Journal of New Theory
ISSN: 2149-1402

36 (2021) 64-74
Journal of New Theory
https://dergipark.org.tr/en/pub/jnt
Open Access

Enumeration of Involutions of Finite Rings

Chalapathi Tekuri [1], **Sajana Shaik** [2]

Article History
Received: 15 Jul 2021
Accepted: 14 Sep 2021
Published: 30 Sep 2021
10.53570/jnt.971924
Research Article

Abstract – In this paper, we study a special class of elements in the finite commutative rings called involutions. An involution of a ring R is an element with the property that $x^2 - 1 = 0$ for some x in R. This study describes both the implementation and enumeration of the involutions of various rings, such as cyclic rings, non-cyclic rings, zero-rings, finite fields, and especially rings of Gaussian integers. The paper begins with simple well-known results of an equation $x^2 - 1 = 0$ over the finite commutative ring R. It provides a concrete setting to enumerate the involutions of the finite cyclic and non-cyclic rings R, along with the isomorphic relation $I(R) \cong Z_2^k$.

Keywords – *Cyclic rings, noncyclic rings, zero rings, finite fields, involutions*

Mathematics Subject Classification (2020) – 16W10, 11K65

1. Introduction

In this paper, R denotes a commutative finite ring with unity. We call that a nonzero element u in R is a unit if there is some $x \in R$ such that $ux = 1$. When such an element x exists, it is called the multiplicative inverse of u and denoted by $x = u^{-1}$. The collection of units of the ring R is denoted by $U(R)$. However, $U(R)$ is a multiplicative group concerning the multiplication defined on the ring R. If R is a finite field, then $U(R)$ is a cyclic group. If the unit group $U(R)$ of R is cyclic, then $U(R)$ is finite. The order of R and the order of its group of units will be denoted by $|R|$ and $|U(R)|$, respectively. In the case when $R = Z_n$, $|U(R)| = \varphi(n)$, where $\varphi(n)$ is Euler's phi-function, the number of positive integers less than n and relatively prime to n. If $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ is the decomposition of n into product of distinct prime powers, then $\varphi(n) = n \prod_{p|n}(1 - 1/p)$. It is well known that if a finite commutative ring with unity R decomposes as a direct product $R = R_1 \times R_2 \times \dots \times R_k$, then its group of units decomposes naturally as a direct product of groups. That is, $U(R)$ is isomorphic to $U(R_1) \times U(R_2) \times \dots \times U(R_k)$. The symbol $\cong$ will be used for both ring and group isomorphism. Note that if two rings R and $R'$are isomorphic, $R \cong R'$, then their group of units is isomorphic, $U(R) \cong U(R')$. Since the number of units of Z_n is $|U(Z_n)| = \varphi(n)$ and the number of units in the ring $Z_m \times Z_n$ is $\varphi(m)\varphi(n)$, but in general $\varphi(mn) \neq \varphi(m)\varphi(n)$ for some $m, n \geq 1$. If R is a finite field, then $U(R)$ is a cyclic group. Otherwise, $U(R)$ is an abelian group but not cyclic. If the unit group $U(R)$ of R is cyclic, then $U(R)$ is finite and $|U(R)|$ must be an even number.

[1]chalapathi.tekuri@gmail.com; [2]ssajana.maths@gmail.com (Corresponding Author)
[1]Department of Mathematics, Sree Vidyanikethan Eng. College, Tirupathi, India
[2]Department of Mathematics, P.R. Government College(A), Kakinada, India

Up to isomorphism, there is a unique cyclic group $C_n = \{1, a, a^2, \dots, a^{n-1} : a^n = 1\} = \langle a \rangle$ of order n. But the fundamental theorem of finite abelian groups states that any finite non cyclic abelian group G is isomorphic to a direct product of cyclic groups $C_{n_1}, C_{n_2}, \dots, C_{n_k}$. That is, $G \cong C_{n_1} \times C_{n_2} \times \dots \times C_{n_k}$. Hence, the group of units of a finite commutative ring with unity is isomorphic to a direct product of cyclic groups. For instance, $U(Z_m \times Z_n) \cong U(Z_{mn})$ if and only if $(m, n) = 1$ if and only if $\varphi(mn) = \varphi(m)\varphi(n)$. The problem of classifying the group of units of an arbitrary finite commutative ring with identity is an open problem. However, the problem is solved for certain classes. In the case when $R = Z_n$, its group of units $U(Z_n)$ is characterized by using the following, see [1].

The group of units of the ring Z_n when n is a prime power integer is given by

(1) $U(Z_2) \cong C_1$,

(2) $U(Z_4) \cong C_2$,

(3) $U(Z_{2^k}) \cong U(Z_2) \times U(Z_{2^{k-1}})$, for every $k > 1$. For instance, $U(Z_8) \cong U(Z_2) \times U(Z_4)$. For every prime p, we have $U(Z_{p^\alpha}) \cong C_p \times C_{p^{\alpha-1}}$.

Cross [2] gave a characterization of the group of units of $Z[i]/\langle\alpha\rangle$, where $Z[i]$ is the ring of Gaussian integers and α is an element in $Z[i]$. Smith and Gallian [3] solved the problem when $R = F[i]/\langle f(x)\rangle$ where F is a finite field and $f(x)$ is an irreducible polynomial over F. The related problem of determining the cyclic groups of units for each of the above classes of rings is completely solved. It is well known that $U(Z_n)$ is a cyclic group if and only if $n = 2,4, p^\alpha$ or $2p^\alpha$, where p is an odd prime integer. In [2], Cross showed that the group of units of $Z[i]/\langle\alpha\rangle$ is a cyclic group if and only if (1) $\alpha = (1+i)^k$, where $k = 1,2,3$ and (2) $\alpha = p, (1+i)p$, where p is a prime integer of the form $4k+3$ and α is a Gaussian prime such that $\alpha\bar{\alpha}$ is a prime integer of the form $4k+1$. The problem of determining all quotient rings of polynomials over a finite field with a cyclic group of units was solved by El-Kassar et al., see [4]. For more details about the unit groups and their corresponding properties, we refer to the work [5-6].

