Honam Mathematical J. **33** (2011), No. 2, pp. 181–186

SEMI-PRIMITIVE ROOT MODULO n

Ki-Suk Lee, Miyeon Kwon, Min Kyung Kang and GiCheol Shin

Abstract. Consider a multiplicative group of integers modulo n, denoted by $\mathbb{Z}_n^*$. Any element $a \in \mathbb{Z}_n^*$ is said to be a semi-primitive root if the order of a modulo n is $\phi(n)/2$, where $\phi(n)$ is the Euler phi-function. In this paper, we classify the multiplicative groups of integers having semi-primitive roots and give interesting properties of such groups.

Given a positive integer n, the integers between 1 and n which are coprime to n form a group with multiplication modulo n as the operation [4]; it is denoted by $\mathbb{Z}_n^*$ and is called the multiplicative group of integers modulo n. For any integer a coprime to n, Euler's theorem states that $a^{\phi(n)} \equiv 1 \bmod n$, where $\phi(n)$ is the Euler phi-function [1], that is, the number of elements in $\mathbb{Z}_n^*$ and a is said to be a primitive root modulo n if the order of a modulo n is equal to $\phi(n)$. It is well known [5] that $\mathbb{Z}_n^*$ has a primitive root, equivalently, $\mathbb{Z}_n^*$ is cyclic if and only if n is equal to 1, 2, 4, p^k, or $2p^k$ where p^k is a power of an odd prime number. This leaves us questions about $\mathbb{Z}_n^*$ that does not possess any primitive roots.

With saying that, the following theorem takes us the first step to answer the questions on noncyclic multiplicative groups $\mathbb{Z}_n^*$.

This lemma is well known [2]: we provides its proof for the reader's convenience.

Lemma 1. $\mathbb{Z}_{2^k}^*$, $k > 2$, *is isomorphic to* $C_2 \times C_{2^{k-2}}$. *Furthermore,*

$$\mathbb{Z}_{2^k}^* = \{\pm 3^i \pmod{n} : i = 0, 1, \cdots, 2^{k-2} - 1\}.$$

Proof. According to the Euler's theorem, the order of any odd integer a modulo 2^k must be a power of 2. We will show that the order of 3 modulo n is 2^{k-2} by evaluating 3^{2^m} modulo 2^k.

Received March 10, 2011. Accepted March 25, 2011.
2000 Mathematics Subject Classification. 11A07, 11A05.
Key words and phrases. Multiplicative group of integers modulo n, primitive roots, semi-primitive roots.

First, note that for a given integer $m > 0$, the Binomial theorem assures us

$$(2+1)^{2^m} + 1 = 2\ell_m \quad \text{for some odd integer } \ell_m. \tag{0.1}$$

By factoring, we get

$$\begin{aligned}(2+1)^{2^m} - 1 &= \big((2+1)^{2^{m-1}} + 1\big)\cdots\big((2+1)^2+1\big)\big((2+1)+1\big)\big((2+1)-1\big)\\ &= \big(2\ell_{m-1}\big)\cdots\big(2\ell_2\big)\big(2^2\big)\big(2\big), \text{ where } \ell_i \text{ is an odd integers}\\ &= 2^{m+2}\ell, \text{ where } \ell \text{ is an odd integer.}\end{aligned}$$

This implies that $3^{2^m} - 1 \equiv 0 \pmod{2^k} \Rightarrow m+2 \geq k$. Therefore, the order of 3 modulo 2^k is 2^{k-2}.

Furthermore, the subgroup $\langle 3\rangle$ of $\mathbb{Z}^*_{2^k}$ generated by 3 does not include -1: If $-1 \in \langle 3\rangle$, $-1 \equiv 3^{2^{k-3}} \pmod{2^k}$, the only element of order 2 in $\langle 3\rangle$. This contradicts to (0.1). Therefore, $\mathbb{Z}^*_{2^k} = \langle -1\rangle \times \langle 3\rangle$. □

Theorem 1. *Let $\mathbb{Z}^*_n$ be the multiplicative group of integers modulo n. If $\mathbb{Z}^*_n$ does not have any primitive root, $a^{\phi(n)/2} \equiv 1$ mod n for any integer a coprime to n.*

Proof. Any integer n greater than 1 can be expressed 2^k, $p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$, or $2^k p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$, where $p_i^{k_i}$ is a power of odd prime numbers.

