FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 229–234, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0018

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part V[1]

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Adam Naumowicz
Institute of Computer Science
University of Białystok
Poland

Summary. This paper reports on the formalization of ten selected problems from W. Sierpinski's book "250 Problems in Elementary Number Theory" [5] using the Mizar system [4], [1], [2]. Problems 12, 13, 31, 32, 33, 35 and 40 belong to the chapter devoted to the divisibility of numbers, problem 47 concerns relatively prime numbers, whereas problems 76 and 79 are taken from the chapter on prime and composite numbers.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: `NUMBER05`, version: `8.1.12 5.71.1431`

1. Problem 12

Now we state the proposition:

(1) Let us consider natural numbers n, k. If $n \uparrow\uparrow k = 0$, then $n = 0$.

Let x be an odd natural number and i be a natural number. Let us note that $x \uparrow\uparrow i$ is odd.

Let x be a non zero, even natural number and i be a non zero natural number. One can verify that $x \uparrow\uparrow i$ is even. Now we state the proposition:

(2) Let us consider a non zero natural number n. Then there exists a non zero natural number x such that for every natural number i, $n \mid x \uparrow\uparrow (i+1) + 1$.

[1]The Mizar processing has been performed using the infrastructure of the University of Bialystok High Performance Computing Center.

2. Problem 13

Now we state the proposition:

(3) Let us consider natural numbers n, k. Suppose $n = 4 \cdot k + 3$. Then there exist natural numbers p, q such that

(i) $p = 4 \cdot q + 3$, and

(ii) p is prime, and

(iii) $p \mid n$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ if there exists a natural number k such that $\$_1 = 4 \cdot k + 3$, then there exist natural numbers p, q such that $p = 4 \cdot q + 3$ and p is prime and $p \mid \$_1$. For every natural number m such that for every natural number l such that $l < m$ holds $\mathcal{P}[l]$ holds $\mathcal{P}[m]$ by [3, (28)], [6, (29)]. For every natural number n, $\mathcal{P}[n]$. Consider p, q being natural numbers such that $p = 4 \cdot q + 3$ and p is prime and $p \mid n$. □

The functor 4k + 3_Primes yielding a subset of $\mathbb{N}$ is defined by

(Def. 1) for every natural number n, $n \in$ *it* iff there exists a natural number k such that $n = 4 \cdot k + 3$ and n is prime.

Now we state the proposition:

(4) Let us consider a natural number n. If $n \in$ 4k + 3_Primes, then $n \geqslant 3$.

Let us observe that 4k + 3_Primes is infinite. Now we state the proposition:

(5) Let us consider a natural number n. Suppose $n \in$ 4k + 3_Primes. Let us consider an even natural number x, and a natural number i. Then $n \nmid x \uparrow\uparrow (i + 2) + 1$. The theorem is a consequence of (4).

3. Problem 31

Now we state the propositions:

(6) Let us consider an integer a. If $3 \nmid a$, then $a^3 \bmod 9 = 1$ or $a^3 \bmod 9 = 8$.

(7) Let us consider integers a, b, c. If $9 \mid a^3 + b^3 + c^3$, then $3 \mid a$ or $3 \mid b$ or $3 \mid c$. The theorem is a consequence of (6).

4. Problem 32

Now we state the propositions:

(8) Let us consider integers a, b, c, n. Then $a + b + c \bmod n = (a \bmod n) + (b \bmod n) + (c \bmod n) \bmod n$.

(9) Let us consider integers a, b, c, d, n. Then $a+b+c+d \bmod n = (a \bmod n)+(b \bmod n)+(c \bmod n)+(d \bmod n) \bmod n$. The theorem is a consequence of (8).

(10) Let us consider integers a, b, c, d, e, n. Then $a+b+c+d+e \bmod n = (a \bmod n)+(b \bmod n)+(c \bmod n)+(d \bmod n)+(e \bmod n) \bmod n$. The theorem is a consequence of (9).

(11) Let us consider integers a_1, a_2, a_3, a_4, a_5. Suppose $9 \mid {a_1}^3+{a_2}^3+{a_3}^3+{a_4}^3+{a_5}^3$. Then $3 \mid a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5$. The theorem is a consequence of (6) and (10).

5. Problem 33

From now on a, b, c, k, m, n denote natural numbers and p denotes a prime number. Now we state the propositions:

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

(13) Let us consider natural numbers x, y, z. If x and y are relatively prime and $x^2+y^2=z^4$, then $7 \mid x \cdot y$.

(14) (i) 15 and 20 are not relatively prime, and

(ii) $15^2+20^2=5^4$, and

(iii) $7 \nmid 15 \cdot 20$.

6. Problem 35

Let x, y be natural numbers. We say that x and y satisfy Sierpiński Problem 35 if and only if

(Def. 2) $x \cdot (x+1) \mid y \cdot (y+1)$ and $x \nmid y$ and $x+1 \nmid y$ and $x \nmid y+1$ and $x+1 \nmid y+1$.

