On the number of semi-primitive roots modulo \( n \)

Pinkimani Goswami\(^1\) and Madan Mohan Singh\(^2\)

\(^1\) Department of Mathematics, North-Eastern Hill University  
Permanent Campus, Shillong–793022, Meghalaya, India  
e-mail: pinkimanigoswami@yahoo.com

\(^2\) Department of Basic Sciences and Social Sciences, North-Eastern Hill University  
Permanent Campus, Shillong–793022, Meghalaya, India  
e-mail: mmsingh2004@gmail.com

Abstract: Consider the multiplicative group of integers modulo \( n \), denoted by \( \mathbb{Z}^*_n \). An element \( a \in \mathbb{Z}^*_n \) is said to be a semi-primitive root modulo \( n \) if the order of \( a \) is \( \phi(n)/2 \), where \( \phi(n) \) is the Euler’s phi-function. In this paper, we’ll discuss on the number of semi-primitive roots of non-cyclic group \( \mathbb{Z}^*_n \) and study the relation between \( S(n) \) and \( K(n) \), where \( S(n) \) is the set of all semi-primitive roots of non-cyclic group \( \mathbb{Z}^*_n \) and \( K(n) \) is the set of all quadratic non-residues modulo \( n \).

Keywords: Multiplicative group of integers modulo \( n \), Primitive roots, Semi-primitive roots, Quadratic non-residues, Fermat primes.

AMS Classification: 11A07.

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 \( n \). The order of this group is \( \phi(n) \), where \( \phi(n) \) is the Euler’s phi-function.

For any \( a \in \mathbb{Z}^*_n \), the order of \( a \) is the smallest positive integer \( k \) such that \( a^k \equiv 1 \pmod{n} \). Now, \( a \) is said to be a primitive root modulo \( n \) (in short primitive root) if the order of \( a \) is equal to \( \phi(n) \). It is well known 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 \( p \) is an odd prime number and \( k \geq 1 \). In this connection, it is interesting to study \( \mathbb{Z}^*_n \) that does not possess any primitive roots.

As a first step the authors in [1] showed that if \( \mathbb{Z}^*_n \) does not possess primitive roots, then \( a^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n} \) for any integer \( a \in \mathbb{Z}^*_n \). This motivate the following definition:
Definition 1.1. An element $a \in \mathbb{Z}_n^*$ is said to be a semi-primitive root modulo $n$ (in short semi-primitive root) if the order of $a$ is equal to $\phi(n)/2$.

Clearly, if $a \in \mathbb{Z}_n^*$ is a primitive root, then $a^2 \in \mathbb{Z}_n^*$ is a semi-primitive root. In the same paper they classified the non-cyclic groups of the form $\mathbb{Z}_n^*$ possessing semi-primitive roots as follows:

Theorem 1.1. Let $\mathbb{Z}_n^*$ be the multiplicative group of integer 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 $2^k(k > 2)$, $4p_1^{k_1}p_2^{k_2}$, or $2p_1^{k_1}p_2^{k_2}$, where $p_1$ and $p_2$ are odd primes satisfying $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$ and $k_1, k_2 \geq 1$.

In [2], the authors introduced the notion of good semi-primitive (GSP) root modulo $n$. A semi-primitive root $h$ in $\mathbb{Z}_n^*$ is said to be a GSP root if $\mathbb{Z}_n^*$ can be expressed as $\mathbb{Z}_n^* = \langle h \rangle \times \langle -1 \rangle$.

They showed that if $\mathbb{Z}_n^*$ is a non-cyclic group possessing semi-primitive roots then $\mathbb{Z}_n^*$ has exactly $2\phi\left(\frac{\phi(n)}{2}\right)$ (i.e., $\phi(\phi(n))$) incongruent GSP roots. From paper [2] it is clear that the number of semi-primitive root is either $\phi(\phi(n))$ or $\phi(\phi(n)) + \phi\left(\frac{\phi(n)}{4}\right)$ according as $\frac{\phi(n)}{4}$ is even or odd.

