FORMALIZED MATHEMATICS
Vol. 32, No. 1, pp. 1–8, 2024
DOI: 10.2478/forma-2024-0001
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part XIII

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

Rafał Ziobro
Department of Carbohydrate Technology
University of Agriculture
Kraków, Poland

Summary. This paper formalizes problems 41, 92, 121–123, 172, 182, 183, 191, 192 and 192a from "250 Problems in Elementary Number Theory" by Wacław Sierpiński [9].

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; prime number

MML identifier: `NUMBER13`, version: `8.1.14 5.79.1465`

Introduction

In this paper, Problems 41 from Section I, 92, 121, 122, 123 from Section IV, 172, 182, 183, 191, 192, and 192a from Section V of [9] are formalized, using the Mizar formalism [3, 2]. The paper is a part of the project *Formalization of Elementary Number Theory in Mizar* [7].

In the preliminary section, we proved some trivial but useful facts about numbers.

In problem 92 the inequality $p_{k+1} + p_{k+2} \leqslant p_1 * p_2 * \cdots * p_k$ should be justified for any integer $k \geqslant 3$, where p_k denotes the k-th prime. Because we count primes starting from the index 0, we formulated the fact as:

```
3 <= k implies
   primenumber(k) + primenumber(k+1) <= Product primesFinS(k);
```

where `primesFinS(k)` denotes the finite sequence of primes of the length `k`, and elements of finite sequences are indexed from 1.

Problem 121 about finding the least positive integer n for which $k \cdot 2^{2^n} + 1$ is composite is represented as separated theorems for every positive $k \leqslant 10$.

Problem 122 requires finding all positive integers $k \leqslant 10$ such that every number $k \cdot 2^{2^n} + 1$ $(n = 1, 2, \dots)$ is composite. The proof lies in the fact that numbers $(3 \cdot t + 2) \cdot 2^{2^n} + 1$ are all divisible by 3 and greater than 3, for every natural t, and every positive natural n. In the book, there are minor misprints in the proof, where $2 \cdot 2^{2^2} + 1$ should be $2 \cdot 2^{2^n} + 1$ and $5 \cdot 2^{2^2} + 1$ should be $5 \cdot 2^{2^n} + 1$.

Problems 191 and 192 are generalized from positive integers to non-zero integers.

Problem 192a is formulated incorrectly in the book. It asks to prove that the system of two equations $x^2 + 7y^2 = z^2$ and $7x^2 + y^2 = t^2$ has no solutions in positive integers x, y, z, and t. However, it has solutions, for instance, $x = 3$, $y = 1$, $z = 4$, and $t = 8$. The example is provided in the book.

Proofs of other problems are straightforward formalizations of solutions given in the book.

1. Preliminaries

From now on a, b, c, k, m, n denote natural numbers, i, j denote integers, and p denotes a prime number.

Now we state the propositions:

(1) If $n < 3$, then $n = 0$ or $n = 1$ or $n = 2$.

(2) If $n < 4$, then $n = 0$ or $n = 1$ or $n = 2$ or $n = 3$.

(3) If $n < 5$, then $n = 0$ or $n = 1$ or $n = 2$ or $n = 3$ or $n = 4$.

Let us note that $\frac{1}{2}$ is non integer and there exists a rational number which is non natural and there exists a rational number which is non integer.

Now we state the proposition:

(4) If $j \neq 0$ and $\frac{i}{j}$ is integer, then $j \mid i$.

Let q be a non integer rational number. One can verify that $q^{\mathbf{2}}$ is non integer.

Now we state the proposition:

(5) If $\frac{a}{b} \cdot c$ is natural and $b \neq 0$ and a and b are relatively prime, then there exists a natural number d such that $c = b \cdot d$.

2. Problem 41

Let us consider an integer k. Now we state the propositions:

(6) $2 \cdot k + 1$ and $9 \cdot k + 4$ are relatively prime.

(7) $\gcd(2 \cdot k - 1, 9 \cdot k + 4) = \gcd(k + 8, 17)$.

3. Problem 92

Now we state the proposition:

(8) If $m > 1$ and $n > 1$ and m and n are relatively prime, then there exist prime numbers p, q such that $p \mid m$ and $p \nmid n$ and $q \mid n$ and $q \nmid m$ and $p \neq q$.

Let us consider k. The functor $\boxed{\text{primesFinS}(k)}$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by

(Def. 1) $\operatorname{len} it = k$ and for every natural number i such that $i < k$ holds $it(i+1) = \operatorname{pr}(i)$.

Let us observe that primesFinS(0) is empty.

Now we state the propositions:

(9) $\text{primesFinS}(1) = \langle 2 \rangle$.

(10) $\text{primesFinS}(2) = \langle 2, 3 \rangle$.

(11) $\text{primesFinS}(3) = \langle 2, 3, 5 \rangle$.