Now we state the propositions:

(15) Let us consider natural numbers x, y. Suppose $x = 36 \cdot k + 14$ and $y = (12 \cdot k + 5) \cdot (18 \cdot k + 7)$. Then x and y satisfy Sierpiński Problem 35.

(16) $\{\langle x, y \rangle$, where x, y are natural numbers : x and y satisfy Sierpiński Problem 35$\}$ is infinite.

Proof: Set $A = \{\langle x, y \rangle$, where x, y are natural numbers : x and y satisfy Sierpiński Problem 35$\}$. Define $\mathcal{F}$(natural number) $= \langle 36 \cdot \$_1 + 14, (12 \cdot \$_1+5)\cdot(18\cdot\$_1+7)\rangle$. 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. □

(17) 14 and 35 satisfy Sierpiński Problem 35.

(18) There exist no natural numbers x, y such that $x < 14$ and $y < 35$ and x and y satisfy Sierpiński Problem 35.

7. Problem 40

Now we state the propositions:

(19) If $a \mid b$, then $n^a - 1 \mid n^b - 1$.

(20) $2^{2^n} + 1 \mid 2^{2^{2^n}+1} - 2$. The theorem is a consequence of (19).

8. Problem 47

Now we state the propositions:

(21) If $n \mid 4$, then $n = 1$ or $n = 2$ or $n = 4$.

(22) If $n > 6$, then there exist natural numbers a, b such that $a > 1$ and $b > 1$ and $n = a + b$ and a and b are relatively prime. The theorem is a consequence of (21).

9. Problem 76

Let n be a natural number. We say that n satisfies Sierpiński Problem 76a if and only if

(Def. 3) for every natural number x such that $n < x < n + 10$ holds x is not prime.

Let m be a natural number. We say that m satisfies Sierpiński Problem 76b if and only if

(Def. 4) for every natural number x such that $10 \cdot m < x < 10 \cdot (m + 1)$ holds x is not prime.

Now we state the propositions:

(23) 113 satisfies Sierpiński Problem 76a.

(24) 114 satisfies Sierpiński Problem 76a.

(25) 115 satisfies Sierpiński Problem 76a.

(26) 116 satisfies Sierpiński Problem 76a.

(27) 117 satisfies Sierpiński Problem 76a.

(28) 139 satisfies Sierpiński Problem 76a.

(29) 181 satisfies Sierpiński Problem 76a.

(30) If n satisfies Sierpiński Problem 76a and $n \leqslant 181$, then $n \in \{113, 114, 115, 116, 117, 139, 181\}$.

(31) 20 satisfies Sierpiński Problem 76b.

(32) 32 satisfies Sierpiński Problem 76b.

(33) 51 satisfies Sierpiński Problem 76b.

(34) 53 satisfies Sierpiński Problem 76b.

(35) 62 satisfies Sierpiński Problem 76b.

(36) If m satisfies Sierpiński Problem 76b and $m \leqslant 62$, then $m \in \{20, 32, 51, 53, 62\}$.

10. Problem 79

Now we state the propositions:

(37) If $c \neq 0$ and $c < b$, then $\frac{a \cdot b + c}{b}$ is not integer.

(38) There exist no positive natural numbers m, n such that $m^{\mathbf{2}} - n^{\mathbf{2}} = 1$.

(39) There exist no positive natural numbers m, n such that $m^{\mathbf{2}} - n^{\mathbf{2}} = 4$. The theorem is a consequence of (38).

(40) $(2 \cdot n + 1)^{\mathbf{2}} \bmod 8 = 1$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv (2 \cdot \$_1 + 1)^{\mathbf{2}} \bmod 8 = 1$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$. $\mathcal{P}[k]$. $\square$

(41) If n is odd, then $n^{\mathbf{2}} \bmod 8 = 1$. The theorem is a consequence of (40).

(42) Let us consider prime numbers q, s, t. Suppose $q^{\mathbf{2}} = s^{\mathbf{2}} + t^{\mathbf{2}}$. Then

- (i) s is even and t is odd, or
- (ii) s is odd and t is even.

The theorem is a consequence of (39).

(43) There exist no prime numbers q, s, t such that $q^{\mathbf{2}} = s^{\mathbf{2}} + t^{\mathbf{2}}$. The theorem is a consequence of (42) and (39).

(44) Let us consider prime numbers p, q, r, s, t. Suppose $p^{\mathbf{2}} + q^{\mathbf{2}} = r^{\mathbf{2}} + s^{\mathbf{2}} + t^{\mathbf{2}}$. Then

- (i) p is even, or
- (ii) q is even, or
- (iii) r is even, or
- (iv) s is even, or
- (v) t is even.

(45) There exist no prime numbers p, q, r, s, t such that $p^{\mathbf{2}} + q^{\mathbf{2}} = r^{\mathbf{2}} + s^{\mathbf{2}} + t^{\mathbf{2}}$. The theorem is a consequence of (43) and (41).

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] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[4] 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.

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

[6] Rafał Ziobro. Prime factorization of sums and differences of two like powers. *Formalized Mathematics*, 24(**3**):187–198, 2016. doi:10.1515/forma-2016-0015.

Accepted September 30, 2022