FORMALIZED MATHEMATICS
Volume 7, Number 1, 1998
University 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.

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

1. Preliminary

We use the following convention: a, b, m, n, k, l, i, j, n_1, n_2, n_3 are natural numbers, t is an integer, and f, F are finite sequences of elements of $\mathbb{N}$.

We now state a number of propositions:

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

ISSN 1426–2630

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

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

(4) If $m \neq 0$, then $n \bmod m = (n$ **qua** integer$) \bmod m$.

(5) 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 such that $n \neq 0$ holds $m \bmod n \bmod n = m \bmod n$.

(8) For every n such that $n \neq 0$ holds $(l + m) \bmod n = ((l \bmod n) + (m \bmod n)) \bmod n$.

(9) For every n such that $n \neq 0$ holds $l \cdot m \bmod n = l \cdot (m \bmod n) \bmod n$.

(10) For every n such that $n \neq 0$ holds $l \cdot m \bmod n = (l \bmod n) \cdot m \bmod n$.

(11) For every n such that $n \neq 0$ holds $l \cdot m \mathrm{mod} n = (l \mathrm{mod} n) \cdot (m \mathrm{mod} n) \mathrm{mod} n$.

2. Finite Sequence of Naturals

We now state two propositions:

(12) For every finite sequence f of elements of $\mathbb{N}$ such that $n \neq 0$ and $n \leqslant m$ holds $(f \restriction m)(n) = f(n)$.

(13) For every finite sequence f of elements of $\mathbb{N}$ such that $n \leqslant m$ holds $f \restriction m \restriction n = f \restriction n$.

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

One can prove the following propositions:

(14) For every finite sequence f of elements of $\mathbb{N}$ and for every natural number r holds $\prod(f \frown \langle r \rangle) = \prod f \cdot r$.

(15) For all finite sequences f_1, f_2 of elements of $\mathbb{N}$ holds $\prod(f_1 \frown f_2) = \prod f_1 \cdot \prod f_2$.

(16) $\prod(\varepsilon_{\mathbb{N}}) = 1$.

(17) $\prod\langle a \rangle = a$.

(18) $\prod(\langle a \rangle \frown F) = a \cdot \prod F$.

(19) $\prod\langle n_1, n_2 \rangle = n_1 \cdot n_2$.

(20) $\prod\langle n_1, n_2, n_3 \rangle = n_1 \cdot n_2 \cdot n_3$.

(21) $\prod(i \mapsto (1$ **qua** real number$)) = 1$.

(22) $\prod((i + j) \mapsto m) = \prod(i \mapsto m) \cdot \prod(j \mapsto m)$.

(23) $\prod((i \cdot j) \mapsto m) = \prod(j \mapsto \prod(i \mapsto m))$.

(24) $\prod(i \mapsto (n_1 \cdot n_2)) = \prod(i \mapsto n_1) \cdot \prod(i \mapsto n_2)$.

(25) 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 by:

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

We now state several propositions:

(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 such that $m \neq 0$ holds $F \bmod m \bmod m = F \bmod m$.

(29) For every F such that $m \neq 0$ holds $a \cdot (F \bmod m) \bmod m = a \cdot F \bmod m$.

(30) For all finite sequences F, G of elements of $\mathbb{N}$ such that $m \neq 0$ holds $F \frown G \bmod m = (F \bmod m) \frown (G \bmod m)$.

(31) For all finite sequences F, G of elements of $\mathbb{N}$ such that $m \neq 0$ 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 $n_{\mathbb{N}}^{k}$ is a natural number.

We now state the proposition

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

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

The following propositions are true:

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

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

Acknowledgments

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

References

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

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[4] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[5] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\mathrm{T}}$. Arcs, line segments and special polygonal arcs. *Formalized Mathematics*, 2(**5**):617–621, 1991.

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

[7] Andrzej Kondracki. The chinese remainder theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[8] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.

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

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

[11] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

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

Received June 10, 1998