In the rest of this paper $\mathbb{Z}_n^*$ is considered as a non-cyclic group possessing semi-primitive root i.e., $n$ is equal to $2^k(k > 2)$, $4p_1^{k_1}p_2^{k_2}$, or $2p_1^{k_1}p_2^{k_2}$, where $p_1$ and $p_2$ are odd primes satisfying $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$ and $k_1, k_2 \geq 1$.

This paper is organized as follows. Section 2 is devoted to the number of semi-primitive roots of $\mathbb{Z}_n^*$ and in section 3 we discuss the relation between set of all semi-primitive roots of $\mathbb{Z}_n^*$ and set of all quadratic non-residues modulo $n$. Throughout the paper all notations are usual. For example the greatest common divisor of two integers $m$ and $n$ is denoted by $(m, n)$, the order of $a$ modulo $n$ is denoted by $\text{ord}_n(a)$ etc.

2 New results on number of semi-primitive roots

In this section we dealing with number of semi-primitive roots for different values of $n$. For positive values of $n$, we define

$$S(n) = \{ g \in \mathbb{Z}_n^* | g \text{ is a semi primitive root modulo } n \}$$

So

$$|S(n)| = \begin{cases} \phi(\phi(n)) + \phi\left(\frac{2\phi(n)}{4}\right), & \text{if } \frac{\phi(n)}{4} \text{ is odd} \\ \phi(\phi(n)), & \text{if } \frac{2\phi(n)}{4} \text{ is even} \end{cases}$$

Where cardinality of $S(n)$ is denoted by $|S(n)|$.

We begin with the following proposition which shows that the number of semi-primitive roots is always greater than 2.

Proposition 2.1. Let $\mathbb{Z}_n^*$ be a non-cyclic group possessing a semi-primitive root. Then the number of semi-primitive roots is at least 3.
Proposition 2.4. Let \( p \) be an odd prime be the number of semi-primitive roots. Then the number of semi-primitive roots is always an even number except for \( 12 \) or \( 3 \) or \( 6 \) or \( 8 \) or \( 10 \). The number of semi-primitive roots is given by \( \frac{\phi(n)}{4} \).

Proof. The number of semi-primitive roots is given by \( \phi(\phi(n)) + \phi(\frac{\phi(n)}{4}) \) or \( \phi(\phi(n)) \) according as \( \frac{\phi(n)}{4} \) is odd or even. As \( \phi(n) > 2 \), so \( \phi(\phi(n)) \) is even. Therefore number of semi-primitive roots is greater than 1.

Consider the smallest possible case \( \phi(\phi(n)) = 2 \). Then \( \phi(n) = 3, 4 \) or 6. The only possibility is \( \phi(n) = 4 \), which implies that \( \frac{\phi(n)}{4} \) is odd. So the number of semi-primitive roots is greater than 2. \( \square \)

The following proposition gives the necessary and sufficient condition for which \( |S(n)| = 3 \).

Proposition 2.2. Let \( \mathbb{Z}_n^* \) be a non-cyclic group possessing a semi-primitive root. Then \( \mathbb{Z}_n^* \) has exactly 3 semi-primitive roots iff \( n = 2^3 \text{ or } 12 \).

Proof. The number of semi-primitive roots is given by \( \phi(\phi(n)) + \phi\left(\frac{\phi(n)}{4}\right) \) or \( \phi(\phi(n)) \) according as \( \frac{\phi(n)}{4} \) is odd or even. As \( \phi(n) > 2 \), so \( \phi(\phi(n)) \) is even. Therefore \( \phi(\phi(n)) + \phi\left(\frac{\phi(n)}{4}\right) = 3 \), which implies \( \frac{\phi(n)}{4} \) is odd. The only possibility of \( \phi\left(\frac{\phi(n)}{4}\right) \) is 1, which implies \( \phi(n) = 4 \). So \( n = 5, 8, 10 \) or 12. But \( n \neq 5, 10 \) as they are not any of the above form. So \( n = 8 \) or 12. \( \square \)

In the following proposition we showed that number of semi-primitive roots is always an even number for \( n = 2^4, 12 \).

