Int. J. Res. Ind. Eng. Vol. 8, No. 1 (2019) 77–88

International Journal of Research in Industrial Engineering

www.riejournal.com

Number Theoretic Properties of the Commutative Ring Z_n

Sh. Sajana[1,*], D. Bharathi[2]

[1] Department of Mathematics and Statistics, P.R. Govt. College (A), Kakinada, Andhra Pradesh, India.
[2] Department of Mathematics, S.V. University, Tirupati, Andhra Pradesh, India.

A B S T R A C T

This paper deals with the number theoretic properties of non-unit elements of the ring Z_n. Let D be the set of all non-trivial divisors of a positive integer n. Let D_1 and D_2 be the subsets of D having the least common multiple which are incongruent to zero modulo n with every other element of D and congruent to zero modulo n with at least one another element of D, respectively. Then D can be written as the disjoint union of D_1 and D_2 in Z_n. We explore the results on these sets based on all the characterizations of n. We obtain a formula for enumerating the cardinality of the set of all non-unit elements in Z_n whose principal ideals are equal. Further, we present an algorithm for enumerating these sets of all non-unit elements.

Keywords: Non-unit elements, Non-trivial divisor, Least common multiple, Congruent, Finite commutative ring, Principal ideal.

Article history: *Received: 02 October 2018* *Revised: 01 January 2019* *Accepted: 14 February 2019*

1. Introduction

Number theory is a branch of mathematics and it is devoted primarily to the study of integers and the properties of counting numbers. The positive integers are undoubtedly man's first mathematical creation. In 17th century Fermat was the first to discover the deep properties of integers. Nathanson [1] introduced some specific arithmetical concepts of number theory, in particular the notion of congruence of numbers in graph theory and motivated the special way for emerging of a new class of undirected simple graphs, namely arithmetic graphs.

The set U_n contains all the positive integers which are not exceeding n and relatively prime to n, called the unit elements and cardinality of the set U_n is $\varphi(n)$, the Euler totient function [2]. The set of all elements in the ring Z_n, the ring of integers modulo n can be written as the disjoint

* Corresponding author
E-mail address: ssajana.maths@gmail.com
DOI: 10.22105/riej.2019.159539.1065

union of the sets, the set of all unit elements, U_n , and the set of all zero divisors, $Z(Z_n)$ of Z_n [3-4]. The non-zero elements a and b in a ring R are said to be zero divisors, if $a.b = 0$. The set of all non-zero zero divisors in R is denoted by $Z(R)^* = Z(R) \setminus \{0\}$ and we called $Z(R)$ as the set of non-unit elements.

Let d be an element in Z_n, then the principal ideal of d in Z_n is $(d) = \{0, d, 2d, \dots, n-d\}$ and cardinality of (d) is the number elements in (d), denoted by $|(d)|$. In this paper, we mainly derived a formula for enumerating the cardinality of the set of all non-unit elements in Z_n whose principal ideals are equal and also we present an algorithm for enumerating these sets of all non-unit elements.

2. Basic Properties of the Non-Trivial Divisors of n in Z_n

Definition 1. Every positive integer $n > 1$ can be written as $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, where $p_1 < p_2 < \cdots < p_m$ are primes, α_i is a positive integer for every $i = 1, 2, \dots, m$ and $m \geq 1$, which is called the canonical representation of a positive integer n.

Definition 2. Let a, b, and m be any positive integers. If n divides the difference $a - b$, then we said that a is congruent to b modulo n and we write $a \equiv b \pmod n$. In other words, it is equivalent to the divisibility relation $n|(a-b)$. If n does not divide the difference $a - b$, then we say that a is incongruent to b modulo n and we write $a \not\equiv b \pmod n$.

Definition 3. If a positive integer n can be written as $n = cd$, for some positive integers c and d. Then we say that d divides n or d is a divisor of n and written as $d|n$. Otherwise, we say that d does not divide n or d is not a divisor of n and written as $d \nmid n$. A divisor d of n is called trivial if $d \in \{1, n\}$, otherwise d is called non-trivial divisor of n.

