Calculations on Digraphs of Square Mapping of Eisenstein Integers Modulo n

Hamza Daoub[1 (*)], Osama Shafah[2], and Fathi A M Bribesh[3]

[1,3] Dept. of Mathematics, University of Zawia, Libya

[2] Dept. of Mathematics, Sabratha University, Libya

Abstract

Let ξ be a primitive third root of unity, and $\mathbb{Z}_n[\xi] = \{a + b\xi | a, b \in \mathbb{Z}_n\}$, is the ring of Eisenstein integers modulo n, $n < \infty$. Define the mapping $\varphi: \mathbb{Z}_n[\xi] \to \mathbb{Z}_n[\xi]$ by $\varphi(a + b\xi) = (a + b\xi)^2 = a^2 - b^2 + (2ab - b^2)\xi$ which represents the directed graph $G(\mathbb{Z}_n[\xi])$. This study investigates the properties of the graph $G(\mathbb{Z}_n[\xi])$ with calculations obtained by applications of computer arithmetic using the Modern Technical Computing Software, Wolfram Mathematica.

Key Words: *Eisenstein integers, Eisenstein prime, iteration digraph, quadratic residue.*

(*) Email: h.daoub@zu.edu.ly

1. Introduction

Regarding to the Fundamental Theorem of Algebra, for any given positive integer n, the polynomial of the form $x^n - 1$ has exactly n solutions in the complex plane. These solutions are known as complex n^{th} roots of unity of the form $e^{\frac{2\pi ik}{n}}$ for each integer k; $1 \leq k \leq n$. When this sum is restricted on those values of k that are relatively prime to n, we obtain the n^{th} cyclotomic polynomial, denoted $\phi_n(x)$.

We particularly attracted to the third cyclotomic polynomial, given by the form $\phi_3(\xi) = \xi^2 + \xi + 1$. The specific root of $\phi_3(\xi)$ is the cubic complex root of unity, henceforward will be denoted by ξ where $\xi = \frac{1}{2}(-1 + i\sqrt{3})$, is an element in the fraction field of $\mathbb{Q}[\sqrt{-3}]$ and of course of $\mathbb{Z}\left[\sqrt{-3}\right]$. The set $\mathbb{Z}[\xi] = \{a + b\xi,\ a, b \in \mathbb{Z}\}$ under the usual operations of addition and multiplication of complex numbers, forms an integral domain, known as the ring of Eisenstein integers, also indicated by E. This set forms a commutative ring in the algebraic number field $\mathbb{Q}[\xi]$. In fact, the Eisenstein integers form a unique factorization domain.

One of the important tools used in exploring $\mathbb{Z}[\xi]$ is the norm function defined by $N(\alpha) = a^2 - ab + b^2 = 0,\ \alpha = (a + b\xi) \in \mathbb{Z}[\xi]$. The norm function retains some useful properties. First, the function always provides a non-negative integer output, and in fact takes on non-zero values at all non-zero Eisenstein integers. Second, the norm function is completely multiplicative. The element α is called a unit if and only if $N(\alpha) = 1$. It then follows that the only units of $\mathbb{Z}[\xi]$ are $\{\pm 1, \pm\xi, \pm\xi^2\}$. In any given ring, elements that differ only via multiplication by a unit are known as associates. Thus, every element in $\mathbb{Z}[\xi]$ has six different associates [6].

Since the cubic root of unity satisfies the equation $1 + \xi + \xi^2 = 0$, thus, $\xi^2 = -\xi - 1$ which is the other root of the equation $x^2 + x + 1 = 0$, i.e., $\xi^2 = \bar{\xi}$.

It is easily seen that, for any positive integer n, the factor ring E/nE is isomorphic to the ring $\mathbb{Z}_n[\xi] = E_n = \{a + b\xi \mid a, b \in Z_n\}$. Thus E_n is a principal ideal ring. This ring is called the ring of Eisenstein integers modulo n. Such ring properties are widely investigated, see for instance [3], [4], units and zero divisors are completely characterized and counted. This characterization uses the fact that $a + b\xi$ is a unit in E_n if and only if $N(a + b\xi)$ is a unit in $\mathbb{Z}_\mathrm{n}$.

The association between graphs and quadratic congruence is proposed in [5], [8], [9], which provide an interesting connection between number theory, graph theory, and group theory. However, [9] explored properties of the iteration digraph representing a dynamical system occurring in number theory.

