On the Reduced Testing of a Primitive Element in $\mathbb{Z}_n^\times$

Hideo SUZUKI*

The primitive roots in $\mathbb{Z}_n^\times$ are defined and exist iff $n = 2, 4, p^\alpha, 2p^\alpha$. Knuth gave the definition of the primitive roots in $\mathbb{Z}_{p^\alpha}^\times$, and showed the necessary and sufficient condition for testing a primitive root in $\mathbb{Z}_{p^\alpha}^\times$. In this paper we define the primitive elements in $\mathbb{Z}_n^\times$, which is a generalization of primitive roots, as elements that take the maximum multiplicative order. And we give two theorems for the reduced testing of a primitive element in $\mathbb{Z}_n^\times$ for any composite n. It is shown that the two theorems, using a technique of a lemma, for testing a primitive element allow us an effective reduction in testing processes and in computing time cost as a consequence.

Keywords: primitive element modulo a composite, primitive root, universal exponent

$\mathbb{Z}_n^\times$ 中の原始元の簡略化した識別法について

鈴 木 英 男 *

$\mathbb{Z}_n^\times$ の原始根は、$n = 2, 4, p^\alpha, 2p^\alpha$ のときのみ定義され、存在する。 Knuth は、$\mathbb{Z}_{p^\alpha}^\times$ の原始根の識別法のための必要十分条件を示した。 本稿では、最大位数をもつ一般化された原始根として、$\mathbb{Z}_n^\times$ 中の原始元を定義し、任意の合成数 n を法とする $\mathbb{Z}_n^\times$ 中の原始元の簡略化した識別法として２つの定理が示されている。 これら２つの定理は、原始元の識別処理を効果的に簡略化し、結果として高速な識別が可能となる。

キーワード: 合成数を法とする原始元, 原始根, ユニバーサル指数

*東京情報大学 総合情報学部
Tokyo University of Information Sciences, Faculty of Informatics

2015年６月30日受理

1. Introduction

The primitive roots in $\mathbb{Z}_n^\times$ are defined and exist iff $n = 2, 4, p^\alpha, 2p^\alpha$. Knuth[1] gave the definition of the primitive roots in $\mathbb{Z}_{p^\alpha}^\times$, and showed the necessary and sufficient condition for testing a primitive root in $\mathbb{Z}_{p^\alpha}^\times$. In this paper we define the primitive elements in $\mathbb{Z}_n^\times$, which is a generalization of primitive roots, as elements that take the maximum multiplicative order.

In Section 2, we denote the symbols and functions that are used in this paper. In Section 3, we mention the theorems and lemmas that are used in the following section.

In Section 4, we give two theorems for the reduced testing of a primitive element in $\mathbb{Z}_n^\times$ for any composite n. Actually, some practical applications based on number theory, such as linear congruencial random number generation algorithm and number theoretic cryptosystems, essentially need testing of a primitive element.

We will show that the two theorems using a technique for testing a primitive element allow us an effective reduction in testing processes.

2. Notation

In this section, we denote the symbols and functions that are used in this paper. All the numbers which are dealt are positive integers and zero, since we use the least non-negative residue system in modulo operations.

$a \mid b$: a divides b.

$a \nmid b$: a does not divide b.

$a \parallel b$: $a \mid b$ and $a^2 \nmid b$

$lcm(a_1, a_2, \ldots)$: the least common multiple of $a_1, a_2, \ldots$.

$gcd(a_1, a_2, \ldots)$: the greatest common divisor of $a_1, a_2, \ldots$.

$[a, b)$: the set $\{x : a \leq x < b\}$.

$Primes$: the set of prime numbers, e.g., $p_1(:=2), p_2, p_3, \ldots, p_i, p \in Primes$.

$Composites$: the set of composite numbers, e.g., $n \in Composite$.

$\mathbb{Z}_n$: the ring of integer modulo n, $\mathbb{Z}_n := [0, n)$.

$\mathbb{Z}_n^\times$: the multiplicative group of modulo n,
$\mathbb{Z}_n^\times := \{x \in \mathbb{Z}_n : gcd(x, n) = 1\}$.

$\#\{\cdot\}$: the cardinality or the number of elements in a set $\{\cdot\}$.

