FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 151–155, 2009
DOI: 10.2478/v10037-009-0017-7

Properties of Primes and Multiplicative Group of a Field

Kenichi Arai
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In the [16] has been proven that the multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$ is a cyclic group. Likewise, finite subgroup of the multiplicative group of a field is a cyclic group. However, finite subgroup of the multiplicative group of a field being a cyclic group has not yet been proven. Therefore, it is of importance to prove that finite subgroup of the multiplicative group of a field is a cyclic group.

Meanwhile, in cryptographic system like RSA, in which security basis depends upon the difficulty of factorization of given numbers into prime factors, it is important to employ integers that are difficult to be factorized into prime factors. If both p and $2p + 1$ are prime numbers, we call p as Sophie Germain prime, and $2p + 1$ as safe prime. It is known that the product of two safe primes is a composite number that is difficult for some factoring algorithms to factorize into prime factors. In addition, safe primes are also important in cryptography system because of their use in discrete logarithm based techniques like Diffie-Hellman key exchange. If p is a safe prime, the multiplicative group of numbers modulo p has a subgroup of large prime order. However, no definitions have not been established yet with the safe prime and Sophie Germain prime. So it is important to give definitions of the Sophie Germain prime and safe prime.

In this article, we prove finite subgroup of the multiplicative group of a field is a cyclic group, and, further, define the safe prime and Sophie Germain prime, and prove several facts about them. In addition, we define Mersenne number (M_n), and some facts about Mersenne numbers and prime numbers are proven.

MML identifier: GR_CY_3, version: 7.11.02 4.125.1059

The articles [24], [9], [4], [10], [2], [19], [20], [14], [3], [25], [6], [8], [7], [5], [22], [21], [23], [18], [12], [15], [13], [11], [17], [16], and [1] provide the notation and terminology for this paper.

ISSN 1426–2630(p), 1898-9934(e)

1. Properties of Primes

One can prove the following proposition

(1) For all prime numbers p, q and for every natural number k such that $k \mid p \cdot q$ holds $k = 1$ or $k = p$ or $k = q$ or $k = p \cdot q$.

Let p be a natural number. We say that p is safe if and only if:

(Def. 1) There exists a prime number s such that $2 \cdot s + 1 = p$.

Let us observe that there exists a prime number which is safe.

One can prove the following propositions:

(2) For every safe prime number p holds $p \geq 5$.

(3) For every safe prime number p holds $p \bmod 2 = 1$.

(4) For every safe prime number p such that $p \neq 7$ holds $p \bmod 3 = 2$.

(5) For every safe prime number p such that $p \neq 5$ holds $p \bmod 4 = 3$.

(6) For every safe prime number p such that $p \neq 7$ holds $p \bmod 6 = 5$.

(7) For every safe prime number p such that $p > 7$ holds $p \bmod 12 = 11$.

(8) For every safe prime number p such that $p > 5$ holds $p \bmod 8 = 3$ or $p \bmod 8 = 7$.

Let p be a natural number. We say that p is Sophie Germain if and only if:

(Def. 2) $2 \cdot p + 1$ is a prime number.

Let us observe that there exists a prime number which is Sophie Germain.

One can prove the following propositions:

(9) For every Sophie Germain prime number p such that $p > 2$ holds $p \bmod 4 = 1$ or $p \bmod 4 = 3$.

(10) For every safe prime number p there exists a Sophie Germain prime number q such that $p = 2 \cdot q + 1$.

(11) For every safe prime number p there exists a Sophie Germain prime number q such that $\operatorname{Euler} p = 2 \cdot q$.

(12) Let p_1, p_2 be safe prime numbers and N be a natural number. Suppose $p_1 \neq p_2$ and $N = p_1 \cdot p_2$. Then there exist Sophie Germain prime numbers q_1, q_2 such that $\operatorname{Euler} N = 4 \cdot q_1 \cdot q_2$.

(13) For every safe prime number p there exists a Sophie Germain prime number q such that $\operatorname{Card} \mathbb{Z}/p\mathbb{Z}^* = 2 \cdot q$.

