FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 265–269, 2012
DOI: 10.2478/v10037-012-0031-z

VERSITA
versita.com/fm/

# Basic Properties of Primitive Root and Order Function[1]

Na Ma
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

**Summary.** In this paper we defined the reduced residue system and proved its fundamental properties. Then we proved the basic properties of the order function. Finally, we defined the primitive root and proved its fundamental properties. Our work is based on [12], [8], and [11].

MML identifier: `INT_8`, version: `8.0.01 5.3.1162`

The notation and terminology used here have been introduced in the following papers: [1], [18], [9], [4], [7], [5], [20], [16], [17], [19], [14], [2], [15], [3], [10], [13], [22], [23], [21], and [6].

For simplicity, we adopt the following convention: $i$, $s$, $t$, $m$, $n$, $k$ are natural numbers, $d$, $e$ are elements of $\mathbb{N}$, $f_1$ is a finite sequence of elements of $\mathbb{N}$, and $x$ is an integer.

Let $m$ be a natural number. The functor $\mathrm{RelPrimes}\, m$ yields a set and is defined by:

(Def. 1) $\mathrm{RelPrimes}\, m = \{k \in \mathbb{N}\colon m$ and $k$ are relative prime $\wedge\ 1 \leq k\ \wedge\ k \leq m\}$.

We now state the proposition

(1) $\mathrm{RelPrimes}\, m \subseteq \mathrm{Seg}\, m$.

Let $m$ be a natural number. Then $\mathrm{RelPrimes}\, m$ is a subset of $\mathbb{N}$.

Let $m$ be a natural number. Observe that $\mathrm{RelPrimes}\, m$ is finite.

Next we state several propositions:

(2) If $1 \leq m$, then $\mathrm{RelPrimes}\, m \neq \emptyset$.

[1]Authors thank Andrzej Trybulec and Yatsuka Nakamura for the help during writing this article.




ISSN 1426–2630(p), 1898-9934(e)

(3) For every subset $X$ of $\mathbb{Z}$ and for every integer $a$ holds $x \in a \circ X$ iff there exists an integer $y$ such that $y \in X$ and $x = a \cdot y$.

(4) There exists a natural number $r$ such that $(1+s)^t = 1+t\cdot s+\binom{t}{2}\cdot s^{\mathbf{2}}+r\cdot s^3$.

(5) If $n > 1$ and $i$ and $n$ are relative prime, then $i \neq 0$.

(6) For all integers $a$, $b$ and for every natural number $m$ such that $a \cdot b \bmod m = 1$ and $a \bmod m = 1$ holds $b \bmod m = 1$.

(7) For every odd integer $x$ and for every natural number $k$ such that $k \geq 3$ holds $x^{2^{k-'2}} \bmod 2^k = 1$.

In the sequel $p$ is a prime number.

We now state a number of propositions:

(8) If $m \geq 1$, then $\mathrm{Euler}\, p^m = p^m - p^{m-'1}$.

(9) If $n > 1$ and $i$ and $n$ are relative prime, then $\mathrm{order}(i, n) \mid \mathrm{Euler}\, n$.

(10) For all $i$, $n$ such that $n > 1$ and $i$ and $n$ are relative prime holds $i^s \equiv i^t \pmod{n}$ iff $s \equiv t \pmod{\mathrm{order}(i, n)}$.

(11) For all $i$, $n$ such that $n > 1$ and $i$ and $n$ are relative prime holds $i^s \equiv 1 \pmod{n}$ iff $\mathrm{order}(i, n) \mid s$.

(12) Suppose $n > 1$ and $i$ and $n$ are relative prime and $\mathrm{len}\, f_1 = \mathrm{order}(i, n)$ and for every $d$ such that $d \in \mathrm{dom}\, f_1$ holds $f_1(d) = i^{d-'1}$. Let given $d$, $e$. If $d$, $e \in \mathrm{dom}\, f_1$ and $d \neq e$, then $f_1(d) \not\equiv f_1(e) \pmod{n}$.