$Ord_n(a)$: the multiplicative order or the exponent of an element a in $\mathbb{Z}_n^\times$,
$Ord_n(a) := min\{x \in \mathbb{Z}_{>0} : a^x \equiv 1 (\mathrm{mod}\ n)\}$ if $gcd(a, n) = 1$.

$\phi(n)$: Euler's totient function of n or
$\#\{\mathbb{Z}_n^\times\}$,

$$\begin{aligned}\phi(n) &:= \#\{x \in \mathbb{Z}_n : gcd(x, n) = 1\},\\ &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots),\\ &= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3}) \cdots,\end{aligned}$$

$$\text{where } \begin{cases} n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots, \\ \phi(1) = 1, \\ \phi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1). \end{cases}$$

$\lambda(n)$: Carmichael's function of n, the universal exponent modulo n or
the maximum multiplicative order modulo n, ($Theorem$ 3.4)

$$\begin{aligned}\lambda(n) &:= max\{x : y \in \mathbb{Z}_n^\times, x = Ord_n(y)\},\\ &= \lambda(2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots),\\ &= lcm(\lambda(2^{\alpha_1}), \lambda(p_2^{\alpha_2}), \lambda(p_3^{\alpha_3}), \ldots),\end{aligned}$$

$$\text{where } \begin{cases} n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots, \\ \lambda(1) = \phi(1) = 1, \\ \lambda(p_1^{\alpha_1}) = \lambda(2^{\alpha_1}) = \begin{cases} \phi(2^{\alpha_1}) = 2^{\alpha_1 - 1} & (\alpha_1 = 1, 2), \\ \frac{\phi(2^{\alpha_1})}{2} = 2^{\alpha_1 - 2} & (\alpha_1 \geq 3), \end{cases} \\ \lambda(p_i^{\alpha_i}) = \phi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1)\ (i \geq 2). \end{cases}$$

$\psi_n(d)$: the cardinality of elements with a given order d in $\mathbb{Z}_n^{\times}$ with a composite n, and d is a divisors of $\lambda(n)$,
$\psi_n(d) := \#\{x \in \mathbb{Z}_n^{\times} : Ord_n(x) = d\}$ (*Theorem* 3.6).

3. Known results

Here we mention the theorems and lemmas that are used in the following section.

Theorem 3.1 *(Chinese Remainder Theorem[1]). Let $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$ be a positive integer. For a set of integers $u_1, u_2, u_3, \ldots, u_r$, there is exactly one integer u that satisfies the condition*

$$0 \le u < n, \quad \text{and} \quad (\forall\, i \in [1,r])[u \equiv u_i (\bmod\ p_i^{\alpha_i})],$$

in other words, for a set $\{u_i : i \in [1,r]$, an element u_i in $\mathbb{Z}_{p_i^{\alpha_i}}\}$, there is exactly one element u in $\mathbb{Z}_n$ that satisfies the condition

$$(\forall\, i \in [1,r])[u \equiv u_i (\bmod\ p_i^{\alpha_i})].$$

■

Lemma 3.2 *According to Chinese Remainder Theorem, for integers $a, x, n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$,*

$$a^x \equiv 1 \ (\bmod\ n) \quad \textit{iff} \quad (\forall\, i \in [1,r])[a^x \equiv 1 \ (\bmod\ p_i^{\alpha_i})],$$

and conversely,

$$a^x \not\equiv 1 \ (\bmod\ n) \quad \textit{iff} \quad (\exists\, i \in [1,r])[a^x \not\equiv 1 \ (\bmod\ p_i^{\alpha_i})].$$

■

Lemma 3.3 *[1] Let p be a prime, α be a positive integer and $p^{\alpha} > 2$, if*

$$x \equiv 1 \ (\bmod\ p^{\alpha}), \quad x \not\equiv 1 \ (\bmod\ p^{\alpha+1})$$

then

$$x^p \equiv 1 \ (\bmod\ p^{\alpha+1}), \quad x^p \not\equiv 1 \ (\bmod\ p^{\alpha+2}).$$

■

Theorem 3.4 *(Generalized Fermat-Euler Theorem[2]-[3]). Let n and a be intergers,*

$$a^{\lambda(n)} \equiv 1 \ \ (\bmod\ n) \ \ \textit{if} \ \ gcd(a,n) = 1,$$

where $\lambda(n)$ denotes Carmicael's function of n. $\lambda(n)$ is the least exponent which holds the equation for any integer a. Then $\lambda(n)$ is called as the universal exponent modulo n or the maximum multiplicative order modulo n. ■