Our study aims to contribute and enrich the concept of pairing of graph theory with the abstract of finite ring theory, particularly with E_n. Throughout this paper, we introduce supporting basic concepts for the main aim of the study and investigate structural characteristics of squared mapping diagraphs. Always, we consider p is a prime integer, k and n are positive integers, and cycles of length one is indicated as loops.

1. Preliminaries

One of the central problems of number theory is finding solutions (in the integers) of polynomial equations with integer coefficients in one or more variables. We will focus on the most important special case of quadratic congruence $x^2 \equiv z \mod p^k$, namely when p is odd and $k = 1$, i.e., the congruence $x^2 \equiv z \mod p$.

Over $\mathbb{Z}_n$, the number of residue classes $mod\, n$ is simply n. However, over $\mathbb{Z}_n[\xi]$, letting $< n > = \{rn: r \in \mathbb{Z}[\xi]\}$ denote the ideal in $\mathbb{Z}[\xi]$ generated by n the number of residue classes is the cardinality of the quotient ring $\mathbb{Z}[\xi]/< n >$. Therefore, the cardinality of $\mathbb{Z}[\xi] =< n >$, is $|\mathrm{n}|^2$ (see [7]).

For $n > 1$, let $\varphi: \mathbb{Z}_n[\xi] \to \mathbb{Z}_n[\xi]$. The iteration digraph of φ is a directed graph whose vertices are elements of $\mathbb{Z}_n[\xi]$ and such that there exists exactly one directed edge from $\mathrm{z} = a + b\xi$ to $\varphi(\mathrm{z})$ for all $\mathrm{z} \in \mathbb{Z}_n[\xi]$. For each $\mathrm{z} \in \mathbb{Z}_n[\xi]$, let $\varphi(\mathrm{z})$ be the remainder of z^2 $modulo\, n$, i.e., $\varphi(\mathrm{z}) \in \mathbb{Z}_n[\xi]$ and

$$\varphi(a + b\xi) = (a + b\xi)^2 = a^2 - b^2 + (2ab - b^2)\xi \quad mod\, n \qquad (1)$$

From here on, whenever we refer to the iteration digraph of $G(\mathbb{Z}_n[\xi])$, we assume that the mapping φ is as given in Eq.(1).

We identify the vertex a of $\mathbb{Z}_n$ with its residue $modulo\, n$. For brevity we will make statements such as $\gcd(a, n) = 1$, treating the vertex z as a number. Moreover, when we refer, for instance, to the vertex z^2, it is identified as the remainder $\varphi(\mathrm{z})$ given by Eq.(1).

***Definition** 1: If p is an odd prime and z is an integer not divisible by p, then z is a quadratic residue (respectively, quadratic non-residue) of p if there is (respectively, is not) an integer x such that $x^2 \equiv z \ \ mod\, p$.*

***Definition** 2: An Eisenstein integer $a + b\xi$ is said to be Eisenstein prime if it satisfies one of the following conditions*

I. $b = 0$ *and* $a = p$ *prime with* $p \equiv 2\, mod\, 3$

II. $a = 0$ *and* $b = p$ *prime with* $p \equiv 2\, mod\, 3$

III. $N(a + b\xi) = a^2 - ab + b^2 = p$ *prime such that* $p = 3$ *or* $p \equiv 1\, mod\, 3$.

Eisenstein primes are irreducible elements in $\mathbb{Z}[\xi]$. If $a+b\xi$ is an Eisenstein prime then so are its associates $\{\pm(a+b\xi), \pm(b+(b-a)\xi), \pm((a-b)+a\xi)\}$ and conjugates $\{\pm(a+b\xi), \pm(a+(a-b)\xi), \pm((b-a)+b\xi)\}$.

In the following Proposition (see [1]), all residues and non-residues are considered with respect to a fixed prime p.

Proposition 1:

(i) The product of two residues is a residue.

(ii) The product of a residue and a non-residue is a non-residue.

(iii) The product of two non-residues is a residue.

The following Definition (see [2]) introduces the most important piece of mathematical technology that is used to study residues and non-residues in an interesting way.