(13) Suppose $n > 1$ and $i$ and $n$ are relative prime and $\mathrm{len}\, f_1 = \mathrm{order}(i, n)$ and for every $d$ such that $d \in \mathrm{dom}\, f_1$ holds $f_1(d) = i^{d-'1}$. Let given $d$. If $d \in \mathrm{dom}\, f_1$, then $f_1(d)^{\mathrm{order}(i,n)} \bmod n = 1$.

(14) If $n > 1$ and $i$ and $n$ are relative prime, then $\mathrm{order}(i^s, n) = \mathrm{order}(i, n) \operatorname{div} (\mathrm{order}(i, n) \gcd s)$.

(15) Let given $i$, $n$. Suppose $n > 1$ and $i$ and $n$ are relative prime. Then $\mathrm{order}(i, n)$ and $s$ are relative prime if and only if $\mathrm{order}(i^s, n) = \mathrm{order}(i, n)$.

(16) If $n > 1$ and $i$ and $n$ are relative prime and $\mathrm{order}(i, n) = s \cdot t$, then $\mathrm{order}(i^s, n) = t$.

(17) Suppose that

(i) $n > 1$,

(ii) $s$ and $n$ are relative prime,

(iii) $t$ and $n$ are relative prime, and

(iv) $\mathrm{order}(s, n)$ and $\mathrm{order}(t, n)$ are relative prime.

Then $\mathrm{order}(s \cdot t, n) = \mathrm{order}(s, n) \cdot \mathrm{order}(t, n)$.

In the sequel $f_2$, $f_3$ are finite sequences of elements of $\mathbb{N}$.

We now state four propositions:

(18) Suppose $n > 1$ and $s$ and $n$ are relative prime and $t$ and $n$ are relative prime and $\mathrm{order}(s \cdot t, n) = \mathrm{order}(s, n) \cdot \mathrm{order}(t, n)$. Then $\mathrm{order}(s, n)$ and $\mathrm{order}(t, n)$ are relative prime.

(19) If $n > 1$ and $s$ and $n$ are relative prime and $s \cdot t \bmod n = 1$, then $\mathrm{order}(s, n) = \mathrm{order}(t, n)$.

(20) If $n > 1$ and $m > 1$ and $i$ and $n$ are relative prime and $m \mid n$, then $\mathrm{order}(i, m) \mid \mathrm{order}(i, n)$.

(21) If $n > 1$ and $m > 1$ and $m$ and $n$ are relative prime and $i$ and $m \cdot n$ are relative prime, then $\mathrm{order}(i, m \cdot n) = \mathrm{lcm}(\mathrm{order}(i, m), \mathrm{order}(i, n))$.

Let $X$ be a set and let $m$ be a natural number. We say that $X$ is primitive root of $m$ if and only if the condition (Def. 2) is satisfied.

(Def. 2) There exists a finite sequence $f_2$ of elements of $\mathbb{Z}$ such that $\mathrm{len}\, f_2 = \mathrm{len}\, \mathrm{Sgm}\, \mathrm{RelPrimes}\, m$ and for every $d$ such that $d \in \mathrm{dom}\, f_2$ holds $f_2(d) \in [(\mathrm{Sgm}\, \mathrm{RelPrimes}\, m)(d)]_{\mathrm{Cong}\, m}$ and $X = \mathrm{rng}\, f_2$.

We now state several propositions:

(22) $\mathrm{RelPrimes}\, m$ is primitive root of $m$.

(23) If $d, e \in \mathrm{dom}\, \mathrm{Sgm}\, \mathrm{RelPrimes}\, m$ and $d \neq e$, then $(\mathrm{Sgm}\, \mathrm{RelPrimes}\, m)(d) \not\equiv (\mathrm{Sgm}\, \mathrm{RelPrimes}\, m)(e) \pmod{m}$.

