Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 111–118, 2014
DOI: 10.2478/forma-2014-0013

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Proth Numbers

Christoph Schwarzweller
WSB Schools of Banking
Gdańsk, Poland

Summary. In this article we introduce Proth numbers and prove two theorems on such numbers being prime [3]. We also give revised versions of Pocklington's theorem and of the Legendre symbol. Finally, we prove Pepin's theorem and that the fifth Fermat number is not prime.

MSC: 11A41 03B35

Keywords: prime numbers; Pocklington's theorem; Proth's theorem; Pepin's theorem

MML identifier: NAT_6, version: 8.1.03 5.23.1207

The notation and terminology used in this paper have been introduced in the following articles: [11], [6], [14], [13], [9], [16], [10], [1], [8], [2], [5], [7], [12], [15], and [4].

1. Preliminaries

Let n be a positive natural number. Let us note that $n-1$ is natural.

Let n be a non trivial natural number. Observe that $n-1$ is positive.

Let x be an integer number and n be a natural number. Let us observe that x^n is integer.

Let us observe that 1^n reduces to 1.

Let n be an even natural number. Let us observe that $(-1)^n$ reduces to 1.

Let n be an odd natural number. One can verify that $(-1)^n$ reduces to -1.

Now we state the propositions:

(1) Let us consider a positive natural number a and natural numbers n, m. If $n \geqslant m$, then $a^n \geqslant a^m$.

(2) Let us consider a non trivial natural number a and natural numbers n, m. If $n > m$, then $a^n > a^m$. The theorem is a consequence of (1).

ISSN 1426–2630(Print), 1898-9934(Online)

(3) Let us consider a non zero natural number n. Then there exists a natural number k and there exists an odd natural number l such that $n = l \cdot 2^k$.

(4) Let us consider an even natural number n. Then $n \operatorname{div} 2 = \frac{n}{2}$.

(5) Let us consider an odd natural number n. Then $n \operatorname{div} 2 = \frac{n-1}{2}$.

Let n be an even integer number. Let us observe that $\frac{n}{2}$ is integer.

Let n be an even natural number. One can check that $\frac{n}{2}$ is natural.

2. Some Properties of Congruences and Prime Numbers

Let us observe that every natural number which is prime is also non trivial.

Now we state the propositions:

(6) Let us consider a prime natural number p and an integer number a. Then $\gcd(a, p) \neq 1$ if and only if $p \mid a$.

(7) Let us consider integer numbers i, j and a prime natural number p. If $p \mid i \cdot j$, then $p \mid i$ or $p \mid j$. The theorem is a consequence of (6).

(8) Let us consider prime natural numbers x, p and a non zero natural number k. Then $x \mid p^k$ if and only if $x = p$.

(9) Let us consider integer numbers x, y, n. Then $x \equiv y \pmod{n}$ if and only if there exists an integer k such that $x = k \cdot n + y$.

(10) Let us consider an integer number i and a non zero integer number j. Then $i \equiv i \bmod j \pmod{j}$.

(11) Let us consider integer numbers x, y and a positive integer number n. Then $x \equiv y \pmod{n}$ if and only if $x \bmod n = y \bmod n$. The theorem is a consequence of (9) and (10).

(12) Let us consider integer numbers i, j and a natural number n. If $n < j$ and $i \equiv n \pmod{j}$, then $i \bmod j = n$.

(13) Let us consider a non zero natural number n and an integer number x. Then $x \equiv 0 \pmod{n}$ or ... or $x \equiv n - 1 \pmod{n}$. The theorem is a consequence of (10).

(14) Let us consider a non zero natural number n, an integer number x, and natural numbers k, l. Suppose

(i) $k < n$, and

(ii) $l < n$, and

(iii) $x \equiv k \pmod{n}$, and

(iv) $x \equiv l \pmod{n}$.

Then $k = l$. The theorem is a consequence of (12).

(15) Let us consider an integer number x. Then

(i) $x^2 \equiv 0 \pmod{3}$, or

(ii) $x^2 \equiv 1 \pmod 3$.

The theorem is a consequence of (13).

(16) Let us consider a prime natural number p, elements x, y of $\mathbb{Z}/p\mathbb{Z}^*$, and integer numbers i, j. If $x = i$ and $y = j$, then $x \cdot y = i \cdot j \bmod p$.

(17) Let us consider a prime natural number p, an element x of $\mathbb{Z}/p\mathbb{Z}^*$, an integer number i, and a natural number n. If $x = i$, then $x^n = i^n \bmod p$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{\$_1} = i^{\$_1} \bmod p$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(18) Let us consider a prime natural number p and an integer number x. Then $x^2 \equiv 1 \pmod p$ if and only if $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$. The theorem is a consequence of (7).