(12) $p < \operatorname{pr}(k)$ if and only if $\text{primeindex}(p) < k$.

(13) If $\text{primeindex}(p) < k$, then $1 + \text{primeindex}(p) \in \operatorname{dom}(\text{primesFinS}(k))$.

(14) If $\text{primeindex}(p) < k$, then $(\text{primesFinS}(k))(1 + \text{primeindex}(p)) = p$.

(15) If $p < \operatorname{pr}(k)$, then $p \in \operatorname{rng} \text{primesFinS}(k)$. The theorem is a consequence of (13), (12), and (14).

(16) If p and $\prod \text{primesFinS}(k)$ are relatively prime, then $\operatorname{pr}(k) \leqslant p$. The theorem is a consequence of (15).

Let us consider k. Let us note that primesFinS(k) is positive yielding and primesFinS(k) is increasing.

Let R be an extended real-valued binary relation. We say that $\boxed{R \text{ is with values greater}}$ if and only if

(Def. 2) for every extended real r such that $r \in \operatorname{rng} R$ holds $r \geqslant 1$.

Observe that $\langle 1 \rangle$ is with values greater or equal one and there exists a natural-valued finite sequence which is with values greater or equal one.

Let f be an extended real-valued function. Let us observe that f is with values greater or equal one if and only if the condition (Def. 3) is satisfied.

(Def. 3) for every object x such that $x \in \operatorname{dom} f$ holds $f(x) \geqslant 1$.

Let f be an extended real-valued finite sequence. One can verify that f is with values greater or equal one if and only if the condition (Def. 4) is satisfied.

(Def. 4) for every natural number n such that $1 \leqslant n \leqslant \operatorname{len} f$ holds $f(n) \geqslant 1$.

One can verify that every extended real-valued binary relation which is empty is also with values greater or equal one and every extended real-valued binary relation which is with values greater or equal one is also positive yielding.

Now we state the propositions:

(17) If $m \leqslant n$, then $\mathrm{primesFinS}(n) \restriction m = \mathrm{primesFinS}(m)$.

(18) Let us consider extended real-valued binary relations P, R. Suppose $\operatorname{rng} P \subseteq \operatorname{rng} R$ and R is with values greater or equal one. Then P is with values greater or equal one.

(19) Let us consider extended real-valued finite sequences f, g. Suppose $f \frown g$ is with values greater or equal one. Then

(i) f is with values greater or equal one, and

(ii) g is with values greater or equal one.

(20) Let us consider an extended real r. If $\langle r \rangle$ is with values greater or equal one, then $r \geqslant 1$.

Let us consider a with values greater or equal one, real-valued finite sequence f. Now we state the propositions:

(21) $\prod f \geqslant 1$.

PROOF: Define $\mathcal{P}$[finite sequence of elements of $\mathbb{R}$] $\equiv$ for every with values greater or equal one, real-valued finite sequence g such that $g = \$_1$ holds $\prod \$_1 \geqslant 1$. For every finite sequence p of elements of $\mathbb{R}$ and for every element x of $\mathbb{R}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$ by (19), (20), [5, (96)]. For every finite sequence p of elements of $\mathbb{R}$, $\mathcal{P}[p]$ from [4, Sch. 2]. $\square$

(22) $\prod (f \restriction n) \leqslant \prod f$. The theorem is a consequence of (19) and (20).

Let us consider k. One can verify that $\mathrm{primesFinS}(k)$ is with values greater or equal one.

Now we state the proposition:

(23) If $3 \leqslant k$, then $\mathrm{pr}(k) + \mathrm{pr}(k+1) \leqslant \prod \mathrm{primesFinS}(k)$. The theorem is a consequence of (8) and (16).

4. PROBLEM 121

Let k, n be natural numbers. We say that n satisfies Sierpiński Problem 121 for k if and only if

(Def. 5) $k \cdot 2^{2^n} + 1$ is composite and for every positive natural number m such that $m < n$ holds $k \cdot 2^{2^m} + 1$ is not composite.

Now we state the propositions:

(24) 5 satisfies Sierpiński Problem 121 for 1. The theorem is a consequence of (3).

(25) 1 satisfies Sierpiński Problem 121 for 2.

(26) 2 satisfies Sierpiński Problem 121 for 3.

(27) 2 satisfies Sierpiński Problem 121 for 4.

(28) 1 satisfies Sierpiński Problem 121 for 5.

(29) 1 satisfies Sierpiński Problem 121 for 6.

(30) 3 satisfies Sierpiński Problem 121 for 7. The theorem is a consequence of (1).

(31) 1 satisfies Sierpiński Problem 121 for 8.

(32) 2 satisfies Sierpiński Problem 121 for 9.

(33) 2 satisfies Sierpiński Problem 121 for 10.

5. PROBLEM 122

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

(34) $3 \mid (3 \cdot a + 2) \cdot 2^{2^n} + 1$.