By the preceding lemma, $\mathbb{Z}_2 \cong C_1$, $\mathbb{Z}_{2^2} \cong C_2$, and $\mathbb{Z}^*_{2^k}$ $(k > 2) \cong C_2 \times C_{2^{k-2}}$. For the other cases, let us recall the Chinese Remainder Theorem [3]:

$$\begin{aligned}\mathbb{Z}^*_n &\cong \mathbb{Z}^*_{2^k} \times \mathbb{Z}^*_{p_1^{k_1}} \times \cdots \times \mathbb{Z}^*_{p_m^{k_m}}\\ &\cong \begin{cases} C_{\phi(p_1^{k_1})} \times \cdots \times C_{\phi(p_m^{k_m})} & \text{if } k = 0 \text{ or } 1;\\ C_2 \times C_{\phi(p_1^{k_1})} \times \cdots \times C_{\phi(p_m^{k_m})} & \text{if } k = 2;\\ C_2 \times C_{2^{k-2}} \times C_{\phi(p_1^{k_1})} \times \cdots \times C_{\phi(p_m^{k_m})} & \text{if } k > 2.\end{cases}\end{aligned}$$

This implies that if $\mathbb{Z}^*_n$ is not cyclic (equivalently $n \neq 2,\ 4,\ p^k,\ 2p^k$), then $\mathbb{Z}^*_n$ is the direct product of two or more cyclic subgroups of even order, say $S_1, S_2, \cdots$. In that case, the order of any $a \in \mathbb{Z}^*_n$ modulo n is a factor of the least common multiple of $|S_1|,\ |S_2|,\ \cdots$ that is equal to $\frac{\phi(n)}{(|S_1|,\ |S_2|,\ \cdots)} = \frac{\phi(n)}{2k}$, for some integer k, where (a, b) is the greatest common divisor of a and b. This completes the proof. □

This motivates the following definition.

Definition 1. *Let $\mathbb{Z}_n^*$ be the multiplicative group of integers modulo n. Any integer a is said to be be a semi-primitive root modulo n if the order of a modulo n is equal to $\phi(n)/2$.*

Clearly, any $\mathbb{Z}_n^*$ possessing a primitive root a have a semi-primitive root a^2 in $\mathbb{Z}_n^*$. If $\mathbb{Z}_n^*$ is a noncyclic group possessing a semi-primitive root, the following holds.

Theorem 2. *Let $\mathbb{Z}_n^*$ be the multiplicative group of integers modulo n that does not possess any primitive root. Then $\mathbb{Z}_n^*$ has a semi-primitive root if and only if n is equal to 2^k $(k > 2)$, $4p_1^{k_1}$, $p_1^{k_1}p_2^{k_2}$, or $2p_1^{k_1}p_2^{k_2}$, where p_1 and p_2 are odd prime numbers satisfying $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$.*

Proof. Suppose that $\mathbb{Z}_n^*$ has a semi-primitive root h. Then there exits an element $a \in \mathbb{Z}_n^*$ of order 2 such that $\mathbb{Z}_n^* = \langle a \rangle \times \langle h \rangle \cong C_2 \times C_{\phi(n)/2}$, where $\langle a \rangle$ and $\langle h \rangle$ are subgroups of $\mathbb{Z}_n^*$ generated by a and h, respectively. Note that such group does not have a subgroup isomorphic to $C_2 \times C_2 \times C_2$. As we saw in the proof of Theorem 1, $\mathbb{Z}_n^* \cong C_2 \times C_{\phi(n)/2}$ must be one of the following cases because the other cases possess a subgroup isomorphic to $C_2 \times C_2 \times C_2$.