(24) Let $X$ be a finite set. Suppose $X$ is primitive root of $m$. Then

(i) $\overline{\overline{X}} = \mathrm{Euler}\, m$,

(ii) for all integers $x$, $y$ such that $x, y \in X$ and $x \neq y$ holds $x \not\equiv y \pmod{m}$, and

(iii) for every integer $x$ such that $x \in X$ holds $x$ and $m$ are relative prime.

(25) $\emptyset$ is primitive root of $m$ iff $m = 0$.

(26) Let $X$ be a finite subset of $\mathbb{Z}$. Suppose that

(i) $1 < m$,

(ii) $\overline{\overline{X}} = \mathrm{Euler}\, m$,

(iii) for all integers $x$, $y$ such that $x, y \in X$ and $x \neq y$ holds $x \not\equiv y \pmod{m}$, and

(iv) for every integer $x$ such that $x \in X$ holds $x$ and $m$ are relative prime.

Then $X$ is primitive root of $m$.

(27) Let $X$ be a finite subset of $\mathbb{Z}$ and $a$ be an integer. Suppose $m > 1$ and $a$ and $m$ are relative prime and $X$ is primitive root of $m$. Then $a \circ X$ is primitive root of $m$.

Let us consider $i$, $n$. We say that $i$ is RRS of $n$ if and only if:

(Def. 3) $\mathrm{order}(i, n) = \mathrm{Euler}\, n$.

Next we state several propositions:

(28) Suppose $n > 1$ and $i$ and $n$ are relative prime. Then $i$ is RRS of $n$ if and only if for every $f_1$ such that $\mathrm{len}\, f_1 = \mathrm{Euler}\, n$ and for every natural number $d$ such that $d \in \mathrm{dom}\, f_1$ holds $f_1(d) = i^d$ holds $\mathrm{rng}\, f_1$ is primitive root of $n$.

(29) Suppose $p > 2$ and $i$ and $p$ are relative prime and $i$ is RRS of $p$. Let $k$ be a natural number. Then $i^{2\cdot k+1}$ is not quadratic residue mod $p$.

(30) Let $k$ be a natural number. Suppose $k \geq 3$. Let given $m$. If $m$ and $2^k$ are relative prime, then $m$ is not RRS of $2^k$.

(31) If $p > 2$ and $k \geq 2$ and $i$ and $p$ are relative prime and $i$ is RRS of $p$ and $i^{p-'1} \bmod p^{\mathbf{2}} \neq 1$, then $i^{\mathrm{Euler}\, p^{k-'1}} \bmod p^k \neq 1$.

(32) Suppose $n > 1$ and $\mathrm{len}\, f_2 \geq 2$ and for every $d$ such that $d \in \mathrm{dom}\, f_2$ holds $f_2(d)$ and $n$ are relative prime. Let given $f_3$. Suppose that

(i) $\mathrm{len}\, f_3 = \mathrm{len}\, f_2$,

(ii) for every $d$ such that $d \in \mathrm{dom}\, f_3$ holds $f_3(d) = \mathrm{order}(f_2(d), n)$, and

(iii) for all $d$, $e$ such that $d, e \in \mathrm{dom}\, f_3$ and $d \neq e$ holds $f_3(d)$ and $f_3(e)$ are relative prime.

Then $\mathrm{order}(\prod f_2, n) = \prod f_3$.

## 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. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 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] Zhang Dexin. *Integer Theory*. Science Publication, China, 1965.
[9] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.
[10] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.
[11] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Posts and Telecom Press, China, 2007.
[12] Hua Loo Keng. *Introduction to Number Theory*. Beijing Science Publication, China, 1957.
[13] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[14] Artur Korniłowicz. Collective operations on number-membered sets. *Formalized Mathematics*, 17(**2**):99–115, 2009, doi: 10.2478/v10037-009-0011-0.
[15] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[16] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[17] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007, doi:10.2478/v10037-007-0022-7.
[18] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[22] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[23] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

*Received August 6, 2012*