FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Public-Key Cryptography and Pepin's Test for the Primality of Fermat Numbers

Yoshinori Fujisawa
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Hidetaka Shimizu
Information Technology Research Institute
of Nagano Prefecture

Summary. In this article, we have proved the correctness of the Public-Key Cryptography and the Pepin's Test for the Primality of Fermat Numbers ($F(n) = 2^{2^n} + 1$). It is a very important result in the IDEA Cryptography that F(4) is a prime number. At first, we prepared some useful theorems. Then, we proved the correctness of the Public-Key Cryptography. Next, we defined the Order's function and proved some properties. This function is very important in the proof of the Pepin's Test. Next, we proved some theorems about the Fermat Number. And finally, we proved the Pepin's Test using some properties of the Order's Function. And using the obtained result we have proved that F(1), F(2), F(3) and F(4) are prime number.

MML Identifier: `PEPIN`.

The terminology and notation used in this paper are introduced in the following papers: [8], [6], [2], [3], [9], [5], [1], [4], [7], and [10].

1. Some Useful Theorems

We adopt the following convention: d, i, j, k, m, n, p, q, k_1, k_2 are natural numbers and a, b, c, i_1, i_2, i_3, i_4, i_5 are integers.

One can prove the following four propositions:

ISSN 1426–2630

(1) For every i holds i and $i+1$ are relative prime.

(2) For every p such that p is prime holds m and p are relative prime or $\gcd(m,p) = p$.

(3) If $k \mid n \cdot m$ and n and k are relative prime, then $k \mid m$.

(4) If $n \mid m$ and $k \mid m$ and n and k are relative prime, then $n \cdot k \mid m$.

Let n be a natural number. Then $n^{\mathbf{2}}$ is a natural number.

We now state a number of propositions:

(5) If $c > 1$, then $1 \bmod c = 1$.

(6) For every i such that $i \neq 0$ holds $i \mid n$ iff $n \bmod i = 0$.

(7) If $m \neq 0$ and $m \mid n \bmod m$, then $m \mid n$.

(8) If $0 < n$ and $m \bmod n = k$, then $n \mid m - k$.

(9) If $i \cdot p \neq 0$ and p is prime and $k \bmod i \cdot p < p$, then $k \bmod i \cdot p = k \bmod p$.

(10) If $p \neq 0$, then $(a \cdot p + 1) \bmod p = 1 \bmod p$.

(11) If $1 < m$ and $n \cdot k \bmod m = k \bmod m$ and k and m are relative prime, then $n \bmod m = 1$.

(12) If $m \neq 0$, then $(p^k_{\mathbb{N}}) \bmod m = ((p \bmod m)^k_{\mathbb{N}}) \bmod m$.

(13) If $i \neq 0$, then $i^{\mathbf{2}} \bmod (i+1) = 1$.

(14) If $j \neq 0$ and $k^{\mathbf{2}} < j$ and $i \bmod j = k$, then $i^{\mathbf{2}} \bmod j = k^{\mathbf{2}}$.

(15) If p is prime and $i \bmod p = -1$, then $i^{\mathbf{2}} \bmod p = 1$.

(16) If n is even, then $n+1$ is odd.

(17) If $p > 2$ and p is prime, then p is odd.

(18) If $n > 0$, then the n-th power of 2 is even.

(19) If i is odd and j is odd, then $i \cdot j$ is odd.

(20) For every k such that i is odd holds $i^k_{\mathbb{N}}$ is odd.

(21) If $k > 0$ and i is even, then $i^k_{\mathbb{N}}$ is even.

(22) $2 \mid n$ iff n is even.

(23) If $m \cdot n$ is even, then m is even or n is even.

(24) $n^2_{\mathbb{N}} = n^{\mathbf{2}}$.

(25) $2^k_{\mathbb{N}} =$ the k-th power of 2.

(26) If $m > 1$ and $n > 0$, then $m^n_{\mathbb{N}} > 1$.

(27) If $n \neq 0$ and $p \neq 0$, then $n^p_{\mathbb{N}} = n \cdot n^{p -' 1}_{\mathbb{N}}$.

(28) For all n, m such that $m \bmod 2 = 0$ holds $(n^{m \div 2}_{\mathbb{N}})^{\mathbf{2}} = n^m_{\mathbb{N}}$.

(29) If $n \neq 0$ and $1 \leqslant k$, then $(n^k_{\mathbb{N}}) \div n = n^{k -' 1}_{\mathbb{N}}$.

(30) $2^{n+1}_{\mathbb{N}} = (2^n_{\mathbb{N}}) + 2^n_{\mathbb{N}}$.

(31) If $k > 1$ and $k^n_{\mathbb{N}} = k^m_{\mathbb{N}}$, then $n = m$.

(32) $m \leqslant n$ iff $2^m_{\mathbb{N}} \mid 2^n_{\mathbb{N}}$.

(33) If p is prime and $i \mid p_{\mathbb{N}}^{n}$, then $i = 1$ or there exists a natural number k such that $i = p \cdot k$.

(34) For every n such that $n \neq 0$ and p is prime and $n < p_{\mathbb{N}}^{k+1}$ holds $n \mid p_{\mathbb{N}}^{k+1}$ iff $n \mid p_{\mathbb{N}}^{k}$.

(35) For every k such that p is prime and $d \mid p_{\mathbb{N}}^{k}$ and $d \neq 0$ there exists a natural number t such that $d = p_{\mathbb{N}}^{t}$ and $t \leqslant k$.