A ring R is called cyclic if $(R, +)$ is a cyclic group. In [7], the author Buck proved that every cyclic ring is a commutative and commutative finite cyclic ring with unity is isomorphic to the ring Z_n. Further, a ring $(R^0, +, \cdot)$ is a zero ring [8], if $ab = 0$ for every, $a, b \in R^0$, where '0' is the additive identity in R^0. For any finite commutative cyclic ring R without unity, we have $R \cong R^0$ and hence $U(R^0) = \phi$. Let B be a finite Boolean ring with unity, then $b^2 = b$ for every $b \in B$. If $B \cong Z_2$, then B is a Boolean ring with two elements 0,1 and $B^n = B \times B \times \dots \times B$ is a Boolean ring with 2^nelements, and clearly $|U(B^n)| = 1$.

The purpose of this paper is to enumerate the involutions in the group of units of a finite commutative ring with unity and to examine the properties of the involutions in a group of units. For this first, we shall define involutions in various fields of mathematics and their other related fields. Generally, in mathematics and other related fields, involution is a function f and it is equal to its inverse. This means that $f(f(x)) = x$ for all x in the domain of f. So, the involution is a bijection. For this reason, many fields in modern mathematics contain the term involution such as Group theory, Ring theory, and Vector spaces. Moreover, in the Euclidean and the Projective geometry, the involution is a reflection through the origin, and an involution is a projectivity of period 2, respectively. In mathematical logic, the operation of complement in Boolean algebra is called involution, and in classical logic, the negation that satisfies the law of double negation is called involution. Finally, in Computer science, the XOR bitwise operation with a given value for one parameter is also an involution, and RC4 cryptographic cipher is involution, as encryption and decryption operations use the same function. Recently in [9], the authors Fakieh and Nauman studied involutions and their minimalities of Reversible Rings. For further representations of involutions of various rings, the reader refers [10-13].

2. Properties of Involutions of Rings

Throughout this section, we are interested in involutions that have a special property in the elements of rings. Also, this section provides a useful theory that can be used to help to find solutions of equations of the form $x^2 = 1$, where 1 is the multiplicative unity of R.

Definition 2.1. An element u in a finite ring R with unity 1 is called an involution of R if $u^2 = 1$ where 1 is the unity of R. We denote it with $I(R)$, the set of all involutions of R. In particular, $I(R) \subseteq U(R) \subset R$.

For instance, 4 and 6 are the involutions of the ring $R = \{0,2,4,6,8\}$ with unity 6 modulo 10. When the cyclic ring $R = Z_n$, for a given positive integer n, we will use the symbol I_n to denote the set of all involutions of the ring Z_n and we will call it the set of involutions modulo n. For instance, $I_3 = \{1,2\}$, $I_8 = \{1,3,5,7\}$ and $I_{10} = \{1,9\}$. For any finite cyclic ring R with unity and finite zero rings R^0, we have $I(R) \neq \phi$ and $I(R^0) = \phi$. But we can simply verify that I_n is a subgroup of $U(Z_n)$. This is a basic property for the ring R with an abelian unit group $U(R)$. Now we show that $I(R)$ is a subgroup of $U(R)$.

Theorem 2.2. Let R be a commutative ring with unity. Then, $I(R)$ is a subgroup of $U(R)$.

Proof. Since $I(R)$ is a nonempty subset of $U(R)$. It is sufficient to prove that if $u, v \in I(R)$, then $uv^{-1} \in I(R)$. Indeed, if $u^2 = 1$ and $v^2 = 1$, then clearly $(uv^{-1})^2 = u^2(v^{-1})^2 = u^2(v^2)^{-1} = 1$. □

Example 2.3. Let us take the ring $R = Z_5$. Then, $I(R) = \{1,4\}$ and $U(R) = \{1,2,3,4\}$. This clearly shows that $I(R)$ is a subgroup of $U(R)$.

Here, we recall that the Cartesian product of two rings and the results about these rings. For a complete treatment of these rings, see [1]. Let R and S be any two rings. Then, $(R \times S, +, \cdot)$ is again a ring concerning the component-wise addition and component-wise multiplication: $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b)(c, d) = (ac, bd)$, for every $(a, b), (c, d) \in R \times S$. It is well known that $(1_R, 1_S) \in R \times S$ if and only if $1_R \in R$ and $1_S \in S$. Also, Z_{mn} is not isomorphic to $Z_m \times Z_n$ if and only if $gcd(m, n) \neq 1$. In general, the following result is well known in the literature for $U(R)$ and $U(S)$.

Theorem 2.4. If R and S are commutative rings with unity, then $U(R \times S) = U(R) \times U(S)$.

Proof. Since $(1_R, 1_S) \in R \times S$. For $(u, v) \in U(R \times S)$, there exists $(u^{-1}, v^{-1}) \in U(R \times S)$ such that

$$\begin{aligned}(u, v)(u^{-1}, v^{-1}) = (1_R, 1_S) \quad &\Leftrightarrow (uu^{-1}, vv^{-1}) = (1_R, 1_S) \\ &\Leftrightarrow uu^{-1} = 1_R\end{aligned}$$

for some $u^{-1} \in R$ and $vv^{-1} = 1_S$ for some $v^{-1} \in S \Leftrightarrow u \in U(R)$ and $v \in U(S) \Leftrightarrow (u, v) \in U(R) \times U(S)$. Therefore, $U(R \times S) = U(R) \times U(S)$. □

Example 2.5. Let $R = Z_2$ and $S = Z_3$. Then, $R \times S = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$, $U(R) = 1$, and $U(S) = \{1,2\}$. Also, $U(R \times S) = \{1\} \times \{1,2\} = \{(1,1), (1,2)\}$ and $U(R) \times U(S) = \{(1,1), (1,2)\}$.

By Theorem 2.4, the following remark is obvious.

Remark 2.6. For any ring R, we have $I(R) = I(U(R))$.

The strategy is then to express $I(R \times S)$ in terms of $I(R)$ and $I(S)$. It is essential for finding the number of involutions in a finite commutative ring with unity.

Theorem 2.7. For any finite cyclic rings R and S with unity, then we $I(R \times S) = I(R) \times I(S)$.

Proof. Let R be a commutative ring with unity 1_R and S be a commutative ring with unity 1_S. Then by the Theorem 2.2 and Theorem 2.4, $I(R) \subseteq U(R)$, $I(S) \subseteq U(S)$ and $I(R \times S) \subseteq U(R \times S)$. This implies that $I(R) \times I(S)$ is a non-empty subset of $U(R) \times U(S)$.