***Definition** 3: For an odd prime number p and an integer a, the symbol $\left(\frac{a}{p}\right)$,*

$$\left(\frac{a}{p}\right)=\begin{cases} 0 & if\ a\equiv 0 \mod p \\ 1 & if\ a\ is\ a\ quadratic\ residue\ modulo\ p\ and\ a\ \not\equiv\ 0 \mod p \\ -1 & if\ a\ is\ a\ quadratic\ non-residue\ modulo\ p \end{cases}$$

is called the Legendre symbol. It satisfies the following properties:

1) $\left(\frac{-1}{p}\right)=\begin{cases} 1 & if\ p\equiv 1 \mod 4 \\ -1 & if\ p\equiv 3 \mod 4 \end{cases}$

2) $\left(\frac{3}{p}\right)=\begin{cases} 1 & if\ p\equiv 1\ or\ 11 \mod 12 \\ -1 & if\ p\equiv 5\ or\ 7 \mod 12 \end{cases}$

3) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

We recall the definition of the conjugate as an important tool used to study $\mathbb{Z}_n[\xi]$.

Definition *4: If $z = a + b\xi$ in $\mathbb{Z}_n[\xi]$, then the complex conjugate of z denoted $\bar{z}$, is defined $\bar{z} = a + b\xi^2 = (a - b) - b\xi$.*

The concept of nilpotent (idempotent) elements of $\mathbb{Z}_n[\xi]$ plays an interesting part of our study. It is quite important to introduce some properties of nilpotent elements for the sake of completeness.

Lemma *1:*

(i) If $a + b\,\xi$ is a nilpotent in $\mathbb{Z}_n[\xi]$, then $a^2 + b^2 - ab$ is a nilpotent in $\mathbb{Z}_n$.

(ii) $a + b\,\xi$ is a nontrivial idempotent in $\mathbb{Z}_n[\xi]$ if and only if $a^2 - b^2 = a$, $2ab = b + b^2$, and neither a nor b is zero in $\mathbb{Z}_n$.

When $\mathbb{Z}_n$[ξ] has zero-divisors, then $\mathbb{Z}_n$[ξ][x] is not a unique factorization ring, so $x^2 \equiv z \mod n$ has two distinct non-associated factorizations. Therefore, $\mathbb{Z}_n$[ξ][x] is not UFD. However, in the following Proposition $\mathbb{Z}_n$[ξ] is investigated for $n > 2$ to recognize fields (see [4]).

Proposition *2: If p is a positive integer larger than 1, then $\mathbb{Z}_p[\xi]$ is a field if and only if p is a prime such that $p \equiv 2 \mod 3$.*

Let p be a prime number greater than two; according to the Definition of units in $\mathbb{Z}_n[\xi]$, if $z = a + b\xi$, $z^{-1} = c + d\xi$ then the non-zero values c and d are given by

$$c = \frac{a-b}{(-ab+b^2+a^2)} = \frac{a-b}{N(z)}, \quad d = -\frac{b}{N(z)}.$$

I.e.,

$$z^{-1} = \frac{a-b}{N(z)} + \left(-\frac{b}{N(z)}\right)\xi .$$

Note that, if $N(z) = 1$ then $\bar{z} = z^{-1}$

2. Main Results

The main results of our study concern some properties of the directed graph. We stand up on some basic terms such as indegrees and outdegrees of vertices, loops, cycles, components structure, closed paths, and other properties as well as some computer calculations

3.1 Degrees of vertices

In a directed graph, each vertex has an indegree and an outdegree. The indegree of any vertex $v \in V(G)$ in this digraph is the number of distinct roots of the quadratic congruence $x^2 - v = 0$ modulo n. If $\mathbb{Z}_n[\xi]$ is a field, then $\mathbb{Z}_n[\xi][x]$ is a unique factorization domain. Therefore, the incoming degree of v is 2. Otherwise, $\mathbb{Z}_n[\xi][x]$ is not unique factorization domain. Thus, the incoming degree of v is $2k$, where k is a positive integer (represents prime omega function $\Omega(n)$ in some cases). Since φ is a function, then the outdegree of $v \in V(G)$ is one.

If $z_1 = a_1 + b_1\xi$ is a vertex that corresponds to an irreducible polynomial $x^2 - z_1 \equiv 0 \mod n$, and it is a root of the polynomial

$$x^2 - \alpha \equiv 0 \mod n \tag{2}$$

Then, $z_2 = -a_1 - b_1\xi$ is another root of the polynomial (2).

Note that, the vertices $a + b\xi$ and $b + a\xi$ are incident to vertex v, if $a^2 = b^2$.