Lemma 3.5 *From Generalized Fermat-Euler Theorem, for integers n, a, b,*

$$a^b \equiv a^{b \bmod \lambda(n)} \ \ (\bmod\ n).$$

■

Theorem 3.6 *(Cardinality of elements with a given order d in $\mathbb{Z}_n^{\times}$[4]). Let $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots (p_1 = 2)$ be a positive integer and let $\psi_n(d)$ be the function for the cardinality of elements with a given order d in $\mathbb{Z}_n^{\times}$ with a*

composite n.

$$\psi_n(d) := \#\{x \in \mathbb{Z}_n^\times : Ord_n(x) = d\},$$

$$= \sum_{\substack{Combinations(d_1, d_2, d_3, \ldots) \\ hold \\ d = lcm(d_1, d_2, d_3, \ldots)}} \prod_i \psi_{p_i^{\alpha_i}}(d_i),$$

where d_i *is a divisor of* $\lambda(p_i^{\alpha_i})$,

$$\psi_{p_1^{\alpha_1}}(d_1) = \psi_{2^{\alpha_1}}(d_1) = \begin{cases} 1 & (d_1 = 1), \\ 1 & (d_1 = 2, \alpha_1 = 2), \\ 3 & (d_1 = 2, \alpha_1 \geq 3), \\ d_1 & (d_1 \geq 4), \end{cases}$$

$$\psi_{p_i^{\alpha_i}}(d_i) = \phi(d_i) \quad (i \geq 2).$$

■

4. Testing of a primitive element

The primitive roots in $\mathbb{Z}_n^\times$ are defined and exist iff $n = 2, 4, p^\alpha, 2p^\alpha$. In Theorem 4.1, Knuth[1] gave the definition of the primitive roots in $\mathbb{Z}_{p^\alpha}^\times$, and showed the necessary and sufficient condition for testing a primitive root in $\mathbb{Z}_{p^\alpha}^\times$.

Theorem 4.1 *(Testing of a primitive root in* $\mathbb{Z}_{p^\alpha}^\times$ *[1]). The integer* g *is a primitive root in* $\mathbb{Z}_{p^\alpha}^\times$ *iff*

(a) for $p^\alpha = 2, g = 1$,
for $p^\alpha = 4, g = 3$,
for $p^\alpha = 8, g = 3, 5, 7$,
for $p^\alpha = 2^{\alpha \geq 4}, g \equiv 3, 5 \pmod 8$,

(b) for an odd prime p *and* $\alpha = 1$, $gcd(g, p) = 1$ *and*

$$(\forall\, q \mid (p-1), q \neq 1)[\, g^{\frac{p-1}{q}} \not\equiv 1 \pmod p],$$

(c) for an odd prime p *and* $\alpha \geq 2$, g *satisfies the condition* (b) *and*

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

■

Here we define the primitive elements in $\mathbb{Z}_n^\times$, which is a generalization of primitive roots, as elements that take the maximum multiplicative order. The definition of the primitive elements in $\mathbb{Z}_n^\times$ is shown in Theorem 4.2.

Theorem 4.2 *(Testing of a primitive element in* $\mathbb{Z}_n^\times$*). The integer* g *is a primitive element in* $\mathbb{Z}_n^\times$ *if* $gcd(g, n) = 1$ *and*

$$(\forall\, q \in Primes, q \mid \lambda(n))[\, g^{\frac{\lambda(n)}{q}} \not\equiv 1 \pmod n].$$

Proof. Obvious since this is the definition. ■

Using Lemma 3.2, we show the following two theorems for reduced testing of a primitive element in $\mathbb{Z}_n^\times$ for any composite n. As an assumption, the prime factorizations: the modulus $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$ $(p_1, p_2, \ldots, p_r \in Primes)$ and the maximum multiplicative order $\lambda(n) = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdots q_s^{\beta_s}$ $(q_1, q_2, \ldots, q_s \in Primes)$ are given.

