FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 63–68, 2021
DOI: 10.2478/forma-2021-0006

https://sciendo.com/journal/forma

Elementary Number Theory Problems. Part II

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Dariusz Surowik
University of Białystok
Poland

Summary. In this paper problems 14, 15, 29, 30, 34, 78, 83, 97, and 116 from [6] are formalized, using the Mizar formalism [1], [2], [3]. Some properties related to the divisibility of prime numbers were proved. It has been shown that the equation of the form $p^2 + 1 = q^2 + r^2$, where p, q, r are prime numbers, has at least four solutions and it has been proved that at least five primes can be represented as the sum of two fourth powers of integers. We also proved that for at least one positive integer, the sum of the fourth powers of this number and its successor is a composite number. And finally, it has been shown that there are infinitely many odd numbers k greater than zero such that all numbers of the form $2^{2^n} + k$ ($n = 1, 2, \dots$) are composite.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: NUMBER02, version: 8.1.11 5.65.1394

1. Preliminaries

Let D be a non empty set, f be a D-valued finite sequence, and i be a natural number. One can verify that $f{\restriction}i$ is D-valued.

From now on a, b, i, k, m, n denote natural numbers, s, z denote non zero natural numbers, and c denotes a complex number.

Now we state the propositions:

(1) $c^5 = c \cdot c \cdot c \cdot c \cdot c$.

(2) $c^6 = c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (1).

(3) $c^7 = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (2).

(4) $c^8 = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (3).

(5) $c^9 = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (4).

(6) $c^{10} = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (5).

(7) If $a = n - 1$ and $k < n$, then $k = 0$ or ... or $k = a$.

(8) $-1 \operatorname{div} 3 = -1$.

(9) $-1 \bmod 3 = 2$. The theorem is a consequence of (8).

(10) 30 is not prime.

2. Divisibility of Natural Numbers

Now we state the propositions:

(11) If $n < 31$ and n is prime, then $n = 2$ or $n = 3$ or $n = 5$ or $n = 7$ or $n = 11$ or $n = 13$ or $n = 17$ or $n = 19$ or $n = 23$ or $n = 29$. The theorem is a consequence of (10).

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

(13) 113 is prime.

Proof: For every element n of $\mathbb{N}$ such that $1 < n$ and $n \cdot n \leqslant 113$ and n is prime holds $n \nmid 113$. □

(14) 337 is prime.

Proof: For every element n of $\mathbb{N}$ such that $1 < n$ and $n \cdot n \leqslant 337$ and n is prime holds $n \nmid 337$. □

(15) 881 is prime.

Proof: For every element n of $\mathbb{N}$ such that $1 < n$ and $n \cdot n \leqslant 881$ and n is prime holds $n \nmid 881$ by [4, (9)], (12). □

(16) If $k < a$, then $a \cdot b + k \bmod a = k$.

(17) $a \mid a^s + a^z$.

(18) $a \mid a^s - a^z$.

(19) $a \mid a^s \cdot (a^z)$.

Let p, q be prime natural numbers. One can verify that $p \cdot q$ is non prime.

Now we state the propositions:

(20) $11 \mid 2^{341} - 2$. The theorem is a consequence of (6).

(21) $31 \mid 2^{341} - 2$. The theorem is a consequence of (1).

(22) There exists k such that $n = z \cdot k + 0$ or ... or $n = z \cdot k + (z - 1)$.

(23) There exists k such that $n = 3 \cdot k$ or $n = 3 \cdot k + 1$ or $n = 3 \cdot k + 2$. The theorem is a consequence of (22).

(24) There exists k such that $n = 4 \cdot k$ or $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. The theorem is a consequence of (22).

(25) There exists k such that $n = 5 \cdot k$ or $n = 5 \cdot k + 1$ or $n = 5 \cdot k + 2$ or $n = 5 \cdot k + 3$ or $n = 5 \cdot k + 4$. The theorem is a consequence of (22).

(26) There exists 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 $n = 6 \cdot k + 5$. The theorem is a consequence of (22).

(27) There exists k such that $n = 7 \cdot k$ or $n = 7 \cdot k + 1$ or $n = 7 \cdot k + 2$ or $n = 7 \cdot k + 3$ or $n = 7 \cdot k + 4$ or $n = 7 \cdot k + 5$ or $n = 7 \cdot k + 6$. The theorem is a consequence of (22).

(28) There exists k such that $n = 8 \cdot k$ or $n = 8 \cdot k + 1$ or $n = 8 \cdot k + 2$ or $n = 8 \cdot k + 3$ or $n = 8 \cdot k + 4$ or $n = 8 \cdot k + 5$ or $n = 8 \cdot k + 6$ or $n = 8 \cdot k + 7$. The theorem is a consequence of (22).

(29) There exists k such that $n = 9 \cdot k$ or $n = 9 \cdot k + 1$ or $n = 9 \cdot k + 2$ or $n = 9 \cdot k + 3$ or $n = 9 \cdot k + 4$ or $n = 9 \cdot k + 5$ or $n = 9 \cdot k + 6$ or $n = 9 \cdot k + 7$ or $n = 9 \cdot k + 8$. The theorem is a consequence of (22).

