ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.1, 583–588
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.1.57

CHARACTERIZATION OF THE SET OF INVOLUTORY ELEMENTS OF $(Z_n, \oplus_n, \odot_n)$

C. Prameela Rani[1] and M. Siva Parvathi

ABSTRACT. For a positive integer n, $Z_n = \{0, 1, 2, \dots n-1\}$ is a ring of integers modulo n. Let I_v denotes the set of all involuntary elements in Z_n. In this paper, characterization of I_v depending on the positive integer n is discussed and the results are presented.

1. INTRODUCTION

Let $Z_n = \{0, 1, 2, \dots n-1\}$ where n is a positive integer, be a set of equivalence class modulo n, the $(Z_n, \oplus_n)$ be an abelian group of order n, where $\oplus_n$ denotes the addition modulo n. Let I_v denotes the set of all involuntary elements in Z_n. It is easy to see that I_v is a symmetric subset of the group$(Z_n, \oplus_n)$ and the $(I_v, \odot_n)$ is a multiplicative subset of the semigroup $(Z_n^*, \odot_n)$, where $Z_n^* = Z_n - \{0\}$, and $\odot_n$ denotes multiplication modulo n. In this study we have followed Apostol [1] for Number theory terminology. Venkata Anusha et al. [2] defined involutory Cayley graph on the ring of integers modulo n and some basic properties are studied. Motivated by this, in this paper, for various values of n, we have characterized the set of involutory elements of Z_n.

[1] *corresponding author*
2020 *Mathematics Subject Classification.* 05C25.
Key words and phrases. Ring of integers modulo n, Involutory set, Symmetric set.
Submitted: 27.12.2020; *Accepted:* 11.01.2021; *Published:* 24.01.2021.

2. INVOLUTORY SET OF $(Z_n, \oplus_n, \odot_n)$

Definition 2.1. *Let ($Z_n, \oplus_n, \odot_n$) be a ring of integers modulo n. An element $m \in Z_n$ such that $m^2 \equiv 1(\mod n)$ is considered as an involutory element in Z_n. Then the set of involutory elements is denoted by I_v and therefore $I_v = \{m \in Z_n : m^2 \equiv 1(\mod n)$ }.*

Lemma 2.1. *If $(Z_n, \oplus_n, \odot_n)$ is a ring of integers modulo n. Then the set I_v of Involutory elements of $(Z_n, \oplus_n, \odot_n)$ is symmetric.*

Proof. Let $Z_n = \{0, 1, 2, \ldots, n-1\}$ be a ring of integers modulo n with respect to $\oplus_n, \odot_n$. Suppose $m \in I_v \Rightarrow m^2 \equiv 1(\mod n) \Rightarrow m^2 - 1$ is divisible by n, that means $m^2 - 1 = nx$, for some integer x.

Consider $(n-m)^2 - 1 = n^2 + m^2 - 2mn - 1 = n^2 - 2mn + nx = n(n-2m+x) = n$ (some integer). Therefore $(n-m)^2 - 1$ is divisible by n hence $(n-m) \in I_v$. Therefore I_v is symmetric. □

3. CHARACTERIZATION OF INVOLUTORY SET I_v OF $(Z_n, \oplus_n, \odot_n)$

In this section, the number of elements in the involutory set of the ring $(Z_n, \oplus_n, \odot_n)$ of integers modulo n is categorized for different values of n.