First, we have to prove that $I(R \times S) \subseteq I(R) \times I(S)$. For any $(r, s) \in R \times S$, if $(r, s) \in I(R \times S)$ then $(r, s)^2 = (1,1)$, or $(r^2, s^2) = (1,1)$. This is the same as $r^2 = 1$ and $s^2 = 1$. Consequently, $r \in I(R)$ and $s \in I(S)$. Therefore, $(r, s) \in I(R) \times I(S)$. Thus $I(R \times S) \subseteq I(R) \times I(S)$. Similarly, we can show that $I(R) \times I(S) \subseteq I(R \times S)$. Hence, by the set inclusions, $I(R \times S) = I(R) \times I(S)$. □

Example 2.8. Let $R = Z_2$ and $S = Z_3$. Then, $R \times S = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$, $I(R) = \{1\}$, and $I(S) = \{1,2\}$. Therefore, $I(R \times S) = \{(1,1), (1,2)\} = I(R) \times I(S)$.

We will denote with $|I(R)|$, the number of involutions of R. Particularly, if the ring $R = Z_n$, the number $|I_n|$ will represent the number of involutions modulo n. We now state and prove the basic theorem for the involutions of R that shows that the number $|I(R)| > 1$ is even.

Theorem 2.9. For any finite commutative ring R with $|I(R)| > 1$, then $|I(R)|$ is even.

PROOF. Let $u \in I(R)$ and $|I(R)| > 1$. Then, $u^2 = 1$, and $|u|$ divides 2. This implies that $|u| \in \{1,2\}$. By the consequence of Lagrange's theorem [1] for finite groups, $|u||I(R)|$. Therefore, for some positive integer q, $|I(R)| = |u|q$. Suppose $|u| = 1$. Then, clearly $u = 1$, because $u^2 = 1$. So, our assumption $|u| = 1$ is not true. Thus, for every unit $u \neq 1$ in $I(R)$, we have $|u| = 2$. Hence, $|I(R)| = 2q$. This concludes that $|I(R)|$ must be even. □

We observe that $|I(R)|$ is even except $R \cong B^n$, as the following remark illustrates how Theorem 2.9 is applicable.

Remark 2.10. If R is a finite cyclic ring with unity and $|I(R)|$ is an odd number, then it must be equal to one, that is $I(R) = \{1\}$. If $|R| > 2$ and $R \ncong R^0, B^n$ then either $|I(R)| = 1$, or $|I(R)|$ must be even. For instance, $R = \frac{Z_2[x]}{(x^3+1)}$ and $R' = \frac{Z_2[x]}{(x^3+x)}$ are both commutative rings with unity 1, so $I(R) = \{1\}$ and $I(R') = \{1,1 + x + x^2\}$.

Before we proceed, we need to solve the equation $x^2 - 1 = 0$ over the ring R with unity. Note that if $Char(R) = 2$, and then the set of solutions of $x^2 - 1 = 0$ is the same as the set of solutions of $x^2 + 1 = 0$ and vice versa. If $Char(R) \neq 2$, then $x^2 + 1 = 0$ contains either finite or infinite number of solutions over R. In [14], the authors Khanna and Bhambri proved that the equation $x^2 + 1 = 0$ has an infinite number of solutions over the ring of Quaternions. Recently, Suzanne discussed and described the solution of $x^2 + 1 = 0$ in [15]. For finite fields, the following result is well known.

Theorem 2.11. Let F be a finite field with unity 1 and $x^2 = 1$ for some $x \in F$. Then, $x = \pm 1$, in particular, $|I(F)| = 2$.

PROOF. Assume F is a finite field with unity 1 and $x^2 = 1$ over F. Then, algebraically $x^2 - 1 = 0$ implies that $(x - 1)(x + 1) = 0$. If both $(x - 1) \neq 0$ and $(x + 1) \neq 0$, then they are both zero-divisors of F. But F has no zero-divisors because every field is an integral domain. So, either $x - 1 = 0$, or $x + 1 = 0$ for some $x \in F$, so that either $x = 1$, or $x = -1$. Hence, $|I(F)| = 2$. □

Example 2.12. Let $F = \{0,2,4,6,8\}$. Then, $(F, +_{10}, \times_{10})$ is a field with unity 6 and the set of involutions $I(F) = \{4,6\}$.

Now we consider the solutions of the equation $x^2 - 1 = 0$ over the finite commutative ring R. For this, we need to consider two cases, i.e., (i) $U(R)$ is a cyclic group and (ii) $U(R)$ is a non-cyclic group.

Before getting started for the enumeration of involutions, we need to recall two familiar theorems from finite group theory.

Theorem 2.13 (Fundamental theorem of cyclic groups) [1]**.** Every subgroup of a cyclic group is cyclic.

Theorem 2.14 (Fundamental theorem of finite abelian groups) [1]**.** Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.

Theorem 2.15. Let R be a finite cyclic ring with unity 1. Then, $U(R)$ is a cyclic group if and only if $|I(R)| = 2$.

PROOF. Let x be a generator of a finite cyclic group $U(R)$. Then, $U(R) = \langle x \rangle$. Because of $I(R) \subseteq U(R)$, every involution u in $I(R)$ can be written as $u = x^m$ for some positive integer m, $1 \leq m \leq |U(R)|$. Therefore,

$$\begin{aligned} u^2 = 1 &\Leftrightarrow (x^m)^2 = 1 \\ &\Leftrightarrow x^{2m} = 1 \\ &\Leftrightarrow 2m \equiv 0(mod|U(R)|) \end{aligned}$$

Because of $gcd(2, |U(R)|) = 2$, this linear congruence has exactly two solutions. Hence, $|I(R)| = 2$ if and only if $U(R)$ is cyclic. □

Example 2.16. Let us take the ring $R = Z_5$. Then, $I(R) = \{1,4\}$ and $U(R) = \{1,2,3,4\}$. Clearly, $U(R) =< 2 >=< 3 >$ is a cyclic group, and $|I(R)| = 2$.

Theorem 2.17. Let $U(R)$ be the unit group of a finite cyclic ring R with unity 1. For some $k > 1$, $U(R)$ is a non-cyclic group if and only if $|I(R)| = 2^k$.