Let the set D denotes the set of all non-trivial divisors of n, i.e., $D = \{d : d|n, \; d \in Z_n$ and $d \neq 1, n\}$. The following theorem represents partition of the set D in Z_n.

Theorem 1. Let D_1 and D_2 be the sets of all elements in D having the least common multiple which is incongruent to zero modulo n with every other element of D and congruent to zero modulo n with at least one another element of D, respectively. Then D can be written as the disjoint union of D_1 and D_2 in Z_n.

Proof. Let $n > 1$ be any positive integer. Then for any $d_1 \neq d_2$ in D, we have

$$D_1 = \{d_1 \in D : [d_1, d'] \not\equiv 0 \pmod n, \text{ for all } d' \neq d_1 \in D\} \text{ and}$$

$$D_2 = \{d_2 \in D : [d_2, d'] \equiv 0 \pmod n, \text{ for some } d' \neq d_2 \in D\}.$$

Clearly D is the union of D_1 and D_2, i.e., $D = D_1 \cup D_2$. Now, we have to show that D_1 and D_2 are disjoint. Suppose $D_1 \cap D_2 \neq \emptyset$, let $q \in D_1 \cap D_2$. Then $q \in D_1$ and $q \in D_2$. If $q \in D_1$, then q can be written as $q = {p_1}^{\alpha_1 - 1} {p_2}^{\alpha_2 - 1} \dots {p_m}^{\alpha_m - 1}$. Similarly, if $q \in D_2$, then q can be written as $q =$

$p_1p_2 \dots p_m$. Therefore, ${p_1}^{\alpha_1-1}{p_2}^{\alpha_2-1} \dots {p_m}^{\alpha_m-1} = p_1p_2 \dots p_m$. This implies that $\alpha_i - 1 = 1,\ \forall\ 1 \le i \le m$. Therefore $\alpha_i = 2,\ \forall\ 1 \le i \le m$ and hence $n = {p_1}^2{p_2}^2 \dots {p_m}^2$, which shows that q in D_1 but not in D_2 from the definitions of D_1 and D_2. This is a contradiction to the fact that $q \in D_2$. Hence the proof.

Example 1. In the ring Z_{12}, the set of all non-trivial divisors of 12 is $D = \{2,\ 3,\ 4,\ 6\}$. The sets D_1 and D_2 are $D_1 = \{2\}$ and $D_2 = \{\ 3,\ 4,\ 6\}$, which clearly shows that D is the disjoint union of D_1 and D_2.

Lemma 1. In the ring Z_n, for every positive integer n and every prime p, we have

- $D = \emptyset$, if $n = p$.
- $D_1 = D$ and $D_2 = \emptyset$, if $n = p^\alpha$ with $\alpha > 1$.
- $D_1 = \emptyset$ and $D_2 = D$, if $n = p_1p_2 \dots p_m$ with $m > 1$.
- $D = D_1 \cup D_2$, both D_1 and D_2 are non-empty, if $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$, where α_i is a positive integer, for all $1 \le i \le m$ and $\alpha_1 + \alpha_2 + \dots + \alpha_m > m$ with $m \ge 2$.

Proof.