Theorem 3.1. *If $n = 2^\alpha$, where $\alpha \geq 3$ and I_v is the set of involutory elements of ring of integers modulo n, then $|I_v| = 4$.*

Proof. Let Z_n be the ring of integers modulo n and $n = 2^\alpha, \alpha \geq 3$. Then $Z_n = \{1, 2, 3, 2^2, \ldots 2^3, \ldots 2^{\alpha-1}, \ldots 2^\alpha - 1$ }. It is clear that $1^2 \equiv 1(\mod n)$, it implies $1 \in I_v$ and $n - 1 = 2^\alpha - 1 \in I_v$. If $m = 2^{\alpha-1} - 1$, then $(m-1)(m+1) = (2^{\alpha-1} - 2)(2^{\alpha-1}) = 2^\alpha(2^{\alpha-2} - 1)$, is divisible by n. It implies $m^2 \equiv 1(\mod n)$ and $m = 2^{\alpha-1} - 1 \in I_v$. If $m = 2^{\alpha-1} + 1$, then $(m-1)(m+1) = (2^{\alpha-1})(2^{\alpha-1} + 2) = 2^\alpha(2^{\alpha-2} + 1)$, is divisible by n. It implies $m^2 \equiv 1(\mod n)$ and $m = 2^{\alpha-1} + 1 \in I_v$. For any other factor 2^β, where $\beta < \alpha - 1$, neither $2^\beta - 1$ nor $2^\beta + 1$ is the involutary element of Z_n.

Therefore $I_v = \{1, 2^{\alpha-1} - 1, 2^{\alpha-1} + 1, n - 1\}$ and hence $|I_v| = 4$. □

Theorem 3.2. *If $n = p^\alpha$, where p is a prime and $p \neq 2, \alpha \geq 1$ and I_v is the set of involutory elements of ring of integers modulo n then $|I_v| = 2$.*

Proof. Consider the set $(Z_n, \oplus_n, \odot_n)$ the ring of integers modulo n. Let $n = p^\alpha$, where p is a prime and $p \neq 2, \alpha \geq 1$. Then$Z_n = \{0, 1, 2, \ldots p, \ldots p^2, \ldots p^\alpha - 1\}$. Let I_v be the set of involutory elements of $(Z_n, \oplus_n, \odot_n)$. Since $1^2 \equiv 1(\mod n)$, so that $1 \in I_v$ and also by symmetric property of involutory set of Z_n, $n - 1 = p^\alpha - 1 \in I_v$. Any other element $m \in Z_n$ is not an involutory element. For $m = p - 1, (m - 1)(m + 1) = p(p - 2) = p^2 - 2p$, it is not divisible by p^α, so $m^2 \not\equiv 1(\mod n)$ and for $m = p + 1, (m - 1)(m + 1) = p(p + 2) = p^2 + 2p$, which is not divisible by p^α, so $m^2 \not\equiv 1(\mod n)$.

Similarly for any other factor p^β, $\beta < \alpha$, neither $p^\beta - 1$ nor $p^\beta + 1$ lies in I_v. Therefore the set I_v contains only two elements 1 and $n - 1$. Hence $|I_v| = 2$. □

Theorem 3.3. *If $n = 2^\alpha p^{\alpha_1}$ where p is a prime and $\alpha \geq 1$ and I_v is the set of involutory elements of ring of integers modulo n then*

$$|I_v| = \begin{cases} 2, if \alpha = 1, \\ 4, if \alpha = 2, \\ 8, if \alpha \geq 3. \end{cases}$$

Proof. Consider the set $(Z_n, \oplus_n, \odot_n)$, the ring of integers modulo n. Let I_v be the set of involutory elements of $(Z_n, \oplus_n, \odot_n)$.

Let $n = 2^\alpha p^{\alpha_1}$, p is a prime and $\alpha_1 \geq 1$. Then there are three possible cases arise.

Case 1: Suppose $\alpha = 1$. Then $n = 2p^{\alpha_1}, p$ is a prime, $\alpha_1 \geq 1$ and the ring Z_n= $\{0, 1, 2, \ldots p, \ldots 2p^{\alpha_1} - 1\}$. It is clear that 1 and $n - 1$ are the involutory elements of Z_n, since $1^2 \equiv 1(\mod n), 1 \in I_v$ and $n - 1 = 2p^{\alpha_1} - 1 \in I_v$. Also any other factor $p^\beta, \beta < \alpha_1$, neither $p^\beta - 1$ nor $p^\beta + 1$ lies in I_v. Therefore $|I_v| = 2$.