$$\begin{array}{lcl}
\mathbb{Z}_{2^k}^* \ (k > 2) & \cong & C_2 \times C_{2^{k-2}}; \\
\mathbb{Z}_{4p_1^{k_1}}^* & \cong & C_2 \times C_{\phi(p_1^{k_1})}; \\
\mathbb{Z}_{p_1^{k_1}p_2^{k_2}}^* & \cong & C_{\phi(p_1^{k_1})} \times C_{\phi(p_2^{k_2})}; \\
\mathbb{Z}_{2p_1^{k_1}p_2^{k_2}}^* & \cong & C_{\phi(p_1^{k_1})} \times C_{\phi(p_2^{k_2})}.
\end{array}$$

For the last two cases, note that the order of any element in $\mathbb{Z}_n^*$ is a factor of the least common multiple of $\phi(p_1^{k_1})$ and $\phi(p_2^{k_2})$, which is equal to $\frac{\phi(n)}{(\phi(p_1^{k_1}),\ \phi(p_2^{k_2}))}$. Recall that $(\phi(p_1^{k_1}),\ \phi(p_2^{k_2})) \geq 2$. This implies that $\mathbb{Z}_{p_1^{k_1}p_2^{k_2}}^*$ and $\mathbb{Z}_{2p_1^{k_1}p_2^{k_2}}^*$ have a semi-primitive root only when $(\phi(p_1^{k_1}),\ \phi(p_2^{k_2})) = 2$. $\square$

In Lemma 1, we saw that $\mathbb{Z}_{2^k}^*$ $(k > 2) = \{\pm 3^i \pmod{n} : i = 0, 1, \cdots, 2^{k-2}-1\}$. The following theorem shows that any $\mathbb{Z}_n^*$ isomorphic to $C_2 \times C_{\phi(n)/2}$ has a similar representation.

Theorem 3. *Suppose $\mathbb{Z}_n^* \cong C_2 \times C_{\phi(n)/2}$. Then there exists a semi-primitive root $h \in \mathbb{Z}_n^*$ so that $\mathbb{Z}_n^* = \{\pm h^i \pmod{n}\ : i = 0, 1, ..., \phi(n)/2 - 1\}$.*

Proof. If $n = 2^k$ $(k > 2)$, it is already shown in Lemma 1. Let us assume that n is equal to $4p_1^{k_1}$, $p_1^{k_1}p_2^{k_2}$, or $2p_1^{k_1}p_2^{k_2}$.

Let h be a semi-primitive root of $\mathbb{Z}_n^*$ and $\langle h \rangle$ be the subgroup of $\mathbb{Z}_n^*$ generated by h. Then $\langle h \rangle$ has only one element of order 2, which is $h^{\phi(n)/4}$.

If $h^{\phi(n)/4} \not\equiv -1 \pmod{n}$, $\langle h \rangle \cap \langle -1 \rangle = \{1\}$ and hence $\langle h \rangle \times \langle -1 \rangle$ is a desired representation for $\mathbb{Z}_n^*$.

If $h^{\phi(n)/4} \equiv -1 \pmod{n}$ and $\mathbb{Z}_n^* = \langle a \rangle \times \langle h \rangle$ for some $a \in \mathbb{Z}_n^*$ of order 2, then we will claim that $\tilde{h} = ah$ is our desired semi-primitive root:

Clearly, the order of $\tilde{h}$ modulo n is equal to the least common multiple of 2 and $\phi(n)/2$, which is $\phi(n)/2$. We only need to make sure that $\langle \tilde{h} \rangle$ does not contain -1. In order to show that $-1 \notin \langle \tilde{h} \rangle$, write $n = m_1 m_2$ so that both $\mathbb{Z}_{m_1}^*$ and $\mathbb{Z}_{m_2}^*$ have primitive roots and $(m_1, m_2) = 1$. For an example, $2p_1^{k_1} p_2^{k_2} = \left(2p_1^{k_1}\right)\left(p_2^{k_2}\right)$. Then the following holds.

