JOURNAL OF FORMALIZED MATHEMATICS
Volume 9, Released 1997, Published 2003
Inst. of Computer Science, Univ. 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`.

WWW: `http://mizar.org/JFM/Vol9/euler_1.html`

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

1. Preliminary

We adopt the following convention: a, b, c, k, l, m, n denote natural numbers and i, j, x, y denote integers.

The following propositions are true:

(1) For all natural numbers k, n holds $k \in n$ 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 $\wedge\ k_1 \geq 1 \wedge k_1 \leq n\}$ 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 $\overline{\overline{A \setminus \{x\}}} = \overline{\overline{A}} - \overline{\overline{\{x\}}}$.

(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 $k \leq l$.

© Association of Mizar Users

(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 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 $i \cdot x \operatorname{gcd} i \cdot y = i \cdot (x \operatorname{gcd} y)$.

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

2. Euler's Function — Definition and theorems

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

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

One can prove the following proposition

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

Next we state four propositions:

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

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

(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. *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. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal2.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. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[7] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

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

[9] 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.

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

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

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

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

Received December 10, 1997

Published January 2, 2004