(14) Let G be a cyclic finite group and n, m be natural numbers. Suppose $\operatorname{Card} G = n \cdot m$. Then there exists an element a of G such that $\operatorname{ord}(a) = n$ and $\operatorname{gr}(\{a\})$ is a strict subgroup of G.

(15) Let p be a safe prime number. Then there exists a Sophie Germain prime number q and there exist strict subgroups H_1, H_2, H_3, H_4 of $\mathbb{Z}/p\mathbb{Z}^*$ such that $\operatorname{Card} H_1 = 1$ and $\operatorname{Card} H_2 = 2$ and $\operatorname{Card} H_3 = q$ and $\operatorname{Card} H_4 = 2 \cdot q$

and for every strict subgroup H of $\mathbb{Z}/p\mathbb{Z}^*$ holds $H = H_1$ or $H = H_2$ or $H = H_3$ or $H = H_4$.

Let n be a natural number. The functor M_n yielding a natural number is defined as follows:

(Def. 3) $M_n = 2^n - 1$.

The following propositions are true:

(16) $M_0 = 0$.

(17) $M_1 = 1$.

(18) $M_2 = 3$.

(19) $M_3 = 7$.

(20) $M_5 = 31$.

(21) $M_7 = 127$.

(22) $M_{11} = 23 \cdot 89$.

(23) For every prime number p such that $p \neq 2$ holds $M_p \bmod 2 \cdot p = 1$.

(24) For every prime number p such that $p \neq 2$ holds $M_p \bmod 8 = 7$.

(25) For every Sophie Germain prime number p such that $p > 2$ and $p \bmod 4 = 3$ there exists a safe prime number q such that $q \mid M_p$.

(26) Let p be a Sophie Germain prime number. If $p > 2$ and $p \bmod 4 = 1$, then there exists a safe prime number q such that $M_p \bmod q = q - 2$.

(27) For all natural numbers a, n such that $a > 1$ holds $a - 1 \mid a^n - 1$.

(28) For all natural numbers a, p such that $p > 1$ and $a^p - 1$ is a prime number holds $a = 2$ and p is a prime number.

(29) For every natural number p such that $p > 1$ and M_p is a prime number holds p is a prime number.

(30) For every integer a and for all natural numbers x, n holds $a^x \bmod n = (a \bmod n)^x \bmod n$.

(31) For all integers x, y, n such that x and n are relative prime and $x \equiv y \pmod n$ holds y and n are relative prime.

(32) Let a, x be natural numbers and p be a prime number. Suppose a and p are relative prime and $a \equiv x \cdot x \pmod p$. Then x and p are relative prime.

(33) Let a, x be integers and p be a prime number. Suppose a and p are relative prime and $a \equiv x \cdot x \pmod p$. Then x and p are relative prime.

(34) For all integers a, b and for all natural numbers n, x such that $a \equiv b \pmod n$ and $n \neq 0$ holds $a^x \equiv b^x \pmod n$.

(35) For every integer a and for every prime number n such that $a \cdot a \bmod n = 1$ holds $a \equiv 1 \pmod n$ or $a \equiv -1 \pmod n$.

2. Multiplicative Group of a Field

The following proposition is true

(36) For every prime number p holds $\mathbb{Z}/p\mathbb{Z}^* = \mathrm{MultGroup}(\mathbb{Z}_p^{\mathrm{R}})$.

Let F be a commutative skew field. Observe that $\mathrm{MultGroup}(F)$ is commutative.

One can prove the following two propositions:

(37) Let F be a commutative skew field, x be an element of $\mathrm{MultGroup}(F)$, and x_1 be an element of F. If $x = x_1$, then $x^{-1} = {x_1}^{-1}$.

(38) For every commutative skew field F holds every finite subgroup of $\mathrm{MultGroup}(F)$ is a cyclic group.

References

[1] Broderick Arneson and Piotr Rudnicki. Primitive roots of unity and cyclotomic polynomials. *Formalized Mathematics*, 12(**1**):59–67, 2004.
[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[5] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.
[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[13] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[15] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[16] Hiroyuki Okazaki and Yasunari Shidama. Uniqueness of factoring an integer and multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$. *Formalized Mathematics*, 16(**2**):103–107, 2008, doi:10.2478/v10037-008-0015-1.
[17] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[18] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[22] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

[23] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received April 7, 2009