Theorem 4.3 *(Reduced testing of a primitive element in $\mathbb{Z}_n^\times$). The integer g is a primitive element in $\mathbb{Z}_n^\times$ if $gcd(g,n)=1$ and*

$$(\forall\, j \in [1,s])[\,(\exists\, i \in [1,r])[\, g^{\frac{\lambda(n)}{q_j}} \not\equiv 1 \pmod{p_i^{\alpha_i}})]].$$

Proof. According to Theorem 4.2 and Lemma 3.2, this is obvious. ■

Theorem 4.4 *(More reduced testing of a primitive element in $\mathbb{Z}_n^\times$). The integer g is a primitive element in $\mathbb{Z}_n^\times$ if $gcd(g,n)=1$ and*

$$(\forall\, j \in [1,s])[\,(\exists\, i \in [1,r])[\underline{\, g^{\frac{\lambda(n)}{q_j}} \not\equiv 1 \pmod{p_i^{\alpha_i}})}]],$$

where the underlined condition can be replaced to a reduced form in each case as follows:

(a) for $gcd(q_j, \lambda(p_i^{\alpha_i}))=1$, the condition is 'false',

(b) for $p_i=2, \alpha_i=1$, the condition is 'false',

(c) for $p_i=q_j=2, \alpha_i=2$ and $\beta_j=1$, the condition is replaced to $[\, g \equiv 3 \pmod 4]$,

(d) for $p_i=q_j=2, \alpha_i=2$ and $\beta_j \neq 1$, the condition is 'false',

(e) for $p_i=q_j=2, \alpha_i=3$ and $\beta_j=1$, the condition is replaced to $[\, g \equiv 3,5,7 \pmod 8]$,

(f) for $p_i=q_j=2, \alpha_i=3$ and $\beta_j \neq 1$, the condition is 'false',

(g) for $p_i=q_j=2, \alpha_i \geq 4$ and $\beta_j=\alpha_i-2$, the condition is replaced to $[\, g \equiv 3,5 \pmod 8]$,

(h) for $p_i=q_j=2, \alpha_i \geq 4$ and $\beta_j \neq \alpha_i-2$, the condition is 'false',

(i) for $p_i=q_j>2$ and $\beta_j=\alpha_i-1$, the condition is replaced to $[\, g^{\frac{\lambda(n)}{p_i^{\alpha_i-1}}} \not\equiv 1 \pmod{p_i^2}]$,

(j) for $p_i=q_j>2$ and $\beta_j \neq \alpha_i-1$, the condition is 'false',

(k) for otherwise, the condition is replaced to $[\, g^{\frac{\lambda(n)}{p_i^{\alpha_i-1} q_j}} \not\equiv 1 \pmod{p_i}]$.

In the above β_j and α_i relations in $(d),(f),(h)$ and (j), "$\neq$" can be replaced to "$>$".

Proof.

(a) From $q_j \mid \lambda(n)$, $\lambda(p_i^{\alpha_i}) \mid \lambda(n)$, and the assumption $gcd(q_j, \lambda(p_i^{\alpha_i}))=1$, we take $q_j \lambda(p_i^{\alpha_i}) \mid \lambda(n)$, $\lambda(p_i^{\alpha_i}) \mid \frac{\lambda(n)}{q_j}$, and $\frac{\lambda(n)}{q_j} \mod \lambda(p_i^{\alpha_i}) = 0$, successively. From Lemma 3.5, the l.h.s. of the underlined condition is

$$g^{\frac{\lambda(n)}{q_j}} \equiv g^{\frac{\lambda(n)}{q_j} \bmod \lambda(p_i^{\alpha_i})} \equiv g^0 \equiv 1 \pmod{p_i^{\alpha_i}}.$$

(b) From $\lambda(p_i^{\alpha_i})=\lambda(2)=1$, and the assumptions $p_i^{\alpha_i}=2$ and $gcd(g,n)=1$, we get $gcd(g, p_i^{\alpha_i})=gcd(g,2)=1$. For any integer k,

$$g^k \equiv g^{k \bmod \lambda(2)=1} \equiv g^0 \equiv 1 \pmod 2,$$

$$g^{\frac{\lambda(n)}{q_j}} \equiv g^{\frac{\lambda(n)}{q_j} \bmod 1} \equiv g^0 \equiv 1 \pmod{p_i^{\alpha_i}}.$$

(c) From the assumptions $p_i=q_j=2, \alpha_i=2$ and $\beta_j=1$, $2 \| \lambda(n)$. And then $\frac{\lambda(n)}{2}$ is an odd integer. From $gcd(g,n)=1$, $gcd(g,4)=1$. Thus g is also an odd. If the underlined condition

$$g^{\frac{\lambda(n)}{2}} \not\equiv 1 \pmod 4$$

is satisfied, $g \equiv 3 \pmod 4$.

