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

Euler's Theorem and Small Fermat's Theorem

Yoshinori Fujisawa
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Hidetaka Shimizu
Information Technology Research Institute
of Nagano Prefecture

Summary. This article is concerned with Euler's theorem and small Fermat's theorem that play important roles in public-key cryptograms. In the first section, we present some selected theorems on integers. In the following section, we remake definitions about the finite sequence of natural, the function of natural times finite sequence of natural and π of the finite sequence of natural. We also prove some basic theorems that concern these redefinitions. Next, we define the function of modulus for finite sequence of natural and some fundamental theorems about this function are proved. Finally, Euler's theorem and small Fermat's theorem are proved.

MML Identifier: `EULER_2`.

WWW: `http://mizar.org/JFM/Vol10/euler_2.html`

The articles [14], [17], [15], [1], [16], [13], [8], [2], [5], [12], [9], [11], [7], [18], [4], [6], [3], and [10] provide the notation and terminology for this paper.

1. Preliminary

We adopt the following convention: a, b, m, n, k, l are natural numbers, t is an integer, and f, F are finite sequences of elements of $\mathbb{N}$.

The following propositions are true:

(1) a and b **qua** integer are relative prime iff a and b are relative prime.

(2) If $m > 1$ and $m \cdot t \geq 1$, then $t \geq 1$.

(3) If $m > 1$ and $m \cdot t \geq 0$, then $t \geq 0$.

(5)[1] Suppose $a \neq 0$ and $b \neq 0$ and $m \neq 0$ and a and m are relative prime and b and m are relative prime. Then m and $a \cdot b \bmod m$ are relative prime.

(6) Suppose $m > 1$ and $b \neq 0$ and m and n are relative prime and a and m are relative prime and $n = a \cdot b \bmod m$. Then m and b are relative prime.

(7) For every n holds $m \bmod n \bmod n = m \bmod n$.

(8) For every n holds $(l+m) \bmod n = ((l \bmod n) + (m \bmod n)) \bmod n$.

[1] The proposition (4) has been removed.

(9) For every n holds $l \cdot m \bmod n = l \cdot (m \bmod n) \bmod n$.

(10) For every n holds $l \cdot m \bmod n = (l \bmod n) \cdot m \bmod n$.

(11) For every n holds $l \cdot m \bmod n = (l \bmod n) \cdot (m \bmod n) \bmod n$.

2. Finite Sequence of Naturals

Let us consider a, f. Then $a \cdot f$ is a finite sequence of elements of $\mathbb{N}$.

One can prove the following proposition

(25)[2] For all finite sequences R_1, R_2 of elements of $\mathbb{N}$ such that R_1 and R_2 are fiberwise equipotent holds $\prod R_1 = \prod R_2$.

3. Modulus for Finite Sequence of Naturals

Let f be a finite sequence of elements of $\mathbb{N}$ and let m be a natural number. The functor $f \bmod m$ yielding a finite sequence of elements of $\mathbb{N}$ is defined as follows:

(Def. 1) $\mathrm{len}(f \bmod m) = \mathrm{len}\, f$ and for every natural number i such that $i \in \mathrm{dom}\, f$ holds $(f \bmod m)(i) = f(i) \bmod m$.

The following propositions are true:

(26) For every finite sequence f of elements of $\mathbb{N}$ such that $m \neq 0$ holds $\prod(f \bmod m) \bmod m = \prod f \bmod m$.

(27) If $a \neq 0$ and $m > 1$ and $n \neq 0$ and $a \cdot n \bmod m = n \bmod m$ and m and n are relative prime, then $a \bmod m = 1$.

(28) For every F holds $F \bmod m \bmod m = F \bmod m$.

(29) For every F holds $a \cdot (F \bmod m) \bmod m = a \cdot F \bmod m$.

(30) For all finite sequences F, G of elements of $\mathbb{N}$ holds $F \frown G \bmod m = (F \bmod m) \frown (G \bmod m)$.

(31) For all finite sequences F, G of elements of $\mathbb{N}$ holds $a \cdot (F \frown G) \bmod m = (a \cdot F \bmod m) \frown (a \cdot G \bmod m)$.

Let us consider n, k. Then n^k is a natural number.

One can prove the following proposition

(32) If $a \neq 0$ and $m \neq 0$ and a and m are relative prime, then for every b holds a^b and m are relative prime.

4. Euler's Theorem and Small Fermat's Theorem

The following two propositions are true:

(33) If $a \neq 0$ and $m > 1$ and a and m are relative prime, then $a^{\mathrm{Euler}\, m} \bmod m = 1$.

(34) If $a \neq 0$ and m is prime and a and m are relative prime, then $a^m \bmod m = a \bmod m$.

Acknowledgments

The authors wish to thank Professor A. Trybulec for all of his advice on this article.

[2] The propositions (12)–(24) have been removed.

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] Grzegorz Bancerek. Joining of decorated trees. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/trees_4.html`.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[5] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[6] Czesław Byliński. Semigroup operations on finite subsets. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/setwop_2.html`.

[7] Czesław Byliński. The sum and product of finite sequences of real numbers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/rvsum_1.html`.

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

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

[10] Andrzej Kondracki. The Chinese Remainder Theorem. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/wsierp_1.html`.

[11] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/rfinseq.html`.

[12] Rafał Kwiatek. Factorial and Newton coefficients. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/newton.html`.

[13] 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`.

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

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

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

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

[18] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_1.html`.

Received June 10, 1998

Published January 2, 2004