JOURNAL OF FORMALIZED MATHEMATICS
Volume 10, Released 1998, Published 2003
Inst. of Computer Science, Univ. 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`.

WWW: `http://mizar.org/JFM/Vol10/pepin.html`

The articles [10], [14], [11], [13], [6], [2], [1], [8], [7], [9], [12], [4], [5], and [3] provide the notation and terminology for this paper.

1. Some Useful Theorems

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

We now state four propositions:

(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.

The following propositions are true:

(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) $(a \cdot p + 1) \bmod p = 1 \bmod p$.

(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) $p^k \bmod m = (p \bmod m)^k \bmod m$.

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

(14) If $k^{\mathbf{2}} < j$ 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 2^n 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 is odd.

(21) If $k > 0$ and i is even, then i^k 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) $n^2 = n^{\mathbf{2}}$.

(26)[1] If $m > 1$ and $n > 0$, then $m^n > 1$.

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

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

(29) If $n \neq 0$ and $1 \leq k$, then $n^k \div n = n^{k -' 1}$.

(30) $2^{n+1} = 2^n + 2^n$.

(31) If $k > 1$ and $k^n = k^m$, then $n = m$.

(32) $m \leq n$ iff $2^m \mid 2^n$.

(33) If p is prime and $i \mid p^n$, 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 $n < p^{k+1}$ holds $n \mid p^{k+1}$ iff $n \mid p^k$.

(35) For every k such that p is prime and $d \mid p^k$ and $d \neq 0$ there exists a natural number t such that $d = p^t$ and $t \leq k$.

(36) If $p > 1$ and $i \bmod p = 1$, then $i^n \bmod p = 1$.

(37) If $m > 0$, then $n^m \bmod n = 0$.

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

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

[1] The proposition (25) has been removed.

Let a be an integer. Then $a^{\mathbf{2}}$ is a natural number.
Next we 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 $a^{\mathbf{2}} \equiv b^{\mathbf{2}} (\bmod c)$.

(43)[2] 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 Euler $n \neq 0$.

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

(48)[3] If $n \neq 0$, then $n \div n = 1$.

2. Public-Key Cryptography

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

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

Next we state the proposition

(49) Suppose p is prime and q is prime and $p \neq q$ and $n = p \cdot q$ and k_1 and 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 $i^{\mathrm{order}(i,p)} \bmod p = 1$ and for every k such that $k > 0$ and $i^k \bmod p = 1$ holds $0 < \mathrm{order}(i,p)$ and $\mathrm{order}(i,p) \leq k$.

The following propositions are true:

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

(52)[4] If $p > 1$ and $n > 0$ and $i^n \bmod p = 1$ 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 $i^n \bmod p = 1$.

(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 Fermat n yielding a natural number is defined by:

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

We now state several propositions:

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

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

[2] The proposition (42) has been removed.
[3] The proposition (47) has been removed.
[4] The proposition (51) has been removed.

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

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

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

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

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

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

5. PEPIN'S TEST

Next we state several propositions:

(63) If $3^{(\text{Fermat}\,n -' 1) \div 2} \equiv -1 (\bmod \text{Fermat}\,n)$, then $\text{Fermat}\,n$ 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. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/card_1.html`.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[3] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finset_1.html`.

[4] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/euler_1.html`.

[5] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Journal of Formalized Mathematics*, 10, 1998. `http://mizar.org/JFM/Vol10/euler_2.html`.

[6] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_2.html`.

[7] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/binarith.html`.

[8] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Journal of Formalized Mathematics*, 3, 1991. `http://mizar.org/JFM/Vol3/series_1.html`.

[9] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/abian.html`.

[10] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[11] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[12] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers operations: min, max, square, and square root. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/square_1.html`.

[13] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[14] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

Received December 21, 1998

Published January 2, 2004