PROOF. By Theorem 2.14, the finite abelian non-cyclic group $U(R)$ is isomorphic to the direct product of cyclic groups of prime power order. Suppose that the prime factorization of $|U(R)|$ is $p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$, where each p_i is a distinct prime and $k \geq 2$. Then, clearly there exist cyclic groups $U\left(Z_{p_1^{a_1}}\right), U\left(Z_{p_2^{a_2}}\right), \dots, U\left(Z_{p_k^{a_k}}\right)$ of prime power orders such that

$$\begin{aligned} U(R) \cong U\left(Z_{p_1^{a_1}}\right) \times U\left(Z_{p_2^{a_2}}\right) \times \dots \times U\left(Z_{p_k^{a_k}}\right) &\Rightarrow I(U(R)) \cong I\left(U\left(Z_{p_1^{a_1}}\right) \times U\left(Z_{p_2^{a_2}}\right) \times \dots \times U\left(Z_{p_k^{a_k}}\right)\right) \\ &\Rightarrow I(U(R)) \cong I\left(U\left(Z_{p_1^{a_1}}\right)\right) \times I\left(U\left(Z_{p_2^{a_2}}\right)\right) \times \dots \times I\left(U\left(Z_{p_k^{a_k}}\right)\right) \end{aligned}$$

In view of the Remark 2.6 and the Theorem 2.7, we have $I(R) \cong I\left(Z_{p_1^{a_1}}\right) \times I\left(Z_{p_2^{a_2}}\right) \times \dots \times I\left(Z_{p_k^{a_k}}\right)$. From the Theorem 2.15, $U\left(Z_{p_i^{a_i}}\right)$ is a cyclic group and hence $I\left(Z_{p_i^{a_i}}\right) = \left|I\left(U\left(Z_{p_i^{a_i}}\right)\right)\right| = 2$. Therefore, the number of Involutions of a finite cyclic ring R is equal to $|I(R)|$. Clearly, $|U(R)| = p_1^{a_1}p_2^{a_2} \dots p_k^{a_k}$, we have $|I(R)| = \left|I\left(Z_{p_1^{a_1}}\right)\right| \left|I\left(Z_{p_2^{a_2}}\right)\right| \dots \left|I\left(Z_{p_k^{a_k}}\right)\right| = 2.2 \dots 2$ (k times) $= 2^k$. □

Example 2.18. Let the ring $R = Z_8$. Then $U(R) = I(R) = \{1,3,5,7\}$ and therefore $U(R)$ is a non-cyclic and $|I(R)| = 4$.

3. Properties of Involutions of Rings

In the previous section, we studied the properties of the set of involutions of finite commutative rings, particularly, finite cyclic rings. A specifically appealing of elementary number theory is that many fundamental properties of the positive integers relating to their primality, divisibility, and factorization can be carried over to the other sets and algebraic structures of numbers. In this section, we study the set of involutions of Gaussian integers modulo n, complex numbers of the form $a + ib$, where a and b are integers modulo n and $i^2 = -1$. We introduce the concept of Gaussian involution and establish the basic properties of Gaussian involutions over addition and multiplication of complex integers over modulo n.

For any positive integer $n \geq 1$, $< n >$ be the proper principal ideal generated by n in the infinite ring of Gaussian integers $Z_n[i]$. So there exists a quotient ring $Z_n[i]/\langle n \rangle$. In [16], the authors Dresden and Dymacek proved that $Z_n[i]/\langle n \rangle$ is isomorphic to $Z_n[i]$, the ring of Gaussian integers modulo n with unity $1 = 1 + i0$ where $n > 1$. If $n = 1$, then $Z_n[i] = \{0 + i\,0\}$. When $R = Z_n[i]$, for given positive integer $n > 1$, we will use the symbols $U_n[i]$, $I_n[i]$ to denote the set of units and involutions of the ring $Z_n[i]$, and call it the set of all Gaussian units and Gaussian involutions modulo n, respectively. It is well known that $|Z_n[i]| = n^2$ and $Z_n[i]$ is a field if and only if $n \equiv 3(mod\ 4)$ and also for more information about $Z_n[i]$, see [1]. First, we prove that

the basic property of the ring $Z_n[i]$, it indicated that $Z_n[i]$ is not a cyclic ring. First, we notice that $Z_n[i] = \{0\}$ if and only if $n = 1$. Consequently, the following theorem is true for $n > 1$.

Theorem 3.1. The ring $Z_n[i]$ of Gaussian integers modulo n is not a cyclic ring.

PROOF. We use proof by contradiction. Suppose $Z_n[i]$ is a cyclic ring for some values of n. Then there exists an element $\alpha = a + bi \in Z_n[i]$ such that $Z_n[i] =< \alpha >$ with respect to the addition of Gaussian integers modulo n. Now we have reached a contradiction. Note that $c + di \in Z_n[i]$ implies there exists a positive integer m such that

$$\begin{aligned} c + di = m(a + bi)(mod\, n) \quad &\Rightarrow ma \equiv c(mod\, n) \text{and } mb \equiv d(mod\, n) \\ &\Rightarrow Z_n = \langle a \rangle \text{ and } Z_n = \langle b \rangle \\ &\Rightarrow Z_n \times Z_n = \langle a \rangle \times \langle b \rangle \\ &\Rightarrow Z_n \times Z_n = \langle (a, b) \rangle \end{aligned}$$

This implies that the ring $Z_n \times Z_n$ is generated by the element (a, b) and thus $Z_n \times Z_n$ is a cyclic group with a generator (a, b) under addition modulo n, which is a contradiction to the fact that $Z_n \times Z_n$ is not a cyclic group for addition modulo n. This completes the proof. □

It is well known that a Diophantine equation is a polynomial equation for which you seek integer solutions, see [17]. For example, the Pythagorean triples (a, b, c) are positive integer solutions to the equation $a^2 + b^2 = c^2$. Here is another Diophantine equation $a^2 - b^2 = 1$ over the infinite ring of integers $\mathbb{Z}$ to the usual addition and multiplication of integers. According to the literature survey of algebraic equations, there are no positive integer solutions to the Diophantine equation $a^2 - b^2 = 1$ over the ring Z. But we observe that there exist integer solutions over the finite ring Z_n. For instance, the pair $(3, 4)$ satisfies the equation $a^2 - b^2 = 1$ over the ring Z_8. The identity $(a + bi)^2 = 1$ is true over the ring $Z_n[i]$ if and only if $a^2 - b^2 = 1$ and $2ab = 0$ over modulo n.