Proposition 2.3. Let \( \mathbb{Z}_n^* \) be a non-cyclic group possessing a semi-primitive root. Then the number of semi-primitive roots is always an even number except for \( n = 2^3, 12 \).

Proof. Suppose there exist an integer \( n(n \neq 2^3, 12) \), for which number of semi-primitive roots is an odd number (say \( m \)). Since number of semi-primitive roots is odd, so \( \frac{\phi(n)}{4} \) is odd. Now \( \phi(\phi(n)) + \phi\left(\frac{\phi(n)}{4}\right) = m \), so the only possibility is \( \phi\left(\frac{\phi(n)}{4}\right) = 1 \), which implies \( \phi(n) = 4 \). Therefore \( n = 2^3 \text{ or } 12 \), which is a contradiction. \( \square \)

The following proposition is dealing with the number of semi-primitive roots of the form \( 2p \), where \( p \) is odd prime.

Proposition 2.4. Let \( \mathbb{Z}_n^* \) be a non-cyclic group possessing a semi-primitive root. Let \( 2p \), where \( p \) is an odd prime be the number of semi-primitive roots. Then \( p = 3 \text{ and } n = 21, 28 \text{ or } 42 \).

Proof. Suppose \( \frac{\phi(n)}{4} \) is even. For \( p = 3 \), \( \phi(n) = 7, 9, 14 \), or 18, which is not possible. For \( p \geq 5 \), \( \phi(n) = 2p + 1 \), or \( 4p + 2 \) (where \( 2p + 1 \) is prime). Both are not possible. Therefore if \( |S(n)| = 2p \) then \( \frac{\phi(n)}{4} \) must be odd.

Obviously \( n \neq 2^k(k \geq 3) \) as in this case number of semi-primitive roots is 3.

Case (i) Suppose \( n = 4p_1^{k_1} \), where \( p_1 \) is an odd prime and \( k_1 \geq 1 \). As \( p_1 \) is odd prime so \( \phi(p_1) = 2^{k_1-1}q_1 \), where \( l_1 \geq 1 \) and \( q_1 \geq 1 \) is an odd number. If \( k_1 = 1 \) then \( \phi(n) = 2^{l_1+1}q_1 \) and so \( l_1 = 1 \). Therefore \( |S(n)| = 3q_1 \), which implies \( p = 3 \) and \( q_1 = 3 \). So \( n = 28 \).

If \( k_1 > 1 \) then \( \phi(n) = 2^{l_1+1}q_1p_1^{k_1-1} \) and \( l_1 = 1 \). Then \( |S(n)| = 6q_1\phi(q_1)p_1^{k_1-2} \) and therefore \( p = 3q_1\phi(q_1)p_1^{k_1-2} \), which is not possible.

Case (ii) When \( n = p_1^{k_1}p_2^{k_2} \), where \( p_1 \) and \( p_2 \) are odd prime such that \( \phi(p_1^{k_1}), \phi(p_2^{k_2}) = 2 \) and \( k_1, k_2 \geq 1 \). As \( p_1 \) and \( p_2 \) are odd prime so \( \phi(p_1) = 2^{k_1}q_1 \) and \( \phi(p_2) = 2^{k_2}q_2 \) where \( l_1, l_2 \geq 1 \) and
\[ q_1 \geq 1, q_2 \geq 1 \text{ are odd numbers such that } (\phi(q_1), \phi(q_2)) = 1. \text{ As } (\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2 \text{ so at least } l_1 \text{ or } l_2 \text{ is equal to } 1. \text{ Without loss of generality we can assume that } l_1 = 1. \]

