Commun. Korean Math. Soc. **28** (2013), No. 1, pp. 71–77
http://dx.doi.org/10.4134/CKMS.2013.28.1.071

MULTIPLICATIVE GROUPS OF INTEGERS WITH SEMI-PRIMITIVE ROOTS MODULO n

Ki-Suk Lee, Miyeon Kwon, 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 discuss some interesting properties of the multiplicative groups of integers possessing semi-primitive roots and give its applications to solving certain congruences.

1. Introduction

Given a positive integer n, the integers between 1 and n that are coprime to n form a group with multiplication modulo n as the operation; 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's totient function (see [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 (see [4], [5], and [6]) 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.

In this paper, we explore noncyclic multiplicative groups of integers. As a first step, we showed in [3] that if there are no primitve roots modulo n, $a^{\phi(n)/2} \equiv 1 \bmod n$ for any integer a coprime to n. This motivates the following definition.

Definition 1. An integer a is said to be a semi-primitive root modulo n if the order of a modulo n is equal to $\phi(n)/2$.

Clearly, if $\mathbb{Z}_n^*$ possesses a primitive root a, there also exists a semi-primitive root in $\mathbb{Z}_n^*$ such as a^2. Furthermore, the following theorem was proved in [3] to give a classification of noncyclic groups possessing semi-primitive roots.

Received May 29, 2012.
2010 *Mathematics Subject Classification.* 11A07.
Key words and phrases. multiplicative groups of integers, primitive roots, semi-primitive roots.

Theorem 1. *Let $\mathbb{Z}_n^*$ be the multiplicative group of integers modulo n that does not possess any primitive roots. 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 $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$.*

In Section 2, we discuss a representation for noncyclic groups possessing semi-primitive roots. Section 3 provides a constructive way of finding semi-primitive roots and the least positive semi-primitive root modulo n for each n less than 100 is given in Table 1. In Section 4, semi-primitive roots will be used to solve certain congruences.

2. The semi-primitive root theorem

It is shown in [2] that 3 is a semi-primitve root modulo 2^k for any integer k greater than 2 and $\mathbb{Z}_{2^k}^*$, $k > 2$ can be represented as

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

In this section, we extend this result to show that any non-cyclic multiplicative group of integers possessing a semi-primitive root has the same representation as $\mathbb{Z}_{2^k}^*$. Throughout the paper, we denote the least common multiple and the great common divisor of two integers m and n by $[m,\ n]$ and $(m,\ n)$, respectively.

Theorem 2 is also shown in [3]. Here we give a simpler proof.

Theorem 2. *Suppose $\mathbb{Z}_n^* \cong C_2 \times C_{\phi(n)/2}$. Then there exists a semi-primitive root $h \in \mathbb{Z}_n^*$ such that*

$$\mathbb{Z}_n^* = \Big\{ \pm h^i \mod\ n\ :\ i = 1, \dots, \frac{\phi(n)}{2} \Big\}.$$

Proof. 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. If $-1 \notin \langle h \rangle$, then $\langle h \rangle \cap \langle -1 \rangle = \{1\}$ and therefore $\langle h \rangle \times \langle -1 \rangle$ is a desired representation for $\mathbb{Z}_n^*$.

Let us now assume that $\mathbb{Z}_n^* = \langle a \rangle \times \langle h \rangle$ for some $a \in \mathbb{Z}_n^*$ of order 2 and $-1 \in \langle h \rangle$. Then $2 \mid \frac{\phi(n)}{2}$ and $\langle h \rangle = \langle h^2 \rangle \times \langle -1 \rangle \cong C_{\phi(n)/4} \times C_2$, where $\big(\frac{\phi(n)}{4},\ 2\big) = 1$; otherwise $C_{\phi(n)/4} \times C_2$ cannot be cyclic. Putting together, we conclude that $\mathbb{Z}_n^* = \langle a \rangle \times \langle h^2 \rangle \times \langle -1 \rangle = \langle ah^2 \rangle \times \langle -1 \rangle$. □

For the purpose of differentiation, any semi-primitive root h in $\mathbb{Z}_n^*$ is said to be a good semi-primitve (GSP) root if $\mathbb{Z}_n^*$ can be expressed as

$$\mathbb{Z}_n^* = \langle h \rangle \times \langle -1 \rangle.$$

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

Corollary 1. *Suppose that $\mathbb{Z}_n^*$ is a noncyclic group possessing semi-primitive roots. Then $\mathbb{Z}_n^*$ has exactly $2\phi(\frac{\phi(n)}{2})$ incongruent GSP roots.*

Proof. According to Theorem 2, $\mathbb{Z}_n^* = \big\langle h\big\rangle \times \big\langle -1\big\rangle$ for a semi-primitve root $h \in \mathbb{Z}_n^*$. In other words, any element $a \in \mathbb{Z}_n^*$ can be expressed $a = h^i$ or $-h^i$, where $i = 1, 2, \dots, \phi(n)/2$.