Now we are going to study basic properties of Gaussian involutions $I_n[i]$ and next investigate the cardinality of $I_n[i]$ for various values of n.

Definition 3.2. A Gaussian integer $a + ib$ in $Z_n[i]$ is called a Gaussian unit if $a^2 + b^2 \in U_n$ and the set of Gaussian units $Z_n[i]$ is $U_n[i]$. For example, $U_2[i] = \{1, i\}$.

Properties 3.3. The set $U_n[i]$, the collection of Gaussian units in $Z_n[i]$ has the following basic properties.

i. $U_n \subset U_n[i]$ for every $n > 1$.

ii. If $a + ib$ is a Gaussian unit in, then $Z_n[i]$ then $b + ia$ is also a Gaussian unit in $Z_n[i]$.

iii. If $u, v \in U_n$, then $u + iv$ may not be in $U_n[i]$.

iv. For any odd prime p, $p \not\equiv 3(mod\, 4)$, the unit group U_p is cyclic but $U_p[i]$ may not be cyclic.

Example 3.4.

i. For the rings Z_2 and $Z_2[i]$, the corresponding sets of units are $U_2 = \{1\}$ and $U_2[i] = \{1, i\}$. So that clearly $U_2 \subset U_2[i]$.

ii. In the ring $Z_3[i]$, $1 + 2i$ and $2 + i$ are both Gaussian units.

iii. 1 is a unit in U_4, but $1 + i$ is not a unit in $U_4[i]$.

iv. For the prime $p = 5$, the unit group U_5 is cyclic but $U_5[i]$ may not be cyclic.

Definition 3.5. A Gaussian unit $\alpha = a + ib$ is called a Gaussian involution modulo n if $\alpha^2 = 1$. The set of all Gaussian involutions modulo n is denoted by $I_n[i]$, with cardinality $|I_n[i]|$. For example, $|I_2[i]| = |\{i, 1\}| = 2$, $|I_3[i]| = |\{1,2\}| = 2$, and $|I_4[i]| = |\{1,1 + 2i, 3,3 + 2i\}| = 4$.

To determine the structure of the group $I_n[i]$, we must first derive a relation for determining when an element of $I_n[i]$ is a Gaussian involution. Recall that in a finite commutative ring R, a nonzero element is a unit if and only if it is not a zero divisor. Particularly, this is true for the rings Z_n, $Z_n \times Z_n$, $Z_n[i]$, and $Z_n[i] \times Z_n[i]$. Since, $I_n \subseteq U_n$ and $I_n[i] \subseteq U_n[\,i]$. It is clear that $I_n \subseteq I_n[i]$, it is not surprising that there is an interrelationship between the elements in the groups I_n and $I_n[i]$.

Theorem 3.6. Let $\alpha = a + ib$ be a nonzero element in the ring $Z_n[i]$. Then $a + bi \in I_n[i]$ if and only if $a^2 - b^2 = 1$ and $2ab = 0$ over modulo n.

Proof. Suppose that $\alpha = a + ib \in Z_n[i]$ and $\alpha \neq 0$. By the definition of involution,

$$\begin{aligned} \alpha \in I_n[i] \quad &\Leftrightarrow \alpha^2 = 1 \text{ under modulo } n \\ &\Leftrightarrow (a + bi)(a + bi) = 1 \\ &\Leftrightarrow a^2 - b^2 + i2ab = 1 + i0 \\ &\Leftrightarrow a^2 - b^2 = 1 \text{ and } 2ab = 0 \end{aligned}$$

□

Remark 3.7.

i. Every Gaussian involution is a Gaussian unit, but the converse is not true. For instance, $2 + 3i$ is a Gaussian unit in $Z_4[i]$ but not a Gaussian involution, since $2^2 - 3^2 = 3 \neq 1$.

ii. If $a + bi$ is a Gaussian involution, then $b + ai$ may not be a Gaussian involution. For example, $3 + 2i$ is a Gaussian involution in $Z_4[i]$, but $2 + 3i$ is not a Gaussian involution.

In general, it is not clear to satisfy finite groups and their subgroups by resolving the orders of each of its members. According to the Chinese remainder's theorem [18] of numbers, a standard method is to resolve the finite groups to its orders like primes and prime powers as recommended in the following theorems.

Theorem 3.8. [17] If l and m are both relatively prime, then

i. $Z_{lm} \cong Z_l \times Z_m$ and $Z_{lm}[i] \cong Z_l[i] \times Z_m[i]$

ii. $U_{lm} \cong U_l \times U_m$ and $U_{lm}[i] \cong U_l[i] \times U_m[i]$

Theorem 3.9. [17] If $n > 1$ is a positive integer with the canonical form $n = {p_1}^{a_1}{p_2}^{a_2} \dots {p_r}^{a_r}$. Then,

i. $U_n \cong U_{{p_1}^{a_1}} \times U_{{p_2}^{a_2}} \times \dots \times U_{{p_r}^{a_r}}$

ii. $U_n[i] \cong U_{{p_1}^{a_1}}[i] \times U_{{p_2}^{a_2}}[i] \times \dots \times U_{{p_r}^{a_r}}[i]$

We observe the previous results do hold good for the collection of Gaussian involutions modulo n. We know that the collection of positive integers is partitioned into the sets of positive integers n such that $n \equiv 3(mod\ 4)$, $n \equiv 2(mod\ 4)$, $n \equiv 1(mod\ 4)$, and $n \equiv 0(mod\ 4)$. Also, every odd prime can be written as $n \equiv 3(mod\ 4)$ and $n \equiv 1(mod\ 4)$. We observe that, for the even prime 2, $I_2[i] = \{1, i\}$ and thus $|I_2[i]| = 2$. But, for the collection of Gaussian involutions, we accomplish many results.

Theorem 3.10. If p is a prime of the form $p \equiv 3(mod\ 4)$, then $\left|I_p[i]\right| = 2$.

Proof. Because of the prime p of the form $p \equiv 3(mod\ 4)$, the ring $Z_p[i]$ is a field, and this $U_p[\,i]$ is a cyclic group. Hence, by the Theorem [2.11], it is well known that every finite field contains exactly two involutions, so $\left|I_p[i]\right| = 2$. □

Example 3.11.

i. For $p = 3$, $I_3[i] = \{1,3\}$ and $|I_3[i]| = 2$.

ii. For $p = 7$, $I_7[i] = \{1,6\}$ and $|I_7[i]| = 2$.