If \( k_1 = 1 = k_2 \) then \( \phi(n) = 2^{2l+1}q_1q_2 \) and \( l_2 = 1. \) Therefore \( |S(n)| = 3\phi(q_1)\phi(q_2) \Rightarrow 3\phi(q_1)\phi(q_2) = 2p \Rightarrow p = 3 \text{ an either } \phi(q_1) = 1, \phi(q_2) = 2, \text{ or } \phi(q_1) = 2, \phi(q_2) = 1. \text{ So, } p = 3 \text{ and either } q_1 = 1 \text{ and } q_2 = 3 \text{ or } q_1 = 3 \text{ and } q_2 = 1. \text{ And hence } p = 3 \text{ and } n = 21. \]

If \( k_1 = 1, k_2 > 1 \) then \( \phi(n) = 2^{2l+1}q_1q_2p_2^{k_2-1} \) and \( l_2 = 1. \) Then \( |S(n)| = 6q_2\phi(q_1)\phi(q_2)p_2^{k_2-2} = 2p \) and therefore \( 3q_2\phi(q_1)\phi(q_2)p_2^{k_2-2} = p, \) which is not possible. Similarly for \( k_1 > 1, k_2 = 1. \)

If \( k_1 > 1 \text{ and } k_2 > 1 \) then \( p_1 \) and \( p_2 \) are factors of \( |S(n)|, \) so \( |S(n)| \neq 2p. \)

As \( \phi(p_1^{k_1}p_2^{k_2}) = \phi(2p_1^{k_1}p_2^{k_2}) \) so \( |S(n)| = 2p \) if \( p = 3 \) and \( n = 42. \)

Hence from the above cases we can say that if the number of semi-primitive roots is \( 2p \) then \( p = 3 \) and \( n = 21, 28, \text{ or } 42. \)

\[ \square \]

**Note:** It is easy to see that if \( \mathbb{Z}_n^* \) is a non-cyclic group possessing semi-primitive root and if number of semi-primitive roots is of the form \( 2^k p, \) where \( p \) is an odd prime then for \( \frac{\phi(n)}{4} \) is even, \( 0 \leq k \leq 31 \) and \( p = 3. \) It is clear that the number of semi-primitive roots for \( n = 2^k (k > 3) \) is in power of 2. So it is interesting to find the other form of \( n \) for which number of semi-primitive roots is in power of 2.

In this direction we have the following propositions.

**Proposition 2.5.** Let \( \mathbb{Z}_n^* \) be a non-cyclic group possessing a semi-primitive root. Then for \( n = 4p_1^{k_1}, \) where \( p_1 \) is an odd prime and \( k_1 \geq 1 \) has number of semi-primitive roots is in power of 2 (say \( 2^m, \ m \geq 2 \)) iff \( k_1 = 1 \) and either \( p_1 \neq 3 \) is a Fermat prime or \( p_1 \) is a prime of the form \( 2^k q + 1 \) where \( l > 1 \) and \( q \) is the product of Fermat primes.

**Proof.** It is easy to see that if \( k_1 = 1 \) and if \( p_1 \) satisfied any of the above conditions then the number of semi-primitive roots is always in power of 2.

Conversely, let the number of semi-primitive roots be \( 2^m \) \( (m \geq 2) \). There will be two cases to be consider for \( n = 4p_1^{k_1}. \) If \( k_1 > 1 \) then \( p_1 \) is a factor of number of semi-primitive roots, which is not possible. So \( k_1 = 1. \) Also, as \( p_1 \) is odd prime so \( \phi(p_1) = 2^l q, \) where \( q \geq 1 \) is odd number and \( l \geq 1. \) Therefore \( \phi(n) = 2^{l+1}q \) for \( n = 4p_1 \) and

\[
\frac{\phi(n)}{4} = 2^{l-1}q = \begin{cases} 
\text{odd, if } l = 1 \\
\text{even, otherwise}
\end{cases}
\]