For the case of $a = h^i$, $ord_n(h^i) = \frac{ord_n(h)}{\big(ord_n(h),\ i\big)} = \frac{\phi(n)/2}{\big(\phi(n)/2,\ i\big)}$, where $ord_n(a)$ indicates the order of a modulo n. This implies that

$$ord_n(h^i) = \frac{\phi(n)}{2} \iff \left(\frac{\phi(n)}{2},\ i\right) = 1.$$

Since h is a GPS root modulo n, it is also clear that $(h^i)^j \neq -1$ for all integers j. Therefore we can say that there are $\phi(\frac{\phi(n)}{2})$ incongruent GSP roots in $\mathbb{Z}_n^*$ in the form of h^i.

Now we will show that there are also $\phi(\frac{\phi(n)}{2})$ incongruent GPS roots modulo n in the form of $-h^i$. More precisely, $-h^i$ is a GSP root modulo n if and only if $(\frac{\phi(n)}{2},\ i) = 1$. We first note that

$$ord_n(-h^i) = [2, ord_n(h^i)] = \frac{2\ ord_n(h^i)}{(2,\ ord_n(h^i))} = \frac{\phi(n)}{\Big(\frac{\phi(n)}{2},\ i\Big)\Big(2,\ \frac{\phi(n)/2}{(\phi(n)/2,\ i)}\Big)}.$$

Then $ord_n(-h^i) = \frac{\phi(n)}{2}$ if and only if $\big(\frac{\phi(n)}{2},\ i\big)(2,\ \frac{\phi(n)/2}{\big(\phi(n)/2,\ i\big)}) = 2$. In other words,

$$ord_n(-h^i) = \frac{\phi(n)}{2} \iff \begin{array}{llll} (1) & \big(\frac{\phi(n)}{2},\ i\big) = 1 & \text{and} & \big(2,\ \frac{\phi(n)}{2}\big) = 2 \quad \text{or} \\ (2) & \big(\frac{\phi(n)}{2},\ i\big) = 2 & \text{and} & \big(2,\ \frac{\phi(n)}{4}\big) = 1. \end{array}$$

Since $\frac{\phi(n)}{2}$ is even for the cases under our consideration, the first case is simply $\big(\frac{\phi(n)}{2},\ i\big) = 1$. If $(\frac{\phi(n)}{2},\ i) = 1$, $(-h^i)^j \not\equiv -1$ for all integers j: Suppose that $(\frac{\phi(n)}{2},\ i) = 1$ and $(-h^i)^j \equiv -1$ for an integer j. Then j must be an odd integer since h is a GPS root modulo n, which gives us $h^{ij} \equiv 1$, equivalently $\frac{\phi(n)}{2} \mid ij$. Since $(\frac{\phi(n)}{2},\ i) = 1$, we end up with $\frac{\phi(n)}{2} \mid j$ and so j is an even integer since $\frac{\phi(n)}{2}$ is even, leading a contradicton.

For the second case, if $\big(\frac{\phi(n)}{2},\ i\big) = 2$ and $\big(2,\ \frac{\phi(n)}{4}\big) = 1$, $\frac{\phi(n)}{4}$ is an odd integer and i is an even integer. Then $\big(-h^i\big)^{\frac{\phi(n)}{4}} = (-1)\big(h^{\frac{\phi(n)}{2}}\big)^{\frac{i}{2}} \equiv -1 \mod n$, which means that any semi-primitive root modulo n in the second case is not a GSP. This completes the proof that $-h^i$ is a GSP root modulo n if and only if $(\frac{\phi(n)}{2},\ i) = 1$. □

In fact, the proof of Corollary 1 shows us that if $\mathbb{Z}_n^*$ is a noncyclic group possessing semi-primitive roots and $\phi(n)/4$ is an odd intger, then $\mathbb{Z}_n^*$ has $\phi(\frac{\phi(n)}{4})$ more semi-primitive roots in addition to $2\phi(\frac{\phi(n)}{2})$ GSP roots.

3. Finding GSP roots modulo n

While Section 2 is about the existence of GPS roots in a certain class of multiplicative groups of integers, a constructive way of finding a GPS root is given in this section.