Theorem 3.12. For every prime$p$, $p \equiv 3(mod\ 4)$ and $k \geq 1$ then $\left|I_{p^k}[i]\right| = \left|I_{p^k}\right| = 2$.

Proof. By the definition of Gaussian involutions,

$$I_{p^k}[i] = \{a + ib \in Z_{p^k}[i] : (a + ib)^2 = 1\} = \{a + ib \in Z_{p^k}[i] : a^2 - b^2 \equiv 1(mod\ p^k), 2ab \equiv 0(mod\ p^k)\}$$

For the condition $2ab \equiv 0(mod\ p^k)$, there are the following possibilities exist. First suppose $a = 0$ and $b = 0$, then $a^2 - b^2 = 0$. This is a contradiction to the fact that $a^2 - b^2 \equiv 1(mod\ p^k)$. So at least one of a and b must be not equal to zero. Suppose the elements a and b are both not equal to 0. Without loss of generality we may assume that $a = p^q$ and $b = p^{k-q}$ $(q > 0)$, $a^2 - b^2 = (p^q)^2 - (p^{k-q})^2 = p^{2q} - p^{2(k-q)} \not\equiv 1(mod\ p^k)$, a contradiction. Hence, we conclude that the condition $b = 0$ holds good because Gaussian involution is not purely imaginary over modulo p^k. This clears that $I_{p^k}[i] = I_{p^k}$.

Now enumerate the total number of Gaussian involutions in $I_{p^k}[i]$. For this let $x \in I_{p^k}[i]$, we have $\alpha = a + bi = a + 0i = a$ and $a^2 = 1$. This implies that

$$\begin{aligned} a^2 - 1 \equiv 0(mod\ p^k) &\Rightarrow ((a-1)+1)((a-1)+1) - 1 \equiv 0(mod\ p^k) \\ &\Rightarrow ((a-1)+1)^2 - 1 \equiv 0(mod\ p^k) \\ &\Rightarrow (a-1)^2 + 2(a-1) \equiv 0(mod\ p^k) \\ &\Rightarrow (a-1)(a+1) \equiv 0(mod\ p^k) \\ &\Rightarrow p^k | (a-1)(a+1) \end{aligned}$$

This shows that $p^k|(a-1)$, or $p^k|(a+1)$. Now suppose $p^k|(a-1)$, then $a - 1 \equiv 0(mod\ p^k)$. Therefore, $a \equiv 1(mod\ p^k)$ implies that $\alpha = 1$. Again suppose $p^k|(a+1)$, then there exists a positive integer r such that $a + 1 = p^k r$. Now we claim that $r = 1$. Suppose $r > 1$. Then, $a = p^k r - 1$ and $a^2 = 1$. This implies that $(p^k r - 1)^2 = 1$. It follows that, either $r = 0$, or $r = 2(p^{-k})$, this is again a contradiction. So, our assumption that $r > 1$ is not true, and hence $r = 1$. Therefore, $a + 1 = p^k$, and thus $a = \alpha = p^k - 1$. This shows that $\alpha = 1$ and $\alpha = p^k - 1$ are the only two elements in $I_{p^k}[i]$. So, for every prime $p \equiv 3(mod\ 4)$ there is a cyclic subgroup $\langle 1, p^k - 1 : (p^k - 1)^2 \equiv 1(mod\ p^k)\rangle$ in the group $U_{p^k}[i]$ such that $I_{p^k}[i] \cong \langle 1, p^k - 1 : (p^k - 1)^2 \equiv 1(mod\ p^k)\rangle \cong I_{p^k}$. Hence, $\left|I_{p^k}[i]\right| = \left|I_{p^k}\right| = 2$. □

Example 3.13.

i. For $p = 3$ and $k = 2$, $I_{3^2}[i] = I_9[i] = \{1,8\}$ and $|I_{3^2}[i]| = 2$.

ii. For $p = 7$ and $k = 2$, $I_{7^2}[i] = I_{49}[i] = \{1,48\}$ and $|I_{7^2}[i]| = 2$.

Theorem 3.14. If p is a prime of the form $p \equiv 1(mod\ 4)$ and $k \geq 1$, then $\left|I_{p^k}[i]\right| = 4$.

Proof. For the prime p of the form $p \equiv 1(mod\ 4)$, the set of Gaussian involutions of the ring $Z_{p^k}[i]$ is $I_{p^k}[i] = \{a + ib \in Z_{p^k}[i] : (a + ib)^2 \equiv 1(mod\ p^k)\}$. Let $a + ib \in I_{p^k}[i]$, then

$$(a + ib)^2 \equiv 1(mod\ p^k) \Rightarrow a^2 - b^2 \equiv 1(mod\ p^k) \text{ and } 2ab \equiv 0(mod\ p^k)$$

First, $2ab \equiv 0(mod\ p^k)$ means $a = 0$ or $b = 0$. From this condition, the group $I_{p^k}[i]$ reduces to $I_{p^k}[i] = \{a, ib \in Z_{p^k}[i] : a^2 \equiv 1(mod\ p^k)\}, (ib)^2 \equiv 1(mod\ p^k)\}$. This shows that for $a, ib \in I_{p^k}[i]$, we have $p^k|(a^2 - 1)$ and $p^k|(b^2 + 1) \Rightarrow a^2 - 1 \equiv 0(mod\ p^k)$ and $b^2 + 1 \equiv 0(mod\ p^k)$.

These two quadratic congruences give two distinct values for a and two distinct values for b over modulo p^k. Consequently, for α and β in $U_{p^k}[i]$, there is a non-cyclic subgroup $I_{p^k}[i]$ of the group $U_{p^k}[i]$ such that $I_{p^k}[i] = \langle \alpha, \beta : \alpha^2 - 1 \equiv 0(mod\ p^k),\ \beta^2 + 1 \equiv 0(mod\ p^k)\rangle$ whenever the prime $p \equiv 1(mod\ 4)$. Therefore, $\left|I_{p^k}[i]\right| = 4$. □

Example 3.15.