When \( \frac{\phi(n)}{4} \) is odd then \( |S(n)| = 3\phi(q), \) which is not power of 2. When \( \frac{\phi(n)}{4} \) is even, then \( |S(n)| = 2^l \phi(q) \) which implies that \( 2^l \phi(q) = 2^m, \) so either \( \phi(q) = 1 \) or \( \phi(q) \) is power of 2 (say \( 2^a, \ a \geq 1 \)). If \( \phi(q) = 1 \) then \( q = 1 \) and so \( p_1 = 2^l + 1(l > 1). \) Since \( p_1 \) is prime so \( 2^l + 1 \) is also prime, which is possible only when \( l \) is power of 2 i.e. \( 2^l + 1(l > 1) \) is Fermat prime. So \( p_1 (\neq 3) \) is Fermat prime. Suppose \( \phi(q) = 2^a, \ a \geq 1. \) The equation \( \phi(q) = 2^a \) have one odd solution \( q \) iff \( a \leq 31. \) The solution \( q \) is the product of the Fermat primes. So \( p_1 = 2^l q + 1, l > 1, \) where \( q \) is the product of Fermat primes. Hence complete the proved. \[ \square \]
Proposition 2.6. Let $Z_n^*$ be a non-cyclic group possessing a semi-primitive root. Then for $n = p_1^{k_1}p_2^{k_2}$, where $k_1, k_2 \geq 1$ and $p_1, p_2$ are odd primes such that $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$ has number of semi-primitive roots is in power of $2$ (say $2^m$, $m \geq 2$) iff $k_1 = 1 = k_2$ and either any one of $p_1$ and $p_2$ is equal to $3$ or $2q + 1$ where $q$ is the product of Fermat primes and other is of the form $2^lq + 1$ where $l > 1$ and either $q = 1$ or $q$ is the product of Fermat primes.

Proof. It is easy to see that if $p_1$ and $p_2$ satisfied all the above condition then the number of semi-primitive roots is always power of $2$.

Conversely, suppose $n = p_1^{k_1}p_2^{k_2}$, where $p_1, p_2$ are prime such that $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$ and $k_1, k_2 \geq 1$ and let $|S(n)| = 2^m(m \geq 2)$. Since $p_1$ and $p_2$ are odd prime so $\phi(p_1) = 2^{l_1}q_1$ and $\phi(p_2) = 2^{l_2}q_2$ where $q_1, q_2 \geq 1$ are odd numbers and $l_1, l_2 \geq 1$. As $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$, so at least $l_1$ or $l_2$ is equal to $1$ (say $l_1 = 1$) and $(\phi(q_1), \phi(q_2)) = 1$. If $k_1$ or $k_2$ or both greater than $1$ then $p_1$ or $p_2$ or both are the factor(s) of $|S(n)|$, which is not possible. So the only possibility is that $k_1 = 1 = k_2$. Then $\phi(n) = 2^{l_2 - 1}q_1q_2$ and

$$\frac{\phi(n)}{4} = 2^{l_2 - 1}q_1q_2 = \begin{cases} \text{odd, if } l_2 = 1 \\
\text{even, otherwise} \end{cases}$$

When $\frac{\phi(n)}{4}$ is odd, then $|S(n)| = 3\phi(q_1)\phi(q_2)$, which is not power of $2$. When $\frac{\phi(n)}{4}$ is even, then $|S(n)| = 2^{l_2}\phi(q_1)\phi(q_2)$, so either $\phi(q_1)\phi(q_2) = 1$ or $\phi(q_1)\phi(q_2) = 2^a, a \geq 1$. If $\phi(q_1)\phi(q_2) = 1$ then $q_1 = 1 = q_2$ and therefore $p_1 = 3$ and $p_2 = 2^{l_2} + 1(l_2 > 1)$ i.e. $p_2 \neq 3$ is Fermat prime. If $\phi(q_1)\phi(q_2) = 2^a$ then one of $\phi(q_1)$ or $\phi(q_2)$ is equal to $1$ and other is equal to $2^a$. Let $\phi(q_1) = 1$ and $\phi(q_2) = 2^a$ then $q_1 = 1$ so $p_1 = 3$ and $q_2$ is the product of Fermat prime for $a \leq 31$ so $p_2 = 2^{l_2}q_2 + 1, l_2 > 1$. If $\phi(q_1) = 2^a$ and $\phi(q_2) = 1$ then $p_1 = 2q_1 + 1,$ where $q_1$ is the product of Fermat prime for $a \leq 31$ and $p_2 = 2^{l_2} + 1$ is Fermat prime. Hence considering all the cases we can say that either any one of $p_1$ and $p_2$ is equal to $3$ or $2q + 1$ where $q_1$ is the product of Fermat primes and other is of the form $2^lq + 1$ where $l > 1$ and either $q = 1$ and $q$ is the product of Fermat primes.