- If $n = p$, then there does not exist non-trivial divisors of n in the ring Z_n. Clearly $D = \emptyset$.
- If $n = p^\alpha$ with $\alpha > 1$, then the set of all non-trivial divisors of n in the ring Z_n is $D = \{p,\ p^2,\ \dots,\ p^{\alpha-1}\}$. Let x and y be any two distinct arbitrary elements in D. Then there exist two distinct positive integers r and s, $1 \le r,\ s < \alpha$ such that $x = p^r$ and $y = p^s$. Now, the least common multiple of x and y is $[x,\ y] = [p^r,\ p^s] = p^t \not\equiv 0 \pmod{n}$, where $t = \max\{r,\ s\}$. This shows that $D = D_1$.
- If $n = p_1p_2 \dots p_m$ with $m > 1$, then the set of all non-trivial divisors D of n in the ring Z_n is, $D = \{p_1,\ p_2, \dots,\ p_m,\ p_1p_2,\ p_1p_3,\ \dots,\ p_{m-1}p_m,\ \dots,\ p_1p_2 \dots p_{m-1},\ \dots, p_2p_3 \dots p_m\}$. Suppose that $D_1 \ne \emptyset$, we assume $q \in D_1$. By the definition of D_1, element q can be written as $q = {p_1}^{1-1}{p_2}^{1-1} \dots {p_m}^{1-1}$, which contradicts to the fact that D contains non-trivial divisors of n in the ring Z_n. This completes the proof.
- If $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$ with $\alpha_1 + \alpha_2 + \dots + \alpha_m > m$ and $m \ge 2$. Now, we have to show that D_1 and D_2 are non-empty.

Subcase 1. Suppose that both D_1 and D_2 are empty. Then by the Theorem 1, D is empty. But, we know that the total number of non-trivial divisors of n are$(\alpha_1 + 1)(\alpha_2 + 1) \dots$

$(\alpha_m + 1) - 2 > 4$, which contradicts to the fact that D is empty.

Subcase 2. Suppose that D_1 is non-empty and D_2 is empty. Without loss of generality, assume that $n = p^2q$. Then the set D of non-trivial divisors of n in the ring Z_n is $D = \{p,\ p^2,\ q,\ pq\}$. So, there exists $p^2 \in D$ such that whose the least common multiple is congruent to zero modulo n with $q \in D$, i.e., $[p^2,\ q] \equiv 0 \pmod{n}$. This shows that $p^2 \in D_2$, which contradicts to the hypothesis that D_2 is empty.

Subcase 3. Suppose that D_1 is empty and D_2 is non-empty. Similarly in subcase 2, assume $n = p^2q$. Then the set D of non-trivial divisors of n in the ring Z_n is $D = \{p,\ p^2,\ q,\ pq\}$. We have, there exists $p \in D$ such that whose least common multiple is incongruent to zero modulo n with every element in D, i.e., $[p,\ d] \not\equiv 0\ (\mathrm{mod}\ n),\ \forall\ d \neq p \in D$. This shows that $p \in D_1$, which contradicts to the hypothesis that D_1 is empty.

Hence the proof follows from the above three subcases.

Theorem 2. The cardinality of the set of all non-zero zero divisors $Z(Z_n)^*$ in the ring Z_n is $|Z(Z_n)^*| = n - \varphi(n) - 1$.

Proof. For each $n > 1$, we have $Z_n = U_n \cup Z(Z_n)$ and $U_n \cap Z(Z_n) = \emptyset$. Therefore, $|Z_n| = |U_n \cup Z(Z_n)|$ and $|Z(Z_n)| = n - \varphi(n)$.

But $Z(Z_n)^* = Z(Z_n) \backslash \{0\}$ and hence $|Z(Z_n)^*| = n - \varphi(n) - 1$.

Lemma 2. Let x be any element in $P(D_1) = \{x \in Z_n : (x) = (d),\ \text{for some } d \in D_1\}$. Then $[x,\ y] \not\equiv 0(\mathrm{mod}\ n)$, for every $y \neq x$ in $Z(Z_n)^*$.

Proof. From the definition of D_1, we have $D_1 = \{d_1 \in D : [d_1,\ d'] \not\equiv 0\ (\mathrm{mod}\ n),\ \text{for all } d' \neq d_1 \in D\}$, where D is the set of all non-trivial divisors of a positive integer n. This implies that the proof follows.

Theorem 3. Let $P(D_1) = \{x \in Z_n : (x) = (d),\ \text{for some } d \in D_1\}$ and $P(D_2) = \{x \in Z_n : (x) = (d),\ \text{for some } d \in D_2\}$. Then the set of all non-zero zero divisors $Z(Z_n)^*$ of the ring Z_n can be partitioned into the sets $P(D_1)$ and $P(D_2)$.