1. Let $p = 5$.

   i. If $\alpha = 1$, then $I_5[i] = \{1,4,2i,3i\}$ and $|I_5[i]| = 4$.

   ii. If $\alpha = 2$, then $I_{5^2}[i] = I_{25}[i] = \{1,24,7i,18i\}$ and $|I_{5^2}[i]| = 4$.

2. Let $p = 13$.

   i. If $\alpha = 1$, then $I_{13}[i] = \{1,12,5i,8i\}$ and $|I_{13}[i]| = 4$.

   ii. If $\alpha = 2$, then $I_{13^2}[i] = I_{169}[i] = \{1,168,70i,99i\}$ and $|I_{13^2}[i]| = 4$.

Theorem 3.16. For even prime 2 and $k > 1$ then $I_{2^k}[i] \cong I_2[i] \times I_2[i] \times ... \times I_2[i](k\text{times})$ and $\left|I_{2^k}[i]\right| = 2^k$.

PROOF. Since $I_2[i]$ is a cyclic group of order 2, and thus $I_{2^k}[i]$ is a finite abelian but not cyclic. Accordingly, by the fundamental theorem of finite abelian groups, the group $I_{2^k}[i]$ can be written as $I_{2^k}[i] \cong I_2[i] \times I_{2^{k-1}}[i] \cong I_2[i] \times I_2[i] \times I_{2^{k-2}}[i] \cong \cdots \cong I_2[i] \times I_2[i] \times ... \times I_2[i](k \text{ times})$ and hence

$$\begin{aligned} \left|I_{2^k}[i]\right| &= |I_2[i] \times I_2[i] \times ... \times I_2[i](k\text{times})| \\ &= |I_2[i]| \cdot |I_2[i]| \cdot ... \cdot |I_2[i]| \ (k \text{ times}) \\ &= 2 \cdot 2 \cdot ... \cdot 2(k \text{ times}) \\ &= 2^k \end{aligned}$$

□

Example 3.17. For $k = 2$, $I_{2^2}[i] = I_4[i] = \{1,3,1 + 2\,i, 3 + 2i\}$ and $|I_{2^2}[i]| = 4 = 2^2$.

If the prime $p > 2$ then Theorem 3.16 is not true, that is $\left|I_{p^k}[i]\right| \neq p^k$ because $I_{p^k}[i] \ncong I_p[i] \times I_{p^{k-1}}[i]$. For example, $I_{5^2}[i] \ncong I_5[i] \times I_5[i]$. In particular, the following results are well cleared. For any $k > 1$,

i. $Z_{2^k} \ncong Z_2 \times Z_{2^{k-1}}$ and $Z_{2^k}[i] \ncong Z_2[i] \times Z_{2^{k-1}}[i]$

ii. $U_{2^k} \ncong U_2 \times U_{2^{k-1}}$ and $U_{2^k}[i] \ncong U_2[i] \times U_{2^{k-1}}[i]$

iii. $I_{2^k} \cong I_2 \times I_{2^{k-1}}$ and $I_{2^k}[i] \cong I_2[i] \times I_{2^{k-1}}[i]$

Theorem 3.18. If p and q are relatively prime, then $I_{pq}[i] \cong I_p[i] \times I_q[i]$.

PROOF. Without loss of generality, assume that $p \equiv 2(mod\,4)$ and $q \equiv 3(mod\,4)$. Now we define a map $f: I_p[i] \times I_q[i] \to I_{pq}[i]$ by the relation $f((a,b)) = iqa + pb$ for every $(a,b) \in I_p[i] \times I_q[i]$ and the element $iqa + pb \in I_{pq}[i]$ for all a and b. One can easily verify that$f$ is a well-defined group homomorphism. Now to show that f is an injection. For $(a,b),(c,d) \in I_p[i] \times I_q[i]$, we have $f((a,b)) = f((c,d))$. This implies that

$$\begin{aligned} iqa + pb = iqc + pd \quad &\Rightarrow a = c \text{ and } b = d \\ &\Rightarrow (a,b) = (c,d) \end{aligned}$$

Thus f is injective. Since the finite groups $I_p[i] \times I_q[i]$ and $I_{pq}[i]$ have the same cardinality, so that f is surjective and hence f is a group isomorphism. □

For example, take $p \equiv 2$ and $q \equiv 3$, $I_6[i] \cong I_2[i] \times I_3[i]$. We have $I_2[i] = \{1, i\}$, $I_3[i] = \{1,2\}$ and $I_6[i] = \{1,5,2 + 3i, 4 + 3i\}$. Clearly, $(1,1) \to 2 + 3i$, $(1,2) \to 4 + 3i$, $(i,1) \to 5$, and $(i,2) \to 1$.

Theorem 3.19. Let $n > 1$ be a positive integer with the canonical form $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$. Then,

$$I_n[i] \cong I_{p_1^{a_1}}[i] \times I_{p_2^{a_2}}[i] \times ... \times I_{p_r^{ar}}[i] \text{ and } |I_n[i]| \cong \left|I_{p_1^{a_1}}[i]\right| \times \left|I_{p_2^{a_2}}[i]\right| \times ... \times \left|I_{p_r^{ar}}[i]\right|$$

PROOF. It is clear from the Chinese remainder theorem [18]. □

Generally, now establish a formula for enumerating the total number of Gaussian involutions in the Gaussian ring for various values of n. Remember that the cardinality of the Gaussian involutions of the non-cyclic ring $Z_n[i]$ is $|I_n[i]|$ and $I\ (Z_n[i]) = I\ \ (U_n[\,i])$, and the representation theory of the finite cyclic group is a critical base case for the representation theory of more general finite groups. For any integer $n \geq 1$, there exists a finite cyclic group C_n with representation $C_n = \langle a : a^n = 1\rangle$ for multiplication. For instance, a group $C_2 = \{1, a : a^2 = 1\}$ is a cyclic group of order 2, and it is also isomorphic to the cyclic group $Z_2 = \{0,1\}$ for addition modulo 2.

Theorem 3.20. If n is a positive integer, then $|I_n[i]| = 2^k$ for some positive integer k.