Theorem 3. *Let m_1 and m_2 be coprime integers possessing primitive roots a and b, respectively. If $(\phi(m_1), \phi(m_2)) = 2$, there exist semi-primitive roots modulo $n = m_1 m_2$ and the solution to the system of linear congruences*

$$\begin{aligned} x &\equiv a \mod m_1 \\ x &\equiv -b \mod m_2 \end{aligned} \tag{1}$$

is a GSP root modulo n.

Proof. Chinese Remainder theorem ensures us that the system in (1) has a unique solution modulo n, say x_0. Then the fact that a and b are primitive roots and $(m_1, m_2) = 1$ takes us to

$$x_0^{[\phi(m_1),\phi(m_2)]} \equiv 1 \mod n.$$

Suppose $x_0^k \equiv 1 \bmod n$, equivalently $a^k \equiv 1 \mod m_1$ and $(-b)^k \equiv 1 \bmod m_2$. Since a is a primitive root modulo m_1, $\phi(m_1) \mid k$ and, applying $(\phi(m_1), \phi(m_2))=$ 2, we get that k is an even integer. Then $(-b)^k = b^k \equiv 1 \bmod m_2$, equivalently $\phi(m_2) \mid k$. Therefore

$$ord_n(x_0) = [\phi(m_1), \phi(m_2)] = \frac{\phi(m_1)\phi(m_2)}{2} = \frac{\phi(n)}{2}.$$

This concludes that x_0 is a semi-primitive root modulo n. What remains is to show that $x_0^{\phi(n)/4} \not\equiv -1 \bmod n$ and hence x_0 is a GSP root modulo n.
Assume that $x_0^{\phi(n)/4} \equiv -1 \bmod m_1 m_2$. Then, the first congruence $x \equiv a \mod m_1$ gives

$$-1 \equiv (a^{\frac{\phi(m_1)}{2}})^{\frac{\phi(m_2)}{2}} \equiv (-1)^{\frac{\phi(m_2)}{2}} \bmod m_1$$

and therefore $\frac{\phi(m_2)}{2}$ is an odd integer. In the meantime, the second congruence $x \equiv -b \mod m_2$ gives

$$-1 \equiv ((-1)^{\frac{\phi(m_2)}{2}})^{\frac{\phi(m_1)}{2}} (b^{\frac{\phi(m_2)}{2}})^{\frac{\phi(m_1)}{2}} \equiv (-1)^{\frac{\phi(m_1)}{2}} (-1)^{\frac{\phi(m_1)}{2}} \equiv 1 \bmod m_2,$$

which is a contradiction. □

We now provide an example that illustrates the calculation procedure claimed in Theorem 3.

Example 1. Find all GSP roots modulo 93.

Solution. According to Corollary 1 and Theorem 3, there are $2\phi(30)$ incongruent GSP roots modulo 93 and the solution for the system of congruences

$$\begin{aligned} x &\equiv 3 \mod 31 \\ x &\equiv -2 \mod 3 \end{aligned}$$

is a GSP root modulo 93. The solution of the system is $x \equiv 34 \bmod 93$ (See [6] for solving the system of linear congruences) and hence GSP roots modulo 93 are $\pm 34^i$ for positive integers i coprime to 30.

For the reader's convenience, the least primitive root and the least GSP root modulo n for each integer $n \leq 100$ are given in Table 1.

TABLE 1. Least primitive root and GSP root modulo n

n	P	GSP	n	P	GSP	n	P	GSP	n	P	GSP
1	1		26	7		51		5	76		13
2	1		27	2	4	52		7	77		2
3	2	1	28		5	53	2		78		7
4	3	1	29	2		54	5	7	79	3	2
5	2		30		7	55		2	80		
6	5	1	31	3	7	56			81	2	4
7	3	2	32		3	57		5	82	7	
8		3	33		5	58	3		83	2	3
9	2	4	34	3		59	2	3	84		
10	3		35		2	60			85		
11	2	3	36		5	61	2		86	3	9
12		5	37	2		62	3	7	87		2
13	2		38	3	5	63			88		
14	3	9	39		2	64		3	89	3	
15		2	40			65			90		7
16		3	41	6		66		5	91		
17	3		42		11	67	2	4	92		3
18	5	7	43	3	9	68		3	93		13
19	2	4	44		3	69		2	94	5	3
20		3	45		2	70		3	95		2
21		2	46	5	3	71	7	2	96		
22	7	3	47	5	2	72			97	5	
23	5	2	48			73	5		98	3	9
24			49	3	2	74	5		99		5
25	2		50	3		75		2	100		3

4. GSP roots and congruences

This section gives an application of GSP roots to the solution of certain congruences. We illustrate the solution procedure with concrete examples.

Example 2. Find all incongruent solutions of the congruence $x^4 \equiv 4 \bmod 7$.