(35) $2 \cdot 2^{2^n} + 1$ is composite.

(36) $5 \cdot 2^{2^n} + 1$ is composite. The theorem is a consequence of (34).

(37) $8 \cdot 2^{2^n} + 1$ is composite. The theorem is a consequence of (34).

Now we state the proposition:

(38) Let us consider a positive natural number k. Then $k \leqslant 10$ and for every positive natural number n, $k \cdot 2^{2^n} + 1$ is composite if and only if $k \in \{2, 5, 8\}$. The theorem is a consequence of (24), (26), (27), (30), (32), (33), (35), (36), and (37).

6. Problem 123

Now we state the propositions:

(39) $2^{2^{n+1}} + 2^{2^n} + 1 \geqslant 7$.

(40) If $n > 0$, then $2^{2^{n+1}} + 2^{2^n} + 1 \geqslant 21$.

(41) If $n > 1$, then $2^{2^{n+1}} + 2^{2^n} + 1 \geqslant 273$.

(42) If m is even or $m = 2 \cdot n$, then $2^m \bmod 3 = 1$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv 2^{2 \cdot \$_1} \bmod 3 = 1$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (8)]. For every k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(43) If m is odd or $m = 2 \cdot n + 1$, then $2^m \bmod 3 = 2$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv 2^{2 \cdot \$_1 + 1} \bmod 3 = 2$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (8)]. For every k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(44) Let us consider a non zero natural number n. Then $3 \mid 2^{2^{n+1}} + 2^{2^n} + 1$. The theorem is a consequence of (42).

(45) $7 \mid 2^{2^{n+1}} + 2^{2^n} + 1$. The theorem is a consequence of (42) and (43).

Let n be a non zero natural number. Note that $\frac{1}{3} \cdot (2^{2^{n+1}} + 2^{2^n} + 1)$ is natural. Now we state the proposition:

(46) Let us consider a non zero natural number n. If $n > 1$, then $\frac{1}{3} \cdot (2^{2^{n+1}} + 2^{2^n} + 1)$ is composite. The theorem is a consequence of (39), (45), (44), and (41).

7. Problem 172

Now we state the proposition:

(47) Let us consider positive natural numbers n, x, y, z. Then $n^x + n^y = n^z$ if and only if $n = 2$ and $y = x$ and $z = x + 1$.

8. Problem 182

Now we state the proposition:

(48) Let us consider real numbers a, b, c. If $c > 1$ and $c^a = c^b$, then $a = b$.

Let us consider positive natural numbers n, x, y, z, t. Now we state the propositions:

(49) If $x \leqslant y \leqslant z$, then $n^x + n^y + n^z = n^t$ iff $n = 2$ and $y = x$ and $z = x + 1$ and $t = x + 2$ or $n = 3$ and $y = x$ and $z = x$ and $t = x + 1$.
Proof: If $n^x + n^y + n^z = n^t$, then $n = 2$ and $y = x$ and $z = x + 1$ and $t = x + 2$ or $n = 3$ and $y = x$ and $z = x$ and $t = x + 1$ by [10, (5)], [1, (23)], [8, (93)], [6, (8)]. □

(50) $n^x + n^y + n^z = n^t$ if and only if $n = 2$ and $y = x$ and $z = x + 1$ and $t = x + 2$ or $n = 2$ and $y = x + 1$ and $z = x$ and $t = x + 2$ or $n = 2$ and $z = y$ and $x = y + 1$ and $t = y + 2$ or $n = 3$ and $y = x$ and $z = x$ and $t = x + 1$. The theorem is a consequence of (49).

9. PROBLEM 183

Now we state the proposition:

(51) Let us consider positive natural numbers x, y, z, t. Then $4^x+4^y+4^z \neq 4^t$.

10. PROBLEM 191

Now we state the proposition:

(52) Let us consider non zero integers x, y, z, t. Then

(i) $x^{\mathbf{2}} + 5 \cdot y^{\mathbf{2}} \neq z^{\mathbf{2}}$, or

(ii) $5 \cdot x^{\mathbf{2}} + y^{\mathbf{2}} \neq t^{\mathbf{2}}$.

11. PROBLEM 192

Now we state the propositions:

(53) Let us consider non zero integers x, y, z, t. Then

(i) $x^{\mathbf{2}} + 6 \cdot y^{\mathbf{2}} \neq z^{\mathbf{2}}$, or

(ii) $6 \cdot x^{\mathbf{2}} + y^{\mathbf{2}} \neq t^{\mathbf{2}}$.

(54) (i) $3^{\mathbf{2}} + 7 \cdot 1^{\mathbf{2}} = 4^{\mathbf{2}}$, and

(ii) $7 \cdot 3^{\mathbf{2}} + 1^{\mathbf{2}} = 8^{\mathbf{2}}$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[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] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[5] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[6] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[7] 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.

[8] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

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

[10] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

Accepted June 18, 2024