Case 2: Suppose $\alpha = 2$. Then $n = 2^2p^{\alpha_1}$, p is a prime, $\alpha_1 \geq 1$ and the ring $Z_n = \{0, 1, 2, \ldots p, \ldots 2^2p^{\alpha_1} - 1\}$. Clearly 1 and $n - 1$ are the involutory elements of Z_n, since $1^2 \equiv 1(\mod n), 1 \in I_v$ and $n - 1$=$2^2p^{\alpha_1} - 1 \in I_v$. Also for $m = 2p^{\alpha_1} - 1, (m - 1)(m + 1) = (p^{\alpha_1} - 2)2p^{\alpha_1} = 2^2p^{\alpha_1}(p^{\alpha_1} - 1)$, it is divisible by n. That means $m^2 - 1$ is divisible by n. It implies $m \in I_v$. And for $m = 2p^{\alpha_1} + 1, (m - 1)(m + 1) = 2p^{\alpha_1}(2p^{\alpha_1} + 2) = 2^2p^{\alpha_1}(p^{\alpha_1} + 1)$, it is divisible by n. It implies $m^2 - 1$ is divisible by n. Therefore $m \in I_v$. Then the set of involutory elements $I_v = \{1, 2p^{\alpha_1} - 1, 2p^{\alpha_1} + 1, 2^2p^{\alpha_1} - 1\}$ and therefore $|I_v| = 4$.

Case 3: Suppose $\alpha = 3$. Then $n = 2^3p^{\alpha_1}, p$ is a prime,$\alpha_1 \geq 1$ and the ring $Z_n = \{0, 1, 2, \ldots, 2p^{\alpha_1}, \ldots 2^2p^{\alpha_1}, \ldots .2^3p^{\alpha_1} - 1\}$. It is clear that $1, n - 1$ are the involutory

elements of Z_n, since $1^2 \equiv 1(\mod n), 1 \in I_v$ and $n-1 = 2^3p^{\alpha_1} - 1 \in I_v$.
If $m = 2p^{\alpha_1} - 1$, then $(m-1)(m+1) = (2p^{\alpha_1} - 2)2p^{\alpha_1} = 4p^{\alpha_1}(p^{\alpha_1} - 1) = 4p^{\alpha_1}(2x)$, for some positive integer x. Since $p^{\alpha_1} - 1$ is even. It implies $(m-1)(m+1) = 2^3p^{\alpha_1}(x)$. It is divisible by n. Therefore $2p^{\alpha_1} - 1 \in I_v$ and $n - m = 2^3p^{\alpha_1} - 2p^{\alpha_1} + 1 \in I_v$.

If $m = 2p^{\alpha_1} + 1$, then $(m-1)(m+1) = (2p^{\alpha_1})(2p^{\alpha_1} + 2) = 4p^{\alpha_1}(p^{\alpha_1} + 1)4p^{\alpha_1}(2x)$, for some positive integer x, since $p^{\alpha_1} + 1$ is even. It implies $(m-1)(m+1) = 2^3p^{\alpha_1}(x)$, it is divisible by n. Therefore $2p^{\alpha_1} + 1 \in I_v$ and $n - m = 2^3p^{\alpha_1} - 2p^{\alpha_1} - 1 \in I_v$.

If $m = 2^2p^{\alpha_1} - 1$, then $(m-1)(m+1) = (2^2p^{\alpha_1} - 2)2^2p^{\alpha_1} = 2^3p^{\alpha_1}(p^{\alpha_1} - 1)$, it is divisible by n. Therefore $2^2p^{\alpha_1} - 1 \in I_v$.