For comparison, we give two solutions with one using a primitive root and the other using a semi-primitive root.

Solution. (Using a primitive root 3 modulo 7)
Write $x \equiv 3^i$, where $1 \le i \le \phi(7) = 6$. Since $4 \equiv 3^4$ mod 7, we have

$$4i \equiv 4 \mod 6 \Rightarrow \; 2i \equiv 2 \mod 3 \Rightarrow i \equiv 1 \mod 3.$$

Therefore, there are two incongruent solutions: $x \equiv 3$ or $x \equiv 3^4 \equiv 4$ mod 7.

Solution. (Using a GSP root 2 modulo 7)
Write $x \equiv \pm 2^i$, where $1 \le i \le \phi(7)/2 = 3$. Since $4 \equiv 2^2$ mod 7, we have

$$4i \equiv 2 \mod 3 \Rightarrow \; i \equiv 2 \mod 3.$$

So there are two incongruent solutions: $x \equiv 2^2 \equiv 4$ or $x \equiv -2^2 \equiv 3$ mod 7.

In Example 2, we do not see any advantage of using semi-primitive roots as opposed to using primitive roots. However, it becomes beneficial in the case where there are no primitive roots modulo n as shown in the next example.

Example 3. Find all incongruent solutions of the congruence $x^3 \equiv 20$ mod 21.

Solution. (Using primitive roots 2 modulo 3 and 3 modulo 7)
Clearly,

$$x^3 \equiv 20 \mod 21 \quad \Longleftrightarrow \quad \begin{cases} x^3 \equiv 20 \; \equiv 2 \mod 3 \\ x^3 \equiv 20 \; \equiv 6 \mod 7. \end{cases}$$

For $x^3 \equiv 2$ mod 3, write $x \equiv 2^i$, where $1 \le i \le \phi(3) = 2$. We then have

$$3i \equiv 1 \mod 2 \Rightarrow \; i \equiv 1 \mod 2 \Rightarrow x \equiv 2 \mod 3.$$

For $x^3 \equiv 6$ mod 7, write $x \equiv 3^j$, where $1 \le j \le \phi(7) = 6$. Since $6 \equiv 3^3$ mod 7,

$$3j \equiv 3 \mod 6 \Rightarrow \; j \equiv 1 \mod 2 \Rightarrow x \equiv 3^1, \; 3^3, \; \text{or } 3^5 \mod 7.$$

By solving the following three systems of congruences, we finally get three incongruent solutions for $x^3 \equiv 20$ mod 21 that are 5, 17, or 20.

$$\begin{array}{lll} x \equiv \; 2 \mod 3 \;\&\; x \equiv 3 \mod 7 & \Rightarrow & x \equiv 17 \mod 21 \\ x \equiv \; 2 \mod 3 \;\&\; x \equiv 6 \mod 7 & \Rightarrow & x \equiv 20 \mod 21 \\ x \equiv \; 2 \mod 3 \;\&\; x \equiv 5 \mod 7 & \Rightarrow & x \equiv 5 \mod 21. \end{array}$$

The next solution uses a GSP root modulo 21. It gets rid of dealing with several systems of congruences that we have seen in the previous solution.

Solution. (Using a GSP root 2 modulo 21)
Note that $x^3 \equiv 20 \equiv -1$ mod 21. Since 2 is a good semi-primitive root (see Table 1), any element $x \in \mathbb{Z}_{21}^*$ can be written in the form $x \equiv \pm 2^i$ mod 21, for an integer i, and clearly there are no solutions to the congruence in the form of 2^i. Therefore, without loss of generality, we can write $x \equiv -2^i$ modulo 21, where $1 \le i \le \phi(21)/2 = 6$ and have

$$3i \equiv 0 \mod 6 \Rightarrow \; i \equiv 0 \mod 2 \Rightarrow i = 2, \; 4, \; 6 \Rightarrow x \equiv -2^2, \; -2^4, \; -2^6 \mod 21.$$

So there are three incongruent solutions for $x^3 \equiv 20 \bmod 21$ that are -2^2, -2^4, or -2^6: equivalently, 5, 17, or 20.

References

[1] M. Abramowitz and I. A. Stegunl, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, National Bureau of Standards Applied Mathematics Series, 55. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 1964.

[2] C. F. Gauss and A. A. Clarke, *Disquisitiones Arithemeticae*, Springer, New York, 1986.

[3] K. Lee, M. Kwon, M. K. Kang, and G. Shin, *Semi-primitive root modulo n*, Honam Math. J. **33** (2011), no. 2, 181–186.

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

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

[6] 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 address: kslee@knue.ac.kr

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

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