Proof. The set D of all non-trivial divisors of a positive integer n can be written as the disjoint union of the sets D_1 and D_2. This implies the set $Z(Z_n)^*$ can be partitioned into the sets $P(D_1)$ and $P(D_2)$ in the ring Z_n. (By the Theorem 1).

Example 2. In the ring Z_{12}, the set of all non-zero zero divisors is $Z(Z_{12})^* = \{2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 10\}$. The sets $P(D_1) = \{2, 10\}$ and $P(D_2) = \{3,\ 4,\ 6,\ 8,\ 9\}$, which clearly shows that $Z(Z_{12})^*$ is the disjoint union of $P(D_1)$ and $P(D_2)$, because $D = \{2,\ 3,\ 4,\ 6\}$, $D_1 = \{2\}$ and $D_2 = \{3,\ 4,\ 6\}$.

Corollary 1. In the ring Z_n, for every positive integer n and every prime p, we have

- $Z(Z_n)^* = \emptyset$, if $n = p$.
- $Z(Z_n)^* = P(D_1)$, if $n = p^\alpha$ with $\alpha > 1$.
- $Z(Z_n)^* = P(D_2)$, if $n = p_1 p_2 \dots p_m$, with $m > 1$.
- $Z(Z_n)^* = P(D_1) \cup P(D_2)$, both $P(D_1)$ and $P(D_2)$ are non-empty, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, where α_i is a positive integer, for all $1 \leq i \leq m$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_m > m$ with $m \geq 2$.

Proof. The proof directly follows from Lemma 1.

Lemma 3. For every non-trivial divisor d of n, the cardinality of the set (d), principal ideal of d in the ring Z_n is $|(d)| = \frac{n}{d}$.

Proof. We have, the principal ideal of d in the ring Z_n is $(d) = \{0,\ d,\ 2d,\ \dots,\ n-d\}$. It can be written as $(d) = \{0,\ 1d,\ 2d,\ \dots,\ \left(\frac{n}{d}-1\right)d\}$. Clearly, there is a one-to-one correspondence between (d) and $\{0, 1, 2,\ \dots, \frac{n}{d}-1\}$. So, the cardinality of the set (d) is $\frac{n}{d}$.

3. Enumeration of Non-Unit Elements in Z_n Whose Principal Ideals Are Equal

In this section, we partition the set (d) principal ideal of d, which is the union of the sets S_d and T_d for every non-trivial divisor d of n, where $S_d = \left\{rd \in Z_n: (rd) = (d),\ 1 \le r < \frac{n}{d}\right\}$ and $T_d = \left\{rd \in Z_n: (rd) \neq (d),\ 1 \le r < \frac{n}{d}\right\}$. Also, we define the set $S_d{}' = \{rd \in Z_n:\ (rd,\ n) = d,\ 1 \le r < \frac{n}{d}\}$ and proved that $S_d = S_d{}'$ for every non-trivial divisor d of n. Next we obtained a formula for enumerating the cardinality of the set S_d for all d in D.

Theorem 4. Let $S_d = \{rd \in Z_n: (rd) = (d),\ 1 \le r < \frac{n}{d}\}$ and $T_d = \{rd \in Z_n: (rd) \neq (d),\ 1 \le r < \frac{n}{d}\}$, for all d in D. Then $(d) = S_d \cup T_d$, where $S_d \cap T_d = \emptyset$.