Let p be an odd prime number $z = a + b\xi$, and $w = c + d\xi$ are two different vertices with two different non-zero norms are incident to a vertex v. Thus, $N^2(z) \to N(v)$, $N^2(w) \to N(v)$, and $N^2(z) = N^2(w)$. Therefore, $N^2(z) - N^2(w) = 0$, which implies $\big(N(z) - N(w)\big)\big(N(z) + N(w)\big) = 0$. Since the norm of z, w are different, then $N(z) + N(w) = 0$. Thus,

$$a^2 + b^2 + c^2 + d^2 - ab - cd = 0 \tag{3}$$

We know that

$$a^2 - b^2 = c^2 - d^2 \tag{4}$$

$$2ab - b^2 = 2cd - d^2 \tag{5}$$

Solving (3) for the term cd using (4), one gets

$$cd = 2b^2 + 2c^2 - ab \tag{6}$$

Subtracting (4) from (5) leads to

$$a^2 - 2ab = c^2 - 2cd \tag{7}$$

Substitution of (6) in (7), yields

$$a^2 - 2ab = c^2 - 2(2b^2 + 2c^2 - ab)$$

$$-3c^2 = a^2 + 4b^2 - 4ab$$

$$3c^2 = (p-1)(a-2b)^2 \tag{8}$$

By substitution of (8) in (4), we get

$$3d^2 = (p-1)(2a-b)^2 \tag{9}$$

If 3 is a quadratic residue $modulu\, n$, the variables c and d can be written in the form

$$c = \alpha(a-2b)$$

$$d = \alpha(2a-b),$$

for some $\alpha \in \mathbb{Z}_n$, where $\alpha^2 = 3^{-1}(p-1)$.

To determine the case when $3^{-1}(n-1)$ is quadratic residue, we introduce the following theorem

***Theorem** 1: Let p be an odd prime, the quadratic polynomial $x^2 - 3^{-1}(n-1) = 0 \ mod\, p$ is irreducible for $p \equiv 2 \ mod\, 3$, and reducible for $p \equiv 1 \ mod\, 3$.*

Proof:

Let p be any odd prime, and $a, b \in \mathbb{Z}_p$ are non-zero elements such that $ab = 1$. From *Definition 3*, we know $\left(\frac{1}{p}\right) = 1$, and $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Therefore, $1 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, which means a and b are both quadratic residues or both non-quadratic residues.

Now, it is known from [2] that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & if\ p \equiv 1\ mod\ 4 \\ -1 & if\ p \equiv 3\ \ mod\ 4 \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & if\ p \equiv 1\ or\ 11\ \ mod\ 12 \\ -1 & if\ p \equiv 5\ or\ 7\ \ mod\ 12 \end{cases}$$

Thus,

$$\left(\frac{3^{-1}}{p}\right) = \begin{cases} 1 & if\ p \equiv 1\ or\ 11\ \ mod\ 12 \\ -1 & if\ p \equiv 5\ or\ 7\ \ mod\ 12 \end{cases}$$

On one hand, both terms (-1) and 3^{-1} are quadratic residues whenever $p = 4k + 1$ and $p = 12k + 1$, respectively where k is an integer. These primes are $p = 13, 37, 61, 73, 97, 109, \dots$. Since 12 is divisible by 4, then we conclude that (-1) and 3^{-1} are quadratic residues at $p = 12k + 1$.

On the other hand, (-1) and 3^{-1} are quadratic nonresidues together whenever $p = 4k + 3$ and $p = 12k + 7$ for some integers k, where $p = 7,\ 19,\ 31,\ 43,\ 67,\ 79,\ 103,\ \dots$. We conclude that (-1) and 3^{-1} are quadratic non-residue at $p = 12k + 7$. From these two cases we have $(p - 1)$ is divisible by 3, which means $p \equiv 1\ \ mod\ 3$. This completes the proof. ∎

***Remark** 1: If $n = p_1 p_2 \dots p_m$, where p_i is a prime for all $i = 1,2, \dots, m$, and one vertex $v = a + b\xi$ in $V(G)$ satisfies $v = -v$, then the incoming degree of v in a component is $2k - 1$. For instance, in $G(\mathbb{Z}_6[\xi])$ we have a component with 3 indegree vertices as in Figure 1.*