(d) From $q_j^{\beta_j} \| \lambda(n)$, $2^{\beta_j} \| \lambda(n)$, and the assumptions $p_i = q_j = 2, \alpha_i = 2$ and $\beta_j \geq \alpha_i$, we obtain $2^{\beta_j - 1} \| \frac{\lambda(n)}{2}$, $2^{\alpha_i - 1} \mid \frac{\lambda(n)}{2}$ and $\frac{\lambda(n)}{2} \mod \lambda(2^{\alpha_i}) = \frac{\lambda(n)}{2} \mod 2^{\alpha_i - 1} = 0$, successively. Therefore

$$g^{\frac{\lambda(n)}{2}} \equiv g^{\frac{\lambda(n)}{2} \mod \lambda(2^2)} \equiv g^0 \equiv 1 \pmod{2^2}.$$

(e) From the assumptions $p_i = q_j = 2, \alpha_i = 3$ and $\beta_j = 1$, $2 \| \lambda(n)$. Then $\frac{\lambda(n)}{2}$ is an odd integer. From $gcd(g, n) = gcd(g, 8) = 1$, g is also an odd. If the underlined condition

$$g^{\frac{\lambda(n)}{2}} \not\equiv 1 \pmod 8$$

is satisfied, $g \equiv 3, 5, 7 \pmod 8$.

(f) From $q_j^{\beta_j} \| \lambda(n)$, $2^{\beta_j} \| \lambda(n)$, and the assumptions $p_i = q_j = 2, \alpha_i \geq 3$ and $\beta_j \geq \alpha_i - 1$, we obtain $2^{\beta_j - 1} \| \frac{\lambda(n)}{2}$. Then $2^{\alpha_i - 2} \mid \frac{\lambda(n)}{2}$. Successively, we obtain $\frac{\lambda(n)}{2} \mod \lambda(2^{\alpha_i}) = \frac{\lambda(n)}{2} \mod 2^{\alpha_i - 2} = 0$. Further

$$g^{\frac{\lambda(n)}{2}} \equiv g^{\frac{\lambda(n)}{2} \mod \lambda(2^3)} \equiv g^0 \equiv 1 \pmod{2^3}.$$

(g) From the assumptions $p_i = q_j = 2, \alpha_i \geq 4$ and $\beta_j = \alpha_i - 2$, $2^{\beta_j} \| \lambda(n)$. Then $2^{\alpha_i - 2} \| \lambda(n)$. Thus $\frac{\lambda(n)}{2^{\alpha_i - 2}}$ is an odd integer. From $gcd(g, n) = 1$, $gcd(g, 2^{\alpha_i}) = 1$, g is also an odd. Therefore the underlined condition can be written as

$$g^{\frac{\lambda(n)}{2}} \equiv g^{\frac{k 2^{\alpha_i - 2}}{2}} \equiv g^{k 2^{\alpha_i - 3}} \not\equiv 1 \pmod{2^{\alpha_i}},$$

where $k = \frac{\lambda(n)}{2^{\alpha_i - 2}}$, an odd integer. From Lemma 3.3, this condition is reduced to

$$g^{2k} \not\equiv 1 \pmod{16}.$$

If this condition is satisfied, $g \equiv 3, 5 \pmod 8$.

(h) This is same as (f).

(i) From $q_j^{\beta_j} \| \lambda(n)$, $q_j^{\beta_j - 1} \| \frac{\lambda(n)}{q_j}$, and the assumptions $p_i = q_j > 2$ and $\beta_j = \alpha_i - 1$, $p_i^{\alpha_i - 1} \| \lambda(n)$. We obtain $p_i^{\alpha_i - 2} \| \frac{\lambda(n)}{q_j}$. Let $\frac{\lambda(n)}{q_j} = k p_i^{\alpha_i - 2}$. The underlined condition can be written as

$$g^{\frac{\lambda(n)}{q_j}} \equiv g^{k p_i^{\alpha_i - 2}} \not\equiv 1 \pmod{p_i^{\alpha_i}}.$$

From Lemma 3.3, this condition is reduced to

$$g^k \not\equiv 1 \pmod{p_i^2}, \quad g^{\frac{\lambda(n)}{q_j p_i^{\alpha_i - 2}}} \not\equiv 1 \pmod{p_i^2}, \quad g^{\frac{\lambda(n)}{p_i^{\alpha_i - 1}}} \not\equiv 1 \pmod{p_i^2}.$$