(30) There exists k such that $n = 10 \cdot k$ or $n = 10 \cdot k + 1$ or $n = 10 \cdot k + 2$ or $n = 10 \cdot k + 3$ or $n = 10 \cdot k + 4$ or $n = 10 \cdot k + 5$ or $n = 10 \cdot k + 6$ or $n = 10 \cdot k + 7$ or $n = 10 \cdot k + 8$ or $n = 10 \cdot k + 9$. The theorem is a consequence of (22).

(31) $3 \nmid n$ if and only if there exists k such that $n = 3 \cdot k + 1$ or $n = 3 \cdot k + 2$. The theorem is a consequence of (23).

(32) $4 \nmid n$ if and only if there exists k such that $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. The theorem is a consequence of (24).

(33) $5 \nmid n$ if and only if there exists k such that $n = 5 \cdot k + 1$ or $n = 5 \cdot k + 2$ or $n = 5 \cdot k + 3$ or $n = 5 \cdot k + 4$. The theorem is a consequence of (25).

(34) $6 \nmid n$ if and only if there exists k such that $n = 6 \cdot k + 1$ or $n = 6 \cdot k + 2$ or $n = 6 \cdot k + 3$ or $n = 6 \cdot k + 4$ or $n = 6 \cdot k + 5$. The theorem is a consequence of (26).

(35) $7 \nmid n$ if and only if there exists k such that $n = 7 \cdot k + 1$ or $n = 7 \cdot k + 2$ or $n = 7 \cdot k + 3$ or $n = 7 \cdot k + 4$ or $n = 7 \cdot k + 5$ or $n = 7 \cdot k + 6$. The theorem is a consequence of (27).

(36) $8 \nmid n$ if and only if there exists k such that $n = 8 \cdot k + 1$ or $n = 8 \cdot k + 2$ or $n = 8 \cdot k + 3$ or $n = 8 \cdot k + 4$ or $n = 8 \cdot k + 5$ or $n = 8 \cdot k + 6$ or $n = 8 \cdot k + 7$. The theorem is a consequence of (28).

(37) $9 \nmid n$ if and only if there exists k such that $n = 9 \cdot k + 1$ or $n = 9 \cdot k + 2$ or

$n = 9 \cdot k + 3$ or $n = 9 \cdot k + 4$ or $n = 9 \cdot k + 5$ or $n = 9 \cdot k + 6$ or $n = 9 \cdot k + 7$ or $n = 9 \cdot k + 8$. The theorem is a consequence of (29).

(38) $10 \nmid n$ if and only if there exists k such that $n = 10 \cdot k + 1$ or $n = 10 \cdot k + 2$ or $n = 10 \cdot k + 3$ or $n = 10 \cdot k + 4$ or $n = 10 \cdot k + 5$ or $n = 10 \cdot k + 6$ or $n = 10 \cdot k + 7$ or $n = 10 \cdot k + 8$ or $n = 10 \cdot k + 9$. The theorem is a consequence of (30).

(39) $2^{2^z} \bmod 3 = 1$.

Proof: Define $\mathcal{P}$[non zero natural number] $\equiv 2^{2^{\$_1}} \bmod 3 = 1$. $\mathcal{P}[1]$ by [5, (1)]. For every s such that $\mathcal{P}[s]$ holds $\mathcal{P}[s+1]$. For every s, $\mathcal{P}[s]$. □

Let n be an integer. We say that n is composite if and only if

(Def. 1) $2 \leqslant n$ and n is not prime.

One can check that there exists an integer which is composite and there exists a natural number which is composite and every integer which is composite is also positive and every integer which is prime is also non composite and every integer which is composite is also non prime.

Let m, n be composite natural numbers. Observe that $m \cdot n$ is composite.

Now we state the proposition:

(40) If n is composite, then $4 \leqslant n$.

3. Main Problems

Now we state the propositions:

(41) Suppose $1 \leqslant i \leqslant \operatorname{len}\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle - m$. Then $a^m \mid \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle (i)$.

(42) $n^{\mathbf{2}} \mid (n+1)^n - 1$.

Proof: Set $P = \langle \binom{n}{0} n^0 1^n, \ldots, \binom{n}{n} n^n 1^0 \rangle$. Set $c = \operatorname{len} P$. Set $F = P_{\restriction c}$. For every natural number b such that $b \in \operatorname{dom} F$ holds $n^{\mathbf{2}} \mid F(b)$. □

(43) $(2^n - 1)^{\mathbf{2}} \mid 2^{(2^n - 1) \cdot n} - 1$. The theorem is a consequence of (42).

(44) (i) $6 \nmid 2^6 - 2$, and

(ii) $6 \mid 3^6 - 3$, and

(iii) there exists no natural number n such that $n < 6$ and $n \nmid 2^n - 2$ and $n \mid 3^n - 3$.

The theorem is a consequence of (2), (34), (7), and (32).

(45) Let us consider a non zero natural number a. Then there exists a non prime natural number n such that $n \mid a^n - a$. The theorem is a consequence of (18), (20), and (21).