If $m = 2^2p^{\alpha_1} + 1$, then $(m-1)(m+1) = (2^2p^{\alpha_1})(2^2p^{\alpha_1} + 2) = 2^3p^{\alpha_1}(p^{\alpha_1} + 1)$, it is divisible by n. Therefore $2^2p^{\alpha_1} + 1 \in I_v$. Hence the set of involutory elements of Z_n, $I_v = \{1, 2p^{\alpha_1} - 1, 2p^{\alpha_1} + 1, 2^2p^{\alpha_1} + 1, 2^3p^{\alpha_1} - 2p^{\alpha_1} - 1, 2^3p^{\alpha_1} - 2p^{\alpha_1} + 1, 2^3p^{\alpha_1} - 1\}$ and therefore $|I_v| = 8$.

Case 4: Suppose $\alpha > 3$. Then $n = 2^\alpha p^{\alpha_1}, p$ is a prime, $\alpha_1 \geq 1$ and the ring $Z_n = \{0, 1, 2, \ldots, 2^\alpha p^{\alpha_1} - 1\}$. It is clear that $1, n-1$ are the involutory elements of Z_n, since $1^2 \equiv 1(\mod n), 1 \in I_v$ and $n - 1 = 2^\alpha p^{\alpha_1} - 1 \in I_v$. Then the number of distinct partitions of $\{2^{\alpha-1}, 2, p^{\alpha_1}\}$ is 3 and in each partition, there exist two involutory elements. Hence the total number of involutory elements is 8. $\square$

Theorem 3.4. *If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \cdots \cdot p_k^{\alpha_k}$ where each p_i is a prime number and $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 1$ and I_v is the set of involutory elements of ring of integers modulo n, then $|I_v| = 2^k$.*

Proof. Consider the set $(Z_n, \oplus_n, \odot_n)$ the ring of integers modulo n. Let I_v be the set of involutory elements of Z_n. Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3} \ldots .p_k^{\alpha_k}$ where each p_i is a prime number and $\alpha_1, \alpha_2 \ldots, \alpha_k \geq 1$. Consider any two random partitions on distinct prime powers of n, let $P_1 = \{p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_i^{\alpha_i}\}$ and $P_2 = \{p_{i+1}^{\alpha_{i+1}}, p_{i+2}^{\alpha_{i+2}}, \ldots p_k^{\alpha_k}\}$ and $P_1 \cap P_2 = \phi$. Then there exist two positive integers x and y such that $|(p_1^{\alpha_1}.p_2^{\alpha_2} \cdot \cdots \cdot p_i^{\alpha_i})x - (p_{i+1}^{\alpha_{i+1}} \cdot p_{i+2}^{\alpha_{i+2}} \cdot \ldots .p_k^{\alpha_k})y| = 2$, where $1 \leq x \leq p_{i+1}^{\alpha_{i+1}}.p_{i+2}^{\alpha_{i+2}} \cdot \ldots .p_k^{\alpha_k}$ and $1 \leq y \leq p_1^{\alpha_1}.p_2^{\alpha_2} \cdot \ldots .p_i^{\alpha_i}$.

If $m = \frac{(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_i^{\alpha_i})x - (p_{i+1}^{\alpha_{i+1}} \cdot p_{i+2}^{\alpha_{i+2}} \cdot \cdots \cdot p_k^{\alpha_k})y}{2}$ then

$$\begin{aligned}(m-1)(m+1) &= (p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots\cdot p_i^{\alpha_i})x\cdot(p_{i+1}^{\alpha_{i+1}}\cdot p_{i+2}^{\alpha_{i+2}}\cdot\dots\cdot p_k^{\alpha_k})y\\ &= (p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}\cdot\dots\cdot p_k^{\alpha_k})xy.\end{aligned}$$

It is divisible by n. Therefore $m^2 \equiv 1(\mod n)$ and$m \in I_v$ and$n-m \in I_v$. From each partition, we get two involutory elements and the number of distinct random partition of these k prime powers of n is

$$\frac{\binom{k}{1}+\binom{k}{2}+\binom{k}{3}+\dots+\binom{k}{k-1}}{2} = \frac{\binom{k}{0}+\binom{k}{1}+\binom{k}{2}+\dots+\binom{k}{k}-\binom{k}{0}-\binom{k}{k}}{2} = \frac{2^k-2}{2}.$$

