 2$, then $n_1 - 1 \mid 2^{n_1} + 1$ and $n_1 \mid 2^{n_1} + 2$. The theorem is a consequence of (14) and (13).

(16) $\{n$, where n is a non zero, even natural number : $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1\}$ is infinite.

PROOF: Set $X = \{n$, where n is a non zero, even natural number : $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1\}$. X is natural-membered. For every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$. □

Let i be an integer. We say that i is double odd if and only if

(Def. 1) there exists an odd integer j such that $i = 2 \cdot j$.

Let i be a natural number. Let us observe that i is double odd if and only if the condition (Def. 2) is satisfied.

(Def. 2) there exists an odd natural number j such that $i = 2 \cdot j$.

Note that there exists an integer which is double odd and every integer which is double odd is also even. Let i be an odd integer. Observe that $i^2 + 1$ is double odd and $i^{\mathbf{2}} + 1$ is double odd.

Let r be a complex number and n be a natural number. The functor OddEven-Powers(r, n) yielding a complex-valued finite sequence is defined by

(Def. 3) len $it = n$ and for every natural number i such that $1 \leqslant i \leqslant n$ for every natural number m such that $m = n - i$ holds if i is odd, then $it(i) = r^m$ and if i is even, then $it(i) = -r^m$.

Let r be a real number. Let us observe that OddEvenPowers(r, n) is real-valued. Let r be an integer. Let us observe that OddEvenPowers(r, n) is $\mathbb{Z}$-valued. Let us consider a complex number r. Now we state the propositions:

(17) OddEvenPowers$(r, 1) = \langle 1 \rangle$.

(18) $\sum$ OddEvenPowers$(r, 1) = 1$. The theorem is a consequence of (17).

(19) OddEvenPowers$(r, 2 \cdot (k+1)+1) = \langle r^{2 \cdot k+2}, -r^{2 \cdot k+1} \rangle ^\frown$OddEvenPowers$(r, 2 \cdot k + 1)$.

PROOF: Set $n = 2 \cdot (k+1)+1$. Set $N = 2 \cdot k+1$. Set $f =$ OddEvenPowers(r, n). Set $p = \langle r^{2 \cdot k+2}, -r^{2 \cdot k+1} \rangle$. Set $q =$ OddEvenPowers(r, N). For every natural number x such that $x \in \operatorname{dom} p$ holds $f(x) = p(x)$. For every natural number x such that $x \in \operatorname{dom} q$ holds $f(\operatorname{len} p + x) = q(x)$. $\square$

(20) $\sum$ OddEvenPowers$(r, 2 \cdot k+3) = r^{2 \cdot k+2} - r^{2 \cdot k+1} + \sum$ OddEvenPowers$(r, 2 \cdot k + 1)$. The theorem is a consequence of (19).

(21) $r^{2 \cdot n+1} + 1 = (r + 1) \cdot (\sum$ OddEvenPowers$(r, 2 \cdot n + 1))$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv r^{2 \cdot \$_1+1} + 1 = (r+1) \cdot (\sum$ OddEvenPowers$(r, 2 \cdot \$_1 + 1))$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$. $\mathcal{P}[k]$. $\square$

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

(22) If $p^{k+1} \mid a^{p^k} + 1$, then $p^{k+2} \mid a^{p^{k+1}} + 1$.

PROOF: Set $b = a^{p^k}$. $b \equiv -1 \pmod{p}$. For every natural number L, $b^{2 \cdot L} \equiv 1 \pmod{p}$. For every natural number L, $b^{2 \cdot L+1} \equiv -1 \pmod{p}$ by [1, (34)]. Reconsider $F =$ OddEvenPowers(b, p) as a $\mathbb{Z}$-valued finite sequence. Reconsider $M = F \bmod p$ as a $\mathbb{Z}$-valued finite sequence. For every natural number x such that $1 \leqslant x \leqslant \operatorname{len} F$ holds $M(x) = 1$. Set $P = p \mapsto 1$. For every k such that $k \in \operatorname{dom} P$ holds $M(k) = P(k)$. $\sum F \equiv \sum M \pmod{p}$. $\square$

(23) If $p \mid a + 1$, then $p^{k+1} \mid a^{p^k} + 1$ and $p^k \mid a^{p^k} + 1$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv p^{\$_1+1} \mid a^{p^{\$_1}}+1$. For every natural number x such that $\mathcal{P}[x]$ holds $\mathcal{P}[x+1]$. For every natural number x, $\mathcal{P}[x]$. □

(24) Let us consider an odd natural number a. Suppose $a > 1$. Let us consider a natural number s. Suppose s is double odd and a^s+1 is double odd and $s \mid a^s+1$. Then

(i) $a^s+1 > s$, and

(ii) a^s+1 is double odd, and

(iii) $a^{a^s+1}+1$ is double odd, and

(iv) $a^s+1 \mid a^{a^s+1}+1$.