(46) If $7 \nmid a$, then there exists k such that $a^{\mathbf{2}} = 7 \cdot k + 1$ or $a^{\mathbf{2}} = 7 \cdot k + 2$ or $a^{\mathbf{2}} = 7 \cdot k + 4$. The theorem is a consequence of (35).

(47) There exists k such that $a^{\mathbf{2}} = 7 \cdot k$ or $a^{\mathbf{2}} = 7 \cdot k + 1$ or $a^{\mathbf{2}} = 7 \cdot k + 2$ or $a^{\mathbf{2}} = 7 \cdot k + 4$. The theorem is a consequence of (46).

(48) If $7 \nmid a$, then $a^{\mathbf{2}} \bmod 7 = 1$ or $a^{\mathbf{2}} \bmod 7 = 2$ or $a^{\mathbf{2}} \bmod 7 = 4$. The theorem is a consequence of (46) and (16).

(49) (i) $a^{\mathbf{2}} \bmod 7 = 0$, or

(ii) $a^{\mathbf{2}} \bmod 7 = 1$, or

(iii) $a^{\mathbf{2}} \bmod 7 = 2$, or

(iv) $a^{\mathbf{2}} \bmod 7 = 4$.

The theorem is a consequence of (46) and (16).

(50) Suppose there exists k such that $a = 7 \cdot k + 1$ or $a = 7 \cdot k + 2$ or $a = 7 \cdot k + 4$ and there exists k such that $b = 7 \cdot k + 1$ or $b = 7 \cdot k + 2$ or $b = 7 \cdot k + 4$. Then there exists k such that $a + b = 7 \cdot k + 1$ or ... or $a + b = 7 \cdot k + 6$.

(51) Suppose ($a \bmod 7 = 1$ or $a \bmod 7 = 2$ or $a \bmod 7 = 4$) and ($b \bmod 7 = 1$ or $b \bmod 7 = 2$ or $b \bmod 7 = 4$). Then $a + b \bmod 7 = 1$ or ... or $a + b \bmod 7 = 6$. The theorem is a consequence of (16).

(52) If $7 \mid a^{\mathbf{2}} + b^{\mathbf{2}}$, then $7 \mid a$ and $7 \mid b$. The theorem is a consequence of (48) and (49).

(53) (i) $13^{\mathbf{2}} + 1 = 7^{\mathbf{2}} + 11^{\mathbf{2}}$, and

(ii) $17^{\mathbf{2}} + 1 = 11^{\mathbf{2}} + 13^{\mathbf{2}}$, and

(iii) $23^{\mathbf{2}} + 1 = 13^{\mathbf{2}} + 19^{\mathbf{2}}$, and

(iv) $31^{\mathbf{2}} + 1 = 11^{\mathbf{2}} + 29^{\mathbf{2}}$.

(54) (i) $2 = 1^4 + 1^4$, and

(ii) $17 = 1^4 + 2^4$, and

(iii) $97 = 2^4 + 3^4$, and

(iv) $257 = 1^4 + 4^4$, and

(v) $641 = 2^4 + 5^4$.

(55) $0^4 + (0 + 1)^4$ is not composite.

(56) $1^4 + (1 + 1)^4$ is not composite.

(57) $2^4 + (2 + 1)^4$ is not composite.

(58) $3^4 + (3 + 1)^4$ is not composite.

(59) $4^4 + (4 + 1)^4$ is not composite.

(60) (i) $5^4 + (5 + 1)^4$ is composite, and

(ii) there exists no natural number n such that $n < 5$ and $n^4 + (n + 1)^4$ is composite.

The theorem is a consequence of (13), (56), (57), (58), and (59).

(61) If $1 \leqslant a$, then $2^{2^n} + (6 \cdot a - 1) > 6$.

(62) $3 \mid 2^{2^z} + (6 \cdot a - 1)$. The theorem is a consequence of (9) and (39).

(63) If $1 \leqslant a$, then $2^{2^z} + (6 \cdot a - 1)$ is not prime. The theorem is a consequence of (62) and (61).

(64) If $1 \leqslant a$, then $2^{2^z} + (6 \cdot a - 1)$ is composite. The theorem is a consequence of (61) and (63).

(65) Let us consider a non zero natural number z. Then $\{k$, where k is a natural number : k is odd and $2^{2^z} + k$ is composite$\}$ is infinite.

Proof: Set $S = \{k$, where k is a natural number : k is odd and $2^{2^z} + k$ is composite$\}$. Define $\mathcal{F}$(natural number) $= 6 \cdot \$_1 - 1$. Consider f being a many sorted set indexed by $\mathbb{N}_+$ such that for every element n of $\mathbb{N}_+$, $f(n) = \mathcal{F}(n)$. Set $R = \operatorname{rng} f$. $R \subseteq S$. For every element m of $\mathbb{N}$, there exists an element n of $\mathbb{N}$ such that $n \geqslant m$ and $n \in R$. □

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

[4] Marco Riccardi. Pocklington's theorem and Bertrand's postulate. *Formalized Mathematics*, 14(**2**):47–52, 2006. doi:10.2478/v10037-006-0007-y.

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

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

Accepted March 30, 2021