Remark: The above result is true for $n = p_1^{k_1}p_2^{k_2}$ where $p_1, p_2$ are odd primes such that $(\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2$ and $k_1, k_2 \geq 1$ as $\phi(n) = \phi(p_1^{k_1}p_2^{k_2})$.

3 Relation between $S(n)$ and $K(n)$

For a positive integer $n$, set

$$K(n) = \{a \in Z_n^*|a \text{ is quadratic non-residue modulo } n\}$$

Whenever $Z_n^*$ is non-cyclic and $g$ is a semi-primitive root modulo $n$, then $g^{2l}$ for $l = 0, 1, \ldots, \frac{\phi(n)}{4} - 1$ are all the quadratic residue modulo $n$ i.e., number of quadratic residues is $\frac{\phi(n)}{4}$, which gives $|K(n)| = \frac{3}{4}\phi(n)$, where cardinality of $K(n)$ is denoted by $|K(n)|$.

In this section we study the relation between $S(n)$ and $K(n)$. We begin with the following proposition.
**Proposition 3.1.** Let \( Z_n^* \) be the non-cyclic group possessing semi-primitive root. If \( g \) is a semi-primitive root modulo \( n \) then \( g \) is quadratic non-residue (qnr) modulo \( n \).

**Proof.** Suppose \( g \) is a semi-primitive root modulo \( n \) then \( g^\frac{\phi(n)}{2} \equiv 1 \pmod{n} \) and \( \text{ord}_n(g) = \frac{\phi(n)}{2} \). To show that \( g \) is qnr modulo \( n \) that is \( \not\exists x \in Z_n^* \) such that \( x^2 \equiv g \pmod{n} \).

If possible let \( \exists x \in Z_n^* \) such that \( x^2 \equiv g \pmod{n} \). Now

\[
x^2 \equiv g \pmod{n} \Rightarrow x^{\phi(n)} \equiv 1 \pmod{n}.
\]

Again

\[
x^{-\frac{\phi(n)}{2}} = (x^2)^{\frac{\phi(n)}{4}} = g^{\frac{\phi(n)}{4}} \not\equiv 1 \pmod{n}.
\]

So \( \text{ord}_n(x) = \phi(n) \) i.e. \( x \) is a primitive root, which is a contradiction. Therefore \( g \) is quadratic non-residue modulo \( n \).

But converse is not always true. For example 7 is quadratic non-residue modulo \( 2^5 \), but 7 is not semi-primitive root modulo \( 2^5 \). For above proposition it is clear that \( S(n) \subseteq K(n) \). The following proposition gives the necessary and sufficient for \( S(n) = K(n) \).

**Proposition 3.2.** Let \( Z_n^* \) be the non-cyclic group possessing semi-primitive root. Then \( S(n) = K(n) \) iff \( n = 2^3 \) or 12.

**Proof.** We consider the following cases:

Case (i) \( n = 2^k \) \((k > 2)\).

