FORMALIZED MATHEMATICS
Volume 6, Number 4, 1997
University of Białystok

The Euler's Function

Yoshinori Fujisawa
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Summary. This article is concerned with the Euler's function [10] that plays an important role in cryptograms. In the first section, we present some selected theorems on integers. Next, we define the Euler's function. Finally, three theorems relating to the Euler's function are proved. The third theorem concerns two relatively prime integers which make up the Euler's function parameter. In the public key cryptography these two integer values are used as public and secret keys.

MML Identifier: `EULER_1`.

The notation and terminology used here are introduced in the following papers: [12], [6], [1], [13], [9], [2], [3], [7], [8], [14], [11], [15], [4], and [5].

1. Preliminary

We follow the rules: a, b, c, k, l, m, n are natural numbers and i, j, x, y are integers.

The following propositions are true:

(1) $k \in n$ iff $k < n$.

(2) n and n are relative prime iff $n = 1$.

(3) If $k \neq 0$ and $k < n$ and n is prime, then k and n are relative prime.

(4) n is prime and $k \in \{k_1; k_1$ ranges over natural numbers: n and k_1 are relative prime $\wedge\ k_1 \geqslant 1\ \wedge\ k_1 \leqslant n\}$ if and only if n is prime and $k \in n$ and $k \notin \{0\}$.

(5) For every finite set A and for every set x such that $x \in A$ holds $\overline{\overline{A \setminus \{x\}}} = \overline{\overline{A}} - \overline{\overline{\{x\}}}$.

ISSN 1426–2630

(6) If $\gcd(a, b) = 1$, then for every c holds $\gcd(a \cdot c, b \cdot c) = c$.

(7) If $a \neq 0$ and $b \neq 0$ and $c \neq 0$ and $\gcd(a \cdot c, b \cdot c) = c$, then a and b are relative prime.

(8) If $\gcd(a, b) = 1$, then $\gcd(a + b, b) = 1$.

(9) For every c holds $\gcd(a + b \cdot c, b) = \gcd(a, b)$.

(10) Suppose m and n are relative prime. Then there exists k such that

(i) there exist integers i_0, j_0 such that $k = i_0 \cdot m + j_0 \cdot n$ and $k > 0$, and

(ii) for every l such that there exist integers i, j such that $l = i \cdot m + j \cdot n$ and $l > 0$ holds $k \leqslant l$.

(11) If m and n are relative prime, then for every k there exist i, j such that $i \cdot m + j \cdot n = k$.

(12) For all non empty finite sets A, B such that there exists a function from A into B which is one-to-one and onto holds $\overline{\overline{A}} = \overline{\overline{B}}$.

(13) For all integers i, k, n such that $n \neq 0$ holds $(i + k \cdot n) \bmod n = i \bmod n$.

(14) If $a \neq 0$ and $b \neq 0$ and $c \neq 0$ and $c \mid a \cdot b$ and a and c are relative prime, then $c \mid b$.

(15) Suppose $a \neq 0$ and $b \neq 0$ and $c \neq 0$ and a and c are relative prime and b and c are relative prime. Then $a \cdot b$ and c are relative prime.

(16) If $x \neq 0$ and $y \neq 0$ and $i > 0$, then $i \cdot x \gcd i \cdot y = i \cdot (x \gcd y)$.

(17) For every x such that $a \neq 0$ and $b \neq 0$ holds $a + x \cdot b \gcd b = a \gcd b$.

2. Definition of Euler's Function

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

(Def. 1) $\mathrm{Euler}\, n = \overline{\overline{\{k; k \text{ ranges over natural numbers: } n \text{ and } k \text{ are relative prime } \wedge\ k \geqslant 1\ \wedge\ k \leqslant n\}}}$.

We now state several propositions:

(18) $\mathrm{Euler}\, 1 = 1$.

(19) $\mathrm{Euler}\, 2 = 1$.

(20) If $n > 1$, then $\mathrm{Euler}\, n \leqslant n - 1$.

(21) If n is prime, then $\mathrm{Euler}\, n = n - 1$.

(22) If $m > 1$ and $n > 1$ and m and n are relative prime, then $\mathrm{Euler}\, m \cdot n = \mathrm{Euler}\, m \cdot \mathrm{Euler}\, n$.

Acknowledgments

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

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

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

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

[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

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

[7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

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

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

[10] Teiji Takagi. *Elementary Theory of Numbers.* Kyoritsu Publishing Co., Ltd., second edition, 1995.

[11] Yozo Toda. The formalization of simple graphs. *Formalized Mathematics*, 5(**1**):137–144, 1996.

[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

[14] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

[15] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received December 10, 1997