Proof. Since (d) in the ring Z_n consists of all the multiples of d in Z_n and $(d) = (n-d)$, where $n - d \in (d)$ in Z_n, for all d in D. The total number of elements in (d) in the ring Z_n can be written as the disjoint union of two sets such that one of sets is consisting of all elements in Z_n, whose principal ideals are equal to (d) and the another set is consisting of all elements in Z_n, whose principal ideals are not equal to (d) in the ring Z_n, that is

$$(d) = \{rd \in Z_n: (rd) = (d),\ 1 \le r < \tfrac{n}{d}\} \cup \{rd \in Z_n: (rd) \neq (d),\ 1 \le r < \tfrac{n}{d}\}.$$

Setting $S_d = \{rd \in Z_n: (rd) = (d),\ 1 \le r < \frac{n}{d}\}$ and $T_d = \{rd \in Z_n: (rd) \neq (d),\ 1 \le r < \frac{n}{d}\}$. Hence $(d) = S_d \cup T_d$.

Notations 1. For every non-trivial divisor d of n in the ring Z_n, we define the set $S_d{}'$ as $S_d{}' = \{rd \in Z_n:\ (rd,\ n) = d,\ 1 \le r < \frac{n}{d}\} = \{rd \in Z_n: \left(r,\ \frac{n}{d}\right) = 1,\ 1 \le r < \frac{n}{d}\}$.

Theorem 5. [5]**.** Let A and B be any two non-empty sets. Then $A = B$ if and only if $|A| = |B|$ and $A \subset B$.

Theorem 6. Let d in $S_d{}'$ of the ring Z_n. For any rd in $S_d{}'$ with $\left(r,\ \frac{n}{d}\right) = 1$, $1 < r < \frac{n}{d}$, we have $(d) = (rd)$, where d is a non-trivial divisor of n.

Proof. We define a function $g: (d) \longrightarrow (rd)$ by the relation $g(d) = rd,\ \forall\ d \in (d)$.

- For $x,\ y\ \in (d)$, we have $g(x) = g(y)$. This implies that $rx = ry$, where r is a unit in $Z_{\frac{n}{d}}$, because $\left(r,\ \frac{n}{d}\right) = 1$. So there exists $r^{-1} \in Z_{\frac{n}{d}}$ such that $rr^{-1} = 1$.
  Now, $r^{-1}(rx) = r^{-1}(ry)$

  $\Rightarrow (r^{-1}r)x = (r^{-1}r)y$

  $\Rightarrow 1.x = 1.y$

  $\Rightarrow\ x = y.$

This shows that g is one-to-one function.

- For each unit element r in $Z_{\frac{n}{d}}$, there exists r^{-1} in $Z_{\frac{n}{d}}$. For each $r^{-1}(rd) \in (rd)$, there exists $r^{-1}d \in (d)$ such that $g(r^{-1}d) = r(r^{-1}d) = (rr^{-1})d\ = d$.

This shows that g is onto function.

Thus there exists a bijection between (d) and (rd), when $\left(r,\ \frac{n}{d}\right) = 1$. This implies that $|(d)| = |(rd)|$, we have $(rd) \subset (d)$ in the ring Z_n and hence by the Theorem 5, $(d) = (rd)$.

Corollary 2. For any non-trivial divisor d of n and for two distinct elements x and y in $S_d{}'$ of Z_n, we have $(x) = (y)$.

Proof. From the definition of $S_d{}'$, $S_d{}' = \{rd \in Z_n\colon \left(r,\ \frac{n}{d}\right) = 1,\ 1 \le r < \frac{n}{d}\}$ and from Theorem 5, $(d) = (rd)$, for all rd in $S_d{}'$ and for any non-trivial divisor d of n. This implies that the proof follows.

Theorem 7. For any non-trivial divisor d of n, we have $S_d = S_d{}'$.

Proof. We know that $S_d\ = \{rd \in Z_n\colon (rd) = (d),\ 1 \le r < \frac{n}{d}\}$ and
$S_d{}' = \{rd \in Z_n\colon \left(r,\ \frac{n}{d}\right) = 1,\ 1 \le r < \frac{n}{d}\}$.