In this case, we have, \( \phi(n) = 2^{k-1} \), and

\[
\phi(n) = 2^{k-1} = \begin{cases} 
1, & \text{if } k = 3 \\
\text{even}, & \text{otherwise}
\end{cases}
\]

When \( \frac{\phi(n)}{4} \) is odd, then \( |S(n)| = 3 \) and \( |K(n)| = 3^k \phi(n) = 3 \). So \( S(n) = K(n) \) for \( n = 2^3 \).

For \( \frac{\phi(n)}{4} \) is even, \( |S(n)| = 2^{k-2} \) and \( |K(n)| = 3.2^{k-3} \). So \( S(n) \neq K(n) \).

Case (ii) \( n = 4^k p_1^l \), where \( p_1 \) is an odd prime and \( k \geq 1 \).

As \( p_1 \) is odd prime so \( \phi(p_1) = p_1 - 1 = 2^{l_1} q_1 \), where \( l_1 \geq 1 \) and \( q_1 \geq 1 \) is an odd integer.

(a) When \( k_1 = 1 \), we have, \( \phi(n) = 2^{l_1+1} q_1 \) and

\[
\frac{\phi(n)}{4} = 2^{l_1-1} q_1 = \begin{cases} 
\text{odd}, & \text{if } l_1 = 1 \\
\text{even}, & \text{otherwise}
\end{cases}
\]

When \( \frac{\phi(n)}{4} \) is odd, then \( |S(n)| = 3 \phi(q_1) \) and \( |K(n)| = 3 q_1 \). If \( |S(n)| = |K(n)| \) then \( q_1 = 1 \), which implies \( p_1 = 3 \). So \( S(n) = K(n) \) if \( n = 4.3 = 12 \). When \( \frac{\phi(n)}{4} \) is even, then \( |S(n)| = 2^{l_1} \phi(q_1) \) and \( |K(n)| = 3.2^{l_1-1} q_1 \). If \( S(n) = K(n) \) then \( 2 \phi(q_1) = 3 q_1 \), which is not possible.

53
(b) When \( k_1 > 1 \), we have \( \phi(n) = 2^{l_1+1}q_1p_1^{k_1-1} \) and

\[
\frac{\phi(n)}{4} = 2^{l_1-1}q_1p_1^{k_1-1} = \begin{cases} 
\text{odd, if } l_1 = 1 \\
\text{even, otherwise}
\end{cases}
\]

When \( \frac{\phi(n)}{4} \) is odd, then \( |S(n)| = 6q_1\phi(q_1)p_1^{k_1-2} \) and \( |K(n)| = 3q_1p_1^{k_1-1} \). If \( S(n) = K(n) \) then \( 2\phi(q_1) = p_1 \), which is not possible. When \( \frac{\phi(n)}{4} \) is even, then \( |S(n)| = 2^{l_1}q_1\phi(q_1)p_1^{k_1-2} \) and \( |K(n)| = 2^{l_1-1}3q_1p_1^{k_1-1} \). If \( S(n) = K(n) \) then \( 2^{l_1+1}\phi(q_1) = 3p_1 \), which is not possible.

Case (iii) \( n = p_1^{k_1}p_2^{k_2} \), where \( p_1, p_2 \) are odd primes satisfying \( (\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2 \) and \( k_1, k_2 \geq 1 \).

As \( p_1, p_2 \) are odd primes so \( \phi(p_1) = 2^{l_1}q_1 \) and \( \phi(p_2) = 2^{l_2}q_2 \), where \( l_1, l_2 \geq 1 \) and \( q_1, q_2 \geq 1 \) are odd integers. Since \( (\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2 \), so \( (\phi(q_1), \phi(q_2)) = 1 \) and at least \( l_1 \) or \( l_2 \) is equal to 1. Suppose \( l_1 = 1 \).