PROOF. The result is clear if $n = 2$. If $n = 2$ so that $|Z_n[i]| = 4$, then there is only one subgroup, namely $\{1, i\}$ in $Z_n[i]$ with the property that $a^2 = 1$, and so $|I_n[i]| = 2 = 2^1$. Assume that $n > 2$. We now prove this by the two cases, namely, $I_n[i]$ is either cyclic or not. First, suppose $I_n[i]$ is cyclic. Then, there is nothing to prove. Now suppose $I_n[i]$ is a non-cyclic abelian group, then we have to prove that $|I_n[i]| = 2^k$ for some positive integer k. For this, we define a map $f : Z_2 \times Z_2 \times ... \times Z_2 \to I_n[i]$ by the relation $f(a_1, a_2, \dots, a_k) = \alpha_1^{a_1}\alpha_2^{a_2} \dots \alpha_k^{a_k}$ for every element $a_1, a_2, \dots, a_k$ in the non-cyclic group $Z_2 \times Z_2 \times ... \times Z_2 \cong Z_2^k$, where $\alpha_1^{a_1}, \alpha_2^{a_2}, \dots, \alpha_k^{a_k}$ are distinct k involutions of $I_n[i]$. By Theorem 3.18, $I_n[i] \cong Z_2^k$, and hence $|I_n[i]| = \left|Z_2^k\right| = 2^k$. □

For verification of the above results, we obtain the following set of Gaussian involutions of the Gaussian ring $Z_n[i]$ with fixed values of $n = 2,3,4, \dots ,13$, respectively.

$I_2[i] = \{1, i\} \cong C_2,$

$I_3[i] = \{1,2\} \cong C_2,$

$I_4[i] = \{1,3,1 + 2\,i, 3 + 2i\} \cong C_2 \times C_2,$

$I_5[i] = \{1,4,2\,i, 3\,i\} \cong C_2 \times C_2,$

$I_6[i] = \{1,5,2 + 3i, 4 + 3i\} \cong C_2 \times C_2,$

$I_7[i] = \{1,6\} \cong C_2,$

$I_8[i] = \{1,3,5,7,1 + 4i, 3 + 4i, 5 + 4\,i, 7 + 4i\} \cong C_2 \times C_2 \times C_2,$

$I_9[i] = \{1,8\} \cong C_2,$

$I_{10}[i] = \{1,9,3i, 7i, 4 + 5i, 5 + 2i, 6 + 5i, 5 + 8i\}\} \cong C_2 \times C_2 \times C_2,$

$I_{11}[i] = \{1,10\} \cong C_2,$

$I_{12}[i] = \{1,5,7,11,1 + 6i, 5 + 6i, 7 + 6i, 11 + 6i\} \cong C_2 \times C_2 \times C_2,$

$I_{13}[i] = \{1,12,5i, 8i\} \cong C_2 \times C_2$

4. Conclusion

Owing to the involution theory, involutions over finite commutative rings have been widely used in applications such as algebraic cryptography, network security, and coding theory. Further, quadratic polynomials like $x^2 - 1 = 0$ over finite rings and fields have been extensively studied due to their wide applications in block cipher designs, algebraic coding theory, and combinatorial design theory. Following these applications of involutions to characterize the involutory behaviour of the digital control systems, digital logic systems, modern algebraic systems, and generalized cyclotomic systems and this paper gives more concise criterion analytical methods for enumerating Involutions over the finite cyclic and non-cyclic rings.

Author Contributions

All the authors contributed equally to this work. They all read and approved the last version of the manuscript.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] J. A. Gallian, Contemporary Abstract Algebra, *5th edition*, Houghton Mifflin Co., Boston, 1998.

[2] J. T. Cross, *The Euler's φ-function in the Gaussian Integers*, American Mathematical Monthly Journal 55 (1983) 518–528.

[3] J. L. Smith, J. A. Gallian, *Factoring Finite Factor Rings*, Mathematics Magazine 58 (1985) 93–95.

[4] A. N. El-Kassar, H. Y. Chehade, D. Zatout, *Quotient Rings of Polynomials over Finite Fields with Cyclic Groups of units*, Proceedings of the International Conference on Research Trends in Science and Technology, RTST2002, Lebanese American University, Beirut Lebanon (2002) 257–266.

[5] A. N. El-Kassar, H. Y. Chehade, *Generalized Group of Units*, Mathematica Balkanica, New Series 20 (2006) 275–286.

[6] A. A. Allan, M. J. Dunne, J. R. Jack, J. C. Lynd, H. W. Ellingsen, *Classification of the Group of Units in the Gaussian Integers Modulo N**, Pi Mu Epsilon Journal 12 (9) (2008) 513–519.

[7] W. K. Buck, *Cyclic Rings*, *Master's Thesis*, Eastern Illinois University: The Keep (2004).

[8] T. W. Hungerford, *Algebra: Graduate Texts in Mathematics*, Springer, New York, 2003.

[9] W. M. Fakieh, S. K. Nauman, *Reversible Rings with Involutions and Some Minimalities*, The Scientific World Journal, Hindawi Publishing Corporation 2013 (2013) 1–8.

[10] I. N. Herstein, S. Montgomery, *A Note on Division Rings with Involutions*, Michigan Mathematical Journal 18 (1) (1971) 75–79.

[11] D. I. C. Mendes, *A Note on Involution Rings*, Miskolc Mathematical Notes 10 (2) (2009) 155–162.

[12] W. M. Fakieh, *Symmetric Rings with Involutions*, British Journal of Mathematics and Computer Science 8 (6) (2015) 492–505.

[13] T. Chalapathi, R. V. M. S. S. K. Kumar, *Self-Additive Inverse Elements of Neutrosophic Rings and Fields*, Annals of Pure and Applied Mathematics 13 (1) (2017) 63–72.

[14] V. K. Khanna, S. K. Bhambri, A Course in Abstract Algebra, *2nd Edition*, Vikas Publishing House Pvt. Ltd, 1998.

[15] D. Suzanne, *How Many Solutions Does* $x^2 + 1 = 0$ *Have? An Abstract Algebra Project*, PRIMUS Journal 10 (2) (2007) 111–122.

[16] G. Dresden, W. M. Dymacek, *Finding Factors of Factor Rings over the Gaussian Integers*, The American Mathematical Monthly Journal 112 (7) (2018) 602–611.

[17] T. Andreescu, D. Andrica, I. Cucurezean, An Introduction to Diophantine Equations: A Problem-Based Approach, Springer, New York, 2010.

[18] T. M. Apostol, Introduction to Analytic Number Theory, Springer International Student Edition, 1989.