(19) Let us consider a natural number n. Then $-1 \equiv 1 \pmod n$ if and only if $n = 2$ or $n = 1$.

(20) Let us consider an integer number i. Then $-1 \equiv 1 \pmod i$ if and only if $i = 2$ or $i = 1$ or $i = -2$ or $i = -1$. The theorem is a consequence of (19).

3. Some basic properties of relation ">"

Let n, x be natural numbers. We say that x is greater than n if and only if

(Def. 1) $x > n$.

Let n be a natural number. Observe that there exists a natural number which is greater than n and odd and there exists a natural number which is greater than n and even.

Let us observe that every natural number which is greater than n is also n or greater.

One can check that every natural number which is $(n+1)$ or greater is also n or greater and every natural number which is greater than $(n+1)$ is also greater than n and every natural number which is greater than n is also $(n+1)$ or greater.

Let m be a non trivial natural number. One can verify that every natural number which is m or greater is also non trivial.

Let a be a positive natural number, m be a natural number, and n be an m or greater natural number. Let us note that a^n is a^m or greater.

Let a be a non trivial natural number. Let n be a greater than m natural number. Let us observe that a^n is greater than a^m and every natural number which is 2 or greater is also non trivial and every natural number which is non trivial is also 2 or greater and every natural number which is non trivial and odd is also greater than 2.

Let n be a greater than 2 natural number. One can verify that $n-1$ is non trivial.

Let n be a 2 or greater natural number. Let us observe that $n-2$ is natural.

Let m be a non zero natural number and n be an m or greater natural number. One can check that $n-1$ is natural and every prime natural number which is greater than 2 is also odd.

Let n be a natural number. One can check that there exists a natural number which is greater than n and prime.

4. Pocklington's Theorem Revisited

Let n be a natural number.

A divisor of n is a natural number and is defined by

(Def. 2) $it \mid n$.

Let n be a non trivial natural number. One can check that there exists a divisor of n which is non trivial.

Note that every divisor of n is non zero.

Let n be a positive natural number. One can verify that every divisor of n is positive.

Let n be a non zero natural number. Observe that every divisor of n is n or smaller.

Let us note that there exists a divisor of n which is prime.

Let n be a natural number and q be a divisor of n. Let us note that $\frac{n}{q}$ is natural.

Let s be a divisor of n and q be a divisor of s. Let us note that $\frac{n}{q}$ is natural.

Now we state the proposition:

(21) Pocklington's theorem:
Let us consider a greater than 2 natural number n and a non trivial divisor s of $n-1$. Suppose

(i) $s > \sqrt{n}$, and

(ii) there exists a natural number a such that $a^{n-1} \equiv 1 \pmod{n}$ and for every prime divisor q of s, $\gcd(a^{\frac{n-1}{q}} - 1, n) = 1$.

Then n is prime.

5. Euler's Criterion

Let a be an integer number and p be a natural number.

Now we state the propositions:

(22) Let us consider a positive natural number p and an integer number a. Then a is quadratic residue modulo p if and only if there exists an integer number x such that $x^2 \equiv a \pmod{p}$. Proof: If a is quadratic residue

modulo p, then there exists an integer number x such that $x^2 \equiv a \pmod{p}$ by [13, (59)], [8, (81)]. □

(23) 2 is quadratic non residue modulo 3. The theorem is a consequence of (15), (14), and (22).

Let p be a natural number and a be an integer number. The Legendre symbol(a,p) yielding an integer number is defined by the term

$$\text{(Def. 3)} \quad \begin{cases} 1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic residue modulo } p \text{ and } p \neq 1, \\ 0, & \textbf{if } p \mid a, \\ -1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic non residue modulo } p \text{ and} \\ & p \neq 1. \end{cases}$$

Let p be a prime natural number. Note that the Legendre symbol(a,p) is defined by the term

$$\text{(Def. 4)} \quad \begin{cases} 1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic residue modulo } p, \\ 0, & \textbf{if } p \mid a, \\ -1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic non residue modulo } p. \end{cases}$$

Let p be a natural number. We introduce $(\frac{a}{p})$ as a synonym of the Legendre symbol(a,p).

Let us consider a prime natural number p and an integer number a. Now we state the propositions:

(24) (i) $(\frac{a}{p}) = 1$, or

(ii) $(\frac{a}{p}) = 0$, or

(iii) $(\frac{a}{p}) = -1$.