(25) Let us consider a natural number a. If $a > 1$, then $\{n$, where n is a natural number : $n \mid a^n+1\}$ is infinite. The theorem is a consequence of (24) and (1).

(26) $\{n$, where n is a natural number : $n \mid 2^n+2\}$ is infinite. The theorem is a consequence of (16).

(27) $\{n$, where n is a natural number : $5 \mid 2^n-3\}$ is infinite.
PROOF: Set $A = \{n$, where n is a natural number : $5 \mid 2^n-3\}$. Define $\mathcal{F}$(natural number) $= 4 \cdot \$_1 + 3$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element d of $\mathbb{N}$, $f(d) = \mathcal{F}(d)$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

(28) $\{n$, where n is a natural number : $13 \mid 2^n-3\}$ is infinite.
PROOF: Set $A = \{n$, where n is a natural number : $13 \mid 2^n-3\}$. Define $\mathcal{F}$(natural number) $= 12 \cdot \$_1 + 4$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element d of $\mathbb{N}$, $f(d) = \mathcal{F}(d)$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

(29) $2^{n+12} \equiv 2^n \pmod{65}$.

(30) $2^n \equiv 2^{n \bmod 12} \pmod{65}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv 2^{\$_1} \equiv 2^{\$_1 \bmod 12} \pmod{65}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by [7, (11)], [4, (4)]. $\mathcal{P}[k]$. □

(31) $65 \nmid 2^n-3$. The theorem is a consequence of (30) and (2).

(32) 341 is composite.

(33) 561 is composite.

(34) 645 is composite.

(35) 1105 is composite.

(36) $341 \mid 2^{341}-2$.

(37) $3 \mid 2^{561}-2$.

(38) $11 \mid 2^{561}-2$.

(39) $17 \mid 2^{561} - 2$.

(40) $561 \mid 2^{561} - 2$. The theorem is a consequence of (37), (38), (39), and (12).

(41) $3 \mid 2^{645} - 2$.

(42) $5 \mid 2^{645} - 2$.

(43) $43 \mid 2^{645} - 2$.

(44) $645 \mid 2^{645} - 2$. The theorem is a consequence of (41), (42), (43), and (12).

(45) $5 \mid 2^{1105} - 2$.

(46) $13 \mid 2^{1105} - 2$.

(47) $17 \mid 2^{1105} - 2$.

(48) $1105 \mid 2^{1105} - 2$. The theorem is a consequence of (45), (46), (47), and (12).

(49) Let us consider a composite natural number n. If $n \leqslant 1105$ and $n \mid 2^n - 2$, then $n \in \{341, 561, 645, 1105\}$.

(50) $341 \nmid 3^{341} - 3$. The theorem is a consequence of (4) and (3).

(51) $3 \mid 3^{561} - 3$.

(52) $11 \mid 3^{561} - 3$.

(53) $17 \mid 3^{561} - 3$.

(54) $561 \mid 3^{561} - 3$. The theorem is a consequence of (51), (52), (53), and (12).

Now we state the propositions:

(55) $43 \nmid 3^{645} - 3$.

(56) $645 \nmid 3^{645} - 3$. The theorem is a consequence of (55).

Now we state the propositions:

(57) $5 \mid 3^{1105} - 3$.

(58) $13 \mid 3^{1105} - 3$.

(59) $17 \mid 3^{1105} - 3$.

(60) $1105 \mid 3^{1105} - 3$. The theorem is a consequence of (57), (58), (59), and (12).

(61) If $n \leqslant 1105$ and n is composite and $n \mid 2^n - 2$ and $n \mid 3^n - 3$, then $n \in \{561, 1105\}$. The theorem is a consequence of (49), (50), and (56).

(62) If $n \mid 2^n - 2$ and $n \nmid 3^n - 3$, then n is composite.

(63) If $n \leqslant 341$ and $n \mid 2^n - 2$ and $n \nmid 3^n - 3$, then $n = 341$. The theorem is a consequence of (62) and (49).

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

(65) $7 \mid 10^{6 \cdot k + 4} + 3$. The theorem is a consequence of (64).

(66) $10^{6 \cdot k + 4} + 3$ is composite. The theorem is a consequence of (65).

(67) $\{10^n + 3$, where n is a natural number : $10^n + 3$ is composite$\}$ is infinite.
PROOF: Set $X = \{10^n+3$, where n is a natural number : 10^n+3 is composite$\}$. Set $z = 10^{6\cdot 0+4} + 3$. z is composite. X is natural-membered. For every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$ by [5, (66)]. □

References

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

[2] 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] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

[5] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

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

[7] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

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

Accepted September 30, 2022