(j) From $q_j^{\beta_j} \mid \lambda(n)$, and the assumptions $p_i = q_j > 2$ and $\beta_j \geq \alpha_i$, $q_j^{\beta_j} \| \lambda(n)$. Then we get $q_j^{\beta_j - 1} \| \frac{\lambda(n)}{q_j}$, $p_i^{\alpha_i - 1} \mid \frac{\lambda(n)}{q_j}$, and $\frac{\lambda(n)}{q_j} \mod \lambda(p_i^{\alpha_i}) = \frac{\lambda(n)}{q_j} \mod p_i^{\alpha_i - 1} = 0$, successively. Therefore

$$g^{\frac{\lambda(n)}{q_j}} \equiv g^{\frac{\lambda(n)}{q_j} \mod \lambda(p_i^{\alpha_i})} \equiv g^0 \equiv 1 \pmod{p_i^{\alpha_i}}.$$

(k) From $q_j \mid \lambda(n)$, $p_i^{\alpha_i - 1} \mid \lambda(n)$, and the assumptions $gcd(q_j, \lambda(p_i^{\alpha_i})) \neq 1$, $p_i \neq q_j$ and both p_i and $q_j > 2$, we take $q_j p_i^{\alpha_i - 1} \mid \lambda(n)$. Let $\lambda(n) = k p_i^{\alpha_i - 1}$. The underlined condition can be written as

$$g^{\frac{\lambda(n)}{q_j}} \equiv g^{\frac{k p_i^{\alpha_i - 1}}{q_j}} \not\equiv 1 \pmod{p_i^{\alpha_i}}.$$

From Lemma 3.3, this condition is reduced to

$$g^{\frac{k}{q_j}} \not\equiv 1 \pmod{p_i}, \quad g^{\frac{k p_i^{\alpha_i - 1}}{q_j p_i^{\alpha_i - 1}}} \not\equiv 1 \pmod{p_i}, \quad g^{\frac{\lambda(n)}{q_j p_i^{\alpha_i - 1}}} \not\equiv 1 \pmod{p_i}.$$

■

5. Conclusion

The primitive roots in $\mathbb{Z}_n^\times$ are defined and exist iff $n = 2, 4, p^\alpha, 2p^\alpha$. In this paper we have defined the primitive elements in $\mathbb{Z}_n^\times$, which is a generalization of primitive roots, as elements that take the maximum multiplicative order.

In the article[4], we have given the function $\psi_n(d)$ for the cardinality of elements with a given order d in $\mathbb{Z}_n^\times$ for any composite n where d is a divisor of the maximum order $\lambda(n)$. Using this function, the function $\psi_n(\lambda(n))$ computes the cardinality of primitive elements in $\mathbb{Z}_n^\times$.

We have concluded that the two theorems 4.3 and 4.4, using a technique of lemma 3.2, for testing a primitive element allow us an effective reduction in testing processes and in computing time cost as a consequence.

Acknowledgements

A preliminary version of this research was first appeared in [5]. The authors would like to thank Prof. Nakamura, Prof. Ikeda, Prof. Jinno, Prof. Mizutani and Prof. Matsui for their constructive comments.

【References】

[1] Donald E. Knuth : *The Art of Computer Programming, vol.2: Seminumerical Algorithms, 2/e,* Addison-Wesley, 1981.

[2] Robert D. Carmichael : "Note on A New Number Theory Function," *Bulltin of the American Mathematical Society*, vol.16, pp.232-238, Feb. 1910.

[3] David Singmaster : "A Maximal Generalization of Fermat's Theorem," *Mathematics Magazine*, vol.39, pp.103-107, 1966.

[4] Hideo Suzuki, Tadao Nakamura : "On the Cardinality of Elements each with a Given Order in $\mathbb{Z}_n^*$," *Technical Report of IEICE on Information Security*, vol.95, no.31, pp.1-6, Dec. 1995.

[5] Hideo Suzuki, Tadao Nakamura, Tetsuo Ikeda : "On the Reduced Recognition of a Primitive Element in $\mathbb{Z}_n^*$," *Technical Report of IEICE on Information Security*, vol.95, no.32, pp.7-12, Dec. 1995.