Proof: $\gcd(a,p) = 1$ by [9, (21)]. □

(25) (i) $(\frac{a}{p}) = 1$ iff $\gcd(a,p) = 1$ and a is quadratic residue modulo p, and

(ii) $(\frac{a}{p}) = 0$ iff $p \mid a$, and

(iii) $(\frac{a}{p}) = -1$ iff $\gcd(a,p) = 1$ and a is quadratic non residue modulo p.

The theorem is a consequence of (6).

Now we state the propositions:

(26) Let us consider a natural number p. Then $(\frac{p}{p}) = 0$.

(27) Let us consider an integer number a. Then $(\frac{a}{2}) = a \bmod 2$. The theorem is a consequence of (22).

Let us consider a greater than 2 prime natural number p and integer numbers a, b. Now we state the propositions:

(28) If $\gcd(a,p) = 1$ and $\gcd(b,p) = 1$ and $a \equiv b \pmod{p}$, then $(\frac{a}{p}) = (\frac{b}{p})$.

(29) If $\gcd(a,p) = 1$ and $\gcd(b,p) = 1$, then $(\frac{a \cdot b}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$.

Now we state the proposition:

(30) Let us consider greater than 2 prime natural numbers p, q. Suppose $p \neq q$. Then $(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. The theorem is a consequence of (4).

Now we state the proposition:

(31) EULER'S CRITERION:
Let us consider a greater than 2 prime natural number p and an integer number a. Suppose $\gcd(a,p) = 1$. Then $a^{\frac{p-1}{2}} \equiv$ the Legendre symbol(a,p) $(\bmod\, p)$. The theorem is a consequence of (4).

6. PROTH NUMBERS

Let p be a natural number. We say that p is Proth if and only if

(Def. 5) There exists an odd natural number k and there exists a positive natural number n such that $2^n > k$ and $p = k \cdot 2^n + 1$.

One can check that there exists a natural number which is Proth and prime and there exists a natural number which is Proth and non prime and every natural number which is Proth is also non trivial and odd.

Now we state the propositions:

(32) 3 is Proth.

(33) 5 is Proth.

(34) 9 is Proth.

(35) 13 is Proth.

(36) 17 is Proth.

(37) 641 is Proth.

(38) 11777 is Proth.

(39) 13313 is Proth.

Now we state the proposition:

(40) PROTH'S THEOREM - VERSION 1:
Let us consider a Proth natural number n. Then n is prime if and only if there exists a natural number a such that $a^{\frac{n-1}{2}} \equiv -1 \ (\bmod\, n)$. The theorem is a consequence of (1), (8), (20), (21), (17), (10), (12), and (18).

Now we state the propositions:

(41) PROTH'S THEOREM - VERSION 2:
Let us consider a 2 or greater natural number l and a positive natural number k. Suppose

(i) $3 \nmid k$, and

(ii) $k \leqslant 2^l - 1$.

Then $k \cdot 2^l + 1$ is prime if and only if $3^{k \cdot 2^{l-1}} \equiv -1 \ (\bmod\, k \cdot 2^l + 1)$. The theorem is a consequence of (1), (8), (20), (21), (15), (6), (13), (30), (28), (23), and (31).

(42) 641 is prime. The theorem is a consequence of (40) and (37).

7. Fermat Numbers

Let l be a natural number. Note that Fermat l is Proth.

Now we state the propositions:

(43) Pepin's theorem:

Let us consider a non zero natural number l. Then Fermat l is prime if and only if $3^{\frac{\mathrm{Fermat}\, l-1}{2}} \equiv -1 \pmod{\mathrm{Fermat}\, l}$. The theorem is a consequence of (1), (4), and (41).

(44) Fermat 5 is not prime. The theorem is a consequence of (2).

8. Cullen Numbers

Let n be a natural number. The Cullen number of n yielding a natural number is defined by the term

(Def. 6) $n \cdot 2^n + 1$.

Let n be a non zero natural number. Let us observe that the Cullen number of n is Proth.

References

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

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] J. Buchmann and V. Müller. Primality testing. 1992.

[4] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[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] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Operations of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 20(**1**):87–95, 2012. doi:10.2478/v10037-012-0012-2.

[7] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

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

[9] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[10] Hiroyuki Okazaki and Yasunari Shidama. Uniqueness of factoring an integer and multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$. *Formalized Mathematics*, 16(**2**):103–107, 2008. doi:10.2478/v10037-008-0015-1.

[11] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[12] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

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

[14] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[16] Li Yan, Xiquan Liang, and Junjie Zhao. Gauss lemma and law of quadratic reciprocity. *Formalized Mathematics*, 16(**1**):23–28, 2008. doi:10.2478/v10037-008-0004-4.

Received June 9, 2014