(36) If $p > 1$ and $i \bmod p = 1$, then $(i_{\mathbb{N}}^{n}) \bmod p = 1$.

(37) If $m > 0$ and $n > 0$, then $(n_{\mathbb{N}}^{m}) \bmod n = 0$.

(38) If p is prime and n and p are relative prime, then $(n_{\mathbb{N}}^{p-'1}) \bmod p = 1$.

(39) If p is prime and $d > 1$ and $d \mid p_{\mathbb{N}}^{k}$ and $d \nmid (p_{\mathbb{N}}^{k}) \div p$, then $d = p_{\mathbb{N}}^{k}$.

Let a be an integer. Then $a^{\mathbf{2}}$ is a natural number.

We now state several propositions:

(40) For every n such that $n > 1$ holds $m \bmod n = 1$ iff $m \equiv 1 (\bmod\, n)$.

(41) If $a \equiv b (\bmod\, c)$, then $a^{\mathbf{2}} \equiv b^{\mathbf{2}} (\bmod\, c)$.

(42) If $i_5 = i_3 \cdot i_4$ and $i_1 \equiv i_2 (\bmod\, i_5)$, then $i_1 \equiv i_2 (\bmod\, i_3)$ and $i_1 \equiv i_2 (\bmod\, i_4)$.

(43) If $i_1 \equiv i_2 (\bmod\, i_5)$ and $i_1 \equiv i_3 (\bmod\, i_5)$, then $i_2 \equiv i_3 (\bmod\, i_5)$.

(44) 3 is prime.

(45) If $n \neq 0$, then $\mathrm{Euler}\, n \neq 0$.

(46) If $n \neq 0$, then $-n < n$.

(47) For all m, n such that $n > 0$ and $n > m$ holds $m \div n = 0$.

(48) If $n \neq 0$, then $n \div n = 1$.

2. Public-Key Cryptography

Let us consider k, m, n. The functor $\mathrm{Crypto}(m, n, k)$ yielding a natural number is defined as follows:

(Def. 1) $\mathrm{Crypto}(m, n, k) = (m_{\mathbb{N}}^{k}) \bmod n$.

One can prove the following proposition

(49) Suppose p is prime and q is prime and $p \neq q$ and $n = p \cdot q$ and k_1 and $\mathrm{Euler}\, n$ are relative prime and $k_1 \cdot k_2 \bmod \mathrm{Euler}\, n = 1$. Let m be a natural number. If $m < n$, then $\mathrm{Crypto}(\mathrm{Crypto}(m, n, k_1), n, k_2) = m$.

3. Order's Function

Let us consider i, p. Let us assume that $p > 1$ and i and p are relative prime. The functor $\mathrm{order}(i,p)$ yields a natural number and is defined as follows:

(Def. 2) $\mathrm{order}(i,p) > 0$ and $(i_{\mathbb{N}}^{\mathrm{order}(i,p)}) \bmod p = 1$ and for every k such that $k > 0$ and $(i_{\mathbb{N}}^{k}) \bmod p = 1$ holds $0 < \mathrm{order}(i,p)$ and $\mathrm{order}(i,p) \leqslant k$.

One can prove the following propositions:

(50) If $p > 1$, then $\mathrm{order}(1,p) = 1$.

(51) If $p > 1$ and i and p are relative prime, then $\mathrm{order}(i,p) \neq 0$.

(52) If $p > 1$ and $n > 0$ and $(i_{\mathbb{N}}^{n}) \bmod p = 1$ and i and p are relative prime, then $\mathrm{order}(i,p) \mid n$.

(53) If $p > 1$ and i and p are relative prime and $\mathrm{order}(i,p) \mid n$, then $(i_{\mathbb{N}}^{n}) \bmod p = 1$.

(54) If p is prime and i and p are relative prime, then $\mathrm{order}(i,p) \mid p -' 1$.

4. Fermat Number

Let n be a natural number. The functor $\mathrm{Fermat}\, n$ yielding a natural number is defined as follows:

(Def. 3) $\mathrm{Fermat}\, n = (2_{\mathbb{N}}^{2_{\mathbb{N}}^{n}}) + 1$.

Next we state several propositions:

(55) $\mathrm{Fermat}\, 0 = 3$.

(56) $\mathrm{Fermat}\, 1 = 5$.

(57) $\mathrm{Fermat}\, 2 = 17$.

(58) $\mathrm{Fermat}\, 3 = 257$.

(59) $\mathrm{Fermat}\, 4 = 256 \cdot 256 + 1$.

(60) $\mathrm{Fermat}\, n > 2$.

(61) If p is prime and $p > 2$ and $p \mid \mathrm{Fermat}\, n$, then there exists a natural number k such that $p = k \cdot 2_{\mathbb{N}}^{n+1} + 1$.

(62) If $n \neq 0$, then 3 and $\mathrm{Fermat}\, n$ are relative prime.

5. Pepin's Test

We now state several propositions:

(63) If $n > 0$ and $3_{\mathbb{N}}^{(\mathrm{Fermat}\, n -' 1) \div 2} \equiv -1 (\mathrm{mod}\, \mathrm{Fermat}\, n)$, then $\mathrm{Fermat}\, n$ is prime.

(64) 5 is prime.

(65) 17 is prime.

(66) 257 is prime.

(67) $256 \cdot 256 + 1$ is prime.

References

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

[2] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.

[3] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

[4] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

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

[6] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[7] Konrad Raczkowski and Andrzej Nędzusiak. Serieses. *Formalized Mathematics*, 2(**4**):449–452, 1991.

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

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

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

Received December 21, 1998