(a) When \( k_1 = 1 = k_2 \), we have \( \phi(n) = 2^{l_2+1}q_1q_2 \) and

\[
\frac{\phi(n)}{4} = 2^{l_2-1}q_1q_2 = \begin{cases} 
\text{odd, if } l_2 = 1 \\
\text{even, otherwise}
\end{cases}
\]

When \( \frac{\phi(n)}{4} \) is odd, \( |S(n)| = 3\phi(q_1)\phi(q_2) \) and \( |K(n)| = 3q_1q_2 \), so \( S(n) \neq K(n) \). When \( \frac{\phi(n)}{4} \) is even, then \( |S(n)| = 2^{l_2}\phi(q_1)\phi(q_2) \) and \( |K(n)| = 3.2^{l_2-1}q_1q_2 \), so \( S(n) \neq K(n) \).

(b) When \( k_1 = 1, k_2 > 1 \), we have \( \phi(n) = 2^{l_2+1}q_1q_2p_2^{k_2-1} \) and

\[
\frac{\phi(n)}{4} = 2^{l_2-1}q_1q_2p_2^{k_2-1} = \begin{cases} 
\text{odd, if } l_2 = 1 \\
\text{even, otherwise}
\end{cases}
\]

If \( \frac{\phi(n)}{4} \) is odd, \( |S(n)| = 6q_2\phi(q_1)\phi(q_2)p_2^{k_2-2} \) and \( |K(n)| = 3q_1q_2p_2^{k_2-1} \), so \( S(n) \neq K(n) \). If \( \frac{\phi(n)}{4} \) is even, then \( |S(n)| = 2^{l_2}q_2\phi(q_1)\phi(q_2)p_2^{k_2-2} \) and \( |K(n)| = 3.2^{l_2-1}q_1q_2p_2^{k_2-1} \), so \( S(n) \neq K(n) \).

(c) When \( k_1 > 1 \) and \( k_2 = 1 \) then in similar way we get \( S(n) \neq K(n) \).

(d) When \( k_1, k_2 > 1 \), we have \( \phi(n) = 2^{l_2+1}q_1q_2p_1^{k_1-1}p_2^{k_2-1} \) and

\[
\frac{\phi(n)}{4} = 2^{l_2-1}q_1q_2p_1^{k_1-1}p_2^{k_2-1} = \begin{cases} 
\text{odd, if } l_2 = 1 \\
\text{even, otherwise}
\end{cases}
\]

If \( \frac{\phi(n)}{4} \) is odd, \( |S(n)| = 12q_2q_1\phi(q_1)\phi(q_2)p_1^{k_1-2}p_2^{k_2-2} \) and \( |K(n)| = 3q_1q_2p_1^{k_1-1}p_2^{k_2-1} \), so \( S(n) \neq K(n) \). If \( \frac{\phi(n)}{4} \) is even, then \( |S(n)| = 2^{l_2+1}q_1q_2\phi(q_1)\phi(q_2)p_1^{k_1-2}p_2^{k_2-2} \) and \( |K(n)| = 3.2^{l_2-1}q_1q_2p_1^{k_1-1}p_2^{k_2-1} \), so \( S(n) \neq K(n) \).

Case (iv) When \( n = 2p_1^{k_1}p_2^{k_2} \), where \( p_1, p_2 \) are odd primes satisfying \( (\phi(p_1^{k_1}), \phi(p_2^{k_2})) = 2 \) and \( k_1, k_2 \geq 1 \).

As \( \phi(p_1^{k_1}p_2^{k_2}) = \phi(2p_1^{k_1}p_2^{k_2}) \), so in this case also \( S(n) \neq K(n) \).

Hence combining all the cases we get \( S(n) = K(n) \) iff \( n = 2^3 \) or 12. \( \square \)
4 Conclusion and Future work

In this paper, we have dealt with the number of semi-primitive modulo \( n \), which is an application of inverse Euler's \( \varphi \)-function. We also get a connection between set of semi-primitive roots modulo \( n \) and set of quadratic non-residue modulo \( n \).

Semi-primitive roots in non-cyclic groups play almost the same role as primitive roots in cyclic groups, so it may be useful to construct a secure cryptosystem. We will consider this issue in our future work.

References