$$(0.2)\ h^{\phi(n)/4} \equiv -1 \pmod{n} \quad \Rightarrow \quad \begin{cases} \left(h^{\phi(m_1)/2}\right)^{\phi(m_2)/2} \equiv -1 \pmod{m_1}; \\ \left(h^{\phi(m_2)/2}\right)^{\phi(m_1)/2} \equiv -1 \pmod{m_2} \end{cases}$$

Recall that $\mathbb{Z}_{m_1}^*$ is a cyclic group and $h^{\phi(m_1)} \equiv 1 \pmod{m_1}$ from the Euler's Theorem. Then we have that $h^{\phi(m_1)/2} \equiv -1$ or $1 \pmod{m_1}$. This leads us

$$\left(h^{\phi(m_1)/2}\right)^{\phi(m_2)/2} \equiv -1 \pmod{m_1} \quad \Rightarrow \quad \begin{cases} h^{\phi(m_1)/2} \equiv -1 \pmod{m_1}; \\ \phi(m_2)/2 \text{ is an odd integer.} \end{cases}$$

Similarly,

$$\left(h^{\phi(m_2)/2}\right)^{\phi(m_1)/2} \equiv -1 \pmod{m_2} \quad \Rightarrow \quad \begin{cases} h^{\phi(m_2)/2} \equiv -1 \pmod{m_2}; \\ \phi(m_1)/2 \text{ is an odd integer.} \end{cases}$$

Finally, $h^{\phi(n)/4} \equiv -1 \pmod{n} \ \Rightarrow \phi(n)/4$ is an odd integer.

With that in mind, let us now assume that $-1 \in \langle \tilde{h} \rangle = \langle ah \rangle$. Since $\tilde{h}$ is also a semi-primitive root, $\tilde{h}^{\phi(n)/4} \equiv -1 \pmod{n}$. Meanwhile, putting together the given facts that $a^2 \equiv 1 \pmod{n}$, $h^{\phi(n)/4} \equiv -1 \pmod{n}$, and $\phi(n)/4$ is an odd integer, we have $\tilde{h}^{\phi(n)/4} = (ah)^{\phi(n)/4} \equiv -a \pmod{n}$. This gives that $a \equiv 1 \pmod{n}$, contradicting that the order of a

modulo n is 2. It completes the proof that $\tilde{h} = ah$ is our alternative semi-primitive root for the case of $-1 \in \langle h \rangle$. $\square$

We note immediately that the preceding theorem has the following corollary.

Corollary 1. *Let $\mathbb{Z}_n^*$ be a noncyclic group possessing a semi-primitive root h. Then a is a quadratic residue, i.e. $x^2 \equiv a \pmod{n}$ for some $x \in \mathbb{Z}_n^*$, if and only if a is equivalent to a power of h^2 modulo n. Furthermore, $\mathbb{Z}_n^*$ has exactly $\phi(n)/4$ incongruent quadratic residues.*

References

[1] M. Abramowitz, I. A. Stegunl, *Handbook of Mathematical Functions*, Dover Publication, New York, 1964.

[2] C. F. Gauss; A. A. Clarke (translator into English), *Disquisitiones Arithemeticae*, Springer, New York, 1986.

[3] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1994.

[4] H. E. Rose, *A Course in Number Theory*, Oxford University Press Inc., New York, 1994

[5] J. K. Strayer, *Elementary Number Theory*, Waveland Press, Inc., 2002.

Ki-Suk Lee
Department of Mathematics Education, Korea National University of Education,
Chungwongun, Chungbuk 363-791, Korea.
E-mail: kslee@knue.ac.kr

Miyeon Kwon
Department of Mathematics, University of Wisconsin-Platteville,
Platteville, WI 53818, USA.
E-mail: kwonmi@uwplatt.edu

Min Kyung Kang
Department of Mathematics Education, Korea National University of Education,
Chungwongun, Chungbuk 363-791, Korea.
E-mail: mksgod@nate.com

GiCheol Shin
Department of Mathematics Education, Korea National University of Education,
Chungwongun, Chungbuk 363-791, Korea.
E-mail: math06@blue.knue.ac.kr