From all the possible partitions, there exists $2\left(\frac{2^k-2}{2}\right) = 2^k-2$ involutory elements of Z_n. Since for any n, 1 and $n-1 \in I_v$. Therefore the total number of elements in I_v is $2^k-2+2=2^k$. □

Theorem 3.5. *If $n = 2^\alpha\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots p_k^{\alpha_k}$ where p_i is a prime and $\alpha_i \geq 1, \forall i$ and I_v is the set of involutory elements of ring of integers modulo n then*

$$|I_v| = \begin{cases} 2^k, & if \ \ \alpha = 1,\\ 2^{k+1}, & if \ \ \alpha = 2,\\ 2^{k+2}, & if \ \ \alpha \geq 3.\end{cases}$$

Proof. Consider the ring of integers modulo n and $n = 2^\alpha.p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots p_k^{\alpha_k}$ where each p_i is a prime and $\alpha_i \geq 1, \forall i$ Then there are three possible cases arise.

Case 1: Suppose $\alpha = 1$. Then $n = 2^\alpha.p_1^{\alpha_1}.p_2^{\alpha_2}.\dots p_k^{\alpha_k}$. Consider two partitions as $\{2\}$ and $\{p_1^{\alpha_1}.p_2^{\alpha_2}.\dots p_k^{\alpha_k}\}$ on the prime powers of n. Since each p_i is odd, neither $(p_1^{\alpha_1}.p_2^{\alpha_2}.\dots p_k^{\alpha_k})-2$ nor $(p_1^{\alpha_1}.p_2^{\alpha_2}.\dots p_k^{\alpha_k})+2$ is divisible by 2. With this reason, no involutory elements exists. So we consider $2p_i^{\alpha_i}$ for any i, as a single number. Now we have $(2p_i^{\alpha_i}.p_1^{\alpha_1}.p_2^{\alpha_2},\dots,p_{i-1}^{\alpha_i-1}.p_{i+1}^{\alpha_i+1},\dots,p_k^{\alpha_k})$ are k distinct factors of n. By the Theorem 3.4, the number of elements in I_v is 2^k.

Case 2: Suppose $\alpha = 2$. Then $n = 2^2\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots\cdot p_k^{\alpha_k}$. Now we have $2^2\cdot p_i^{\alpha_i}p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots\cdot p_k^{\alpha_k}$ are $k+1$ distinct factors of n. By the Theorem 3.4, the number of elements in I_v is 2^{k+1}.

Case 3: Suppose $\alpha \geq 3$. Then $n = 2^\alpha.p_1^{\alpha_1}.p_2^{\alpha_2}.\dots p_k^{\alpha_k}$. Now the $k+2$ numbers, $2^{\alpha-1}, 2.p_1^{\alpha_1}, p_2^{\alpha_2}.\dots p_k^{\alpha_k}$ are distinct factors of n. By the Theorem 3.4, $|I_v| = 2^{k+2}$. □

REFERENCES

[1] T. M. APOSTAL: *Introduction to Analytical Number Theory*, Springer International, Student Edition, 1989.

[2] M. VENKATA ANUSHA, M. SIVA PARVATHI: *Properties of the Involutory Cayley graph of* $(Z_n, \oplus, \odot)$, AIP Conference Proceedings 2246, (2020), ID020065.

DEPARTMENT OF APPLIED MATHEMATICS
SRI PADMAVATI MAHILA VISVAVIDYALAYAM
TIRUPATI, ANDHRA PRADESH, INDIA
Email address: c.prameela7@gmail.com

DEPARTMENT OF APPLIED MATHEMATICS
SRI PADMAVATI MAHILA VISVAVIDYALAYAM
TIRUPATI, ANDHRA PRADESH, INDIA
Email address: parvathimani2008@gmail.com