Clearly, from the Corollary 2, we have $S_d{}' \subseteq S_d$. Now we prove that the another inclusion $S_d \subseteq S_d{}'$. For this let $x \in S_d$, then there exists r, $1 < r < \frac{n}{d}$ such that $x = rd$. Now, it is enough to show that $x \in S_d{}'$. If possible, assume that $x \notin S_d{}'$.

$\Rightarrow\quad \left(r,\ \frac{n}{d}\right) \neq 1.$

$\Rightarrow\ (rd,\ n) \neq d.$

$\Rightarrow\quad (rd) \subset (d),$

which contradicts to the fact that $(rd) = (d)$. This implies that our assumption is not true. Hence $S_d = S_d{}'$.

Theorem 8. For any non-trivial divisor d of n, the cardinality of the set S_d in the ring Z_n is $|S_d| = \varphi\left(\frac{n}{d}\right)$.

Proof. By the definition, S_d and $S_d{}'$ are two non-empty subsets of Z_n and by the Theorem 7, S_d and $S_d{}'$ are equivalent. So, each element $rd \in \{0,\ 1,\ 2,\ \dots,\ n-1\}$ has a unique highest common factor with n and therefore belongs to one and only one of the sets S_d. This means that the subsets S_d's forms a partition of $Z(Z_n)^*$.

Now, by the definition of S_d, we have $s \in S_d{}'$ if and only if $(s,\ n) = d$ if and only if $(rd,\ n) = d$, where $s = rd$ if and only if $\left(r,\ \frac{n}{d}\right) = 1$, $1 \leq r < \frac{n}{d}$. Therefore, the number of elements in S_d is equal to the number of elements to r, which is relatively prime to $\frac{n}{d}$ and this is equal to $\varphi\left(\frac{n}{d}\right)$.

Example 3. In the ring Z_8, $D = \{2,\ 4\}$.

- For $d = 2$, we have $|S_2| = \varphi\left(\frac{8}{2}\right) = 2$, because 2 and 6 are two elements in S_2 such that $(2) = (6)$.
- For $d = 4$, we have $|S_4| = \varphi\left(\frac{8}{4}\right) = 1$, because 4 is the only element in S_4.

Example 4. In the ring Z_{24}, $D = \{2,\ 3,\ 4,\ 6,\ 8,\ 12\}$.

- For $d = 2$, we have $|S_2| = \varphi\left(\frac{24}{2}\right) = 4$, because $2,\ 10,\ 14$ and 22 are four elements in S_2 such that $(2) = (10) = (14) = (22)$.
- For $d = 3$, we have $|S_3| = \varphi\left(\frac{24}{3}\right) = 4$, because $3,\ 9,\ 15$ and 21 are four elements in S_3 such that $(3) = (9) = (15) = (21)$.
- For $d = 4$, we have $|S_4| = \varphi\left(\frac{24}{4}\right) = 2$, because 4 and 20 are two elements in S_4 such that $(4) = (20)$.
- For $d = 6$, we have $|S_6| = \varphi\left(\frac{24}{6}\right) = 2$, because 6 and 18 are two elements in S_6 such that $(6) = (18)$.
- For $d = 8$, we have $|S_8| = \varphi\left(\frac{24}{8}\right) = 2$, because 8 and 16 are two elements in S_8 such that $(8) = (16)$.
- For $d = 12$, we have $|S_{12}| = \varphi\left(\frac{24}{12}\right) = 1$, because 12 is the only element in S_{12}.

4. Algorithm

In this section, we present an algorithm for enumerating the sets of all non-unit elements in Z_n whose principal ideals are equal.

4.1 Algorithm

Step 1. *Start*
Step 2. *Read input n*
Step 3. *Initialize i, j, k, s, s1, r, t, super [500] [500]*
Step 4. $i \leftarrow 2$
Step 5. $j \leftarrow 1$
Step 6. $r \leftarrow i * j$
Step 7. $s \leftarrow r \ (mod\ n)$
Step 8. *If (s=0) then goto step 9 else step 18*
Step 9. *Super [j] [n]* $\leftarrow j$
Step 10. $k \leftarrow 1$
Step 11. $t \leftarrow j*k$
Step 12. $s1 \leftarrow t \ (mod\ n)$
Step 13. *If (s1=0) then goto step 15 else goto step 14*
Step 14. *Super [j] [s1]* $\leftarrow s1$
Step 15. *If (k < n) then goto step 16 else goto step 18*
Step 16. $k \leftarrow k+1$
Step 17. *Goto step 11*
Step 18. *If (j < n) then goto step 19 else goto step 21*
Step 19. $j \leftarrow j+1$
Step 20. *Goto step 6*
Step 21. *If (i < n) then goto step 22 else goto step 24*
Step 22. $i \leftarrow i+1$
Step 23. *Goto step 5*
Step 24. *Print principal ideals*
Step 25. *End.*

Subroutine algorithm

Step 1. *Start*
Step 2. $j \leftarrow 0$
Step 3. *If (super [j] [n]=0) then goto step 11 else goto step 4*
Step 4. *Print super [j] [n]*
Step 5. $i \leftarrow 0$
Step 6. *If (super [j] [i]=0) then goto step 8 else goto step 7*
Step 7. *Print super [j] [i]*
Step 8. *If (i < 0) then goto step 9 else goto step 11*
Step 9. $i \leftarrow i+1$
Step 10. *Goto step 6*
Step 11. *If (j < n) then goto step 12 else goto step 14*
Step 12. $j \leftarrow j+1$
Step 13. *Goto step 3*
Step 14. *End.*

4.2 Outputs

In this section, we gave the outcome results when we run the program in C-language for various values of n, which is based on the above Algorithm.

- For given number $n = 10$, then the outcomes are

(5),
(2)=(4)=(6)=(8),
Principal ideal(2)={0,2,4,6,8},
Principal ideal(4)={0,2,4,6,8},
Principal ideal(5)={0,5},
Principal ideal(6)={0,2,4,6,8},
Principal ideal(8)={0,2,4,6,8}.

That is, in the ring Z_{10}, $2, 4, 5, 6$ and 8 are non-unit elements such that $(2) = (4) = (6) = (8)$ and (5) is a different set.

- For given number $n = 16$, then the outcomes are

(8),
(4)=(12),
(2)=(6)=(10)=(14).
Principal ideal(2)={0,2,4,6,8,10,12,14},
Principal ideal(4)={0,4,8,12},
Principal ideal(6)={0,2,4,6,8,10,12,14},
Principal ideal(8)={0,8},
Principal ideal(10)={0,2,4,6,8,10,12,14},
Principal ideal(12)={0,4,8,12},
Principal ideal(14)={0,2,4,6,8,10,12,14}.

That is, in the ring Z_{16}, $2, 4, 6, 8, 10, 12$ and 14 are non-unit elements such that $(2) = (6) = (10) = (14)$, $(4) = (12)$ but (8) is only a different set.

Similarly, we found the sets of non-unit elements whose principal ideals are equal for large values of n also.

5. Conclusions

In this paper, we discussed the number theoretic properties of non-unit elements of a finite ring Z_n in different forms of n. The set of non-trivial divisors of n were divided into two disjoint sets ($i.e. D = D_1 \cup D_2$ and $D_1 \cap D_2 = \emptyset$). The results were obtained by using these two sets for different characterizations of n. Also, the cardinality of non-unit elements of Z_n were enumerated whenever their corresponding principle ideals were equal. Finally, the results were verified with suitable examples by using algorithm of C-program.

Acknowledgements

The authors wish to express their cordial thanks to the reviewers for their excellent suggestions and also thanks to Sri K. Muralidhar Naidu for valuable suggestions to improve presentation of this paper.

References

[1] Nathanson, M. B. (1980). Connected components of arithmetic graphs. *Monatshefte für mathematik*, *89*(3), 219-222.
[2] Apostol, T. M. (1989). *Introduction to analytic number theory*. Springer International Student Edition.
[3] Beck, I. (1988). Coloring of commutative rings. *Journal of algebra, 116*, 208-226.
[4] Anderson, D. F., & Livingston, P. S. (1999). The zero-divisor graph of a commutative ring. *Journal of algebra*, *217*(2), 434-447.
[5] Bhattacharya, P. B., Jain, S. K., & Nagpaul, S. R. (1994). *Basic abstract algebra*. Cambridge University Press.
[6] Hungerford, T. W. (2012). *Abstract algebra: an introduction*. Cengage Learning.
[7] Nathanson, M. B. (2008). *Elementary methods in number theory* (Vol. 195). Springer Science & Business Media.

Appendix

Here, we present a program in C-language for finding the sets of all non-unit elements in Z_n whose principal ideals are equally generated in Z_n along with their corresponding principal ideals, for various values of n.

```
#include <dirent.h>
#include <stdio.h>
#include <errno.h>
#include <string.h>
main ( int argc, char *argv[] )
{         get_zero_div(atoi(argv[1]));
}
get_zero_div( int p )
{ char zdiv[1000], pidl[1000], super[1000][1000], test;
        int i, j, k, r, s, t, c, m=0, n=2, cnt=0, key;
        for (  i=0; i<1000; i++ )
        zdiv[i]='N';
        for ( i=0; i<1000; i++)
        pidl[i] = 'N';
        for ( i=2; i<p; i++ )
             {
             for ( j=2; j<p; j++ )
                  {
                      r = I * j ;
                      s = ( r % p );
                      if ( s==0 )
```

```
                    {       zdiv[i] = 'Y';
                            zdiv[j] = 'Y';
        }
                }
              }
for ( i=0; i<1000; i++ )
{
        super [i][0] = -1;
        super [i][1] = -1;
}
For ( i=0; i<p; i++ )
{
        If ( zdiv[i] == 'Y' )
{
 super [m][n] = i;
 n++;
      {
        for ( j=1; j<p; j++ )
               { t = I * j;
                 s = (t % p);
                 if ( s == 0 )
                    {
                     break;
                    }
                 pidl[s] = 'Y';
               }
      }
for ( k=0; k<p; k++ )
{
      if ( pidl [k] == 'Y' )
         {
        super[m][n] = k;
        super[m][1]++;
        n++;
        }
}
        super[m][1]++;

        for ( k=0; k<1000; k++ )
        pidl[k] = 'N';
m++;
n=2;
}
}
for (i=0; i<1000; i++ )
if ( super[i][1] == -1 )
   break;
   cnt = i;
for ( i=0; i<=cnt; i++ )
      { super[i][0] = (i+1);
        key = super[i][1];
```

```
        for ( j=0; j<=cnt; j++ )
          { test = 'N';
           If ( super[j][1] == key )
              {
                 for ( k=2; k<=key+2; k++ )
                 if ( super[i][k] == super[j][k] )
                 test = 'Y';
                 else
                 test = 'N';
              }
               If ( test == 'Y' )
               super[j][0] = i+1;
         }
        }
for ( i=0; i<=cnt; i++ )
{ test = 'N';
  { for ( j=0; j<=cnt; j++ )
    if ( super[j][0] == I )
      {
       printf( "(%d) = ", super[j][2]);
       test='Y';
      }
    If ( test == 'Y' )
    printf ( "\n" );
  }
}
printf ( "\n" );
for ( i=0; i<1000; i++)
     {
       for ( j=2; j<1000; j++ )
          {
           if ( (super[i][j])! = 0 )
              {
               if ( j == 2 )
               printf ( "Principal ideal(%d) = {0,",super[i][j] );
               else
               printf ( "%d,", super[i][j] );
        }
        if ( super[i][j] == 0 )
               {
                 printf ( "}\n" );
                 break;
               }
           }
        if ( super[i][2] == 0 )
         { printf ( "\n" );
          break;
         }
     }
}
```