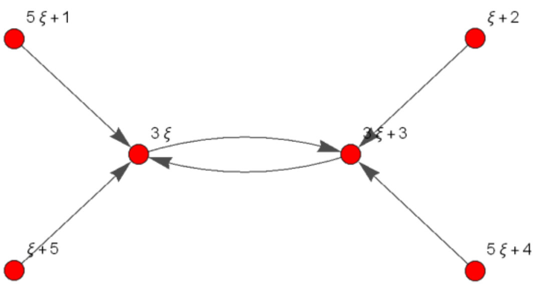


Figure 1: Part of $G(\mathbb{Z}_6[\xi])$

3.2 Components and Closed Paths

Connectivity in an undirected graph means every vertex can reach all other vertices via a path. In fact, an unconnected graph always can be broken down into connected components. A component is said to be strongly connected if there is a directed path from any vertex to all other vertices in that component. I.e., if a vertex u is reachable by vertex v and vice versa. However, a component is weakly connected if one converts all its edges to undirected ones, it becomes a connected component.

In $G(\mathbb{Z}_n[\xi])$, every component with zero indegree vertex must be weakly connected, because the starting vertex cannot be reachable.

Let $n > 3$ be a prime number such that $n \equiv 2 \ mod\, 3$. This means $E_n[X]$ has unique factorization property and every vertex in a component C has indegree 2. The vertex $z = a + b\xi$ with incoming degree 0 in the component C, correspond to irreducible quadratic polynomials $x^2 \equiv z$ in $E_n[X]$. Since the number i of irreducible quadratic polynomials is $i = \frac{n^2-1}{2}$, and $-z = -a - b\xi$ is starting vertex as well. This leads to get a rough upper estimate for the number of components $C_n \leq \frac{i}{2}$.

Definition *5: Let $z = a + b\xi$ be a vertex in $G(\mathbb{Z}_n[\xi])$, then the sequence*

$$\boldsymbol{z \to z^2 \to \cdots \to z^{2^k}}, \tag{10}$$

such that $z^{2^k} \to z$, and $z^{2^j} \neq z^{2^i}$ for all $0 \leq i \neq j \leq k$, forms a cycle of length k, and we write k-cycle.

Suppose that $G(\mathbb{Z}_p[\xi])$ has a loop at the vertex $z = a + b\xi$, so this vertex satisfies $z^2 = z$, which means $a^2 - b^2 + (2ab - b^2)\xi = a + b\xi$. Thus,

$$\boldsymbol{a^2 - b^2 = a} \quad \text{and} \quad \boldsymbol{2ab - b^2 = b}. \tag{11}$$

We note that, if $b = 0$, then $a^2 = a \ mod\, n$, which represents a loop in the graph of quadratic congruence modulo n. While, if $a = 0$ then $b^2 = -b$ and $b^2 = 0$, which implies $b = 0$, this means $z = 0$. Now, if $a, b \neq 0$, then from Eq. (11) we get,

$$a - b = a^2 - 2ab$$

Therefore,

$$a - a^2 = b - 2ab.$$

Since, $b = b(2a - b)$, then

$$b = 2a - 1$$

By substitution in left equation of (11), we get

$$a^2 - 4a^2 + 4a - 1 = a$$

$$\boldsymbol{3a^2 - 3a + 1 = 0}. \tag{12}$$

If the vertex $v \in V(G)$ is a loop. The question here is, what the conjugate of v could be. We provide the answer through the following Proposition.

Proposition *3: Let $z = a + b\xi$ be a vertex in $V(G)$ such that z is a loop then $\bar{z}$ either forms a loop.*

Proof: Suppose that $z = a + b\xi$ then, $\bar{z} = a - b + (-b)\xi$, therefore $\varphi(\bar{z}) = \bar{z}^2 = (a-b)^2 - b^2 + [2(a-b)(-b) - b^2]\xi$. We want to prove that $\bar{z}^2 = \bar{z}$.

Since,

$$\bar{z}^2 = (a-b)^2 - b^2 + [2(a-b)(-b) - b^2]\xi.$$

Therefore,

$$(a-b)^2 - b^2 = a^2 - 2ab \tag{13}$$

$$2(a-b)(-b) - b^2 = b^2 - 2ab \tag{14}$$

From (11), $2ab = b + b^2, a^2 - b^2 = a$ and by substitution in (13) and (14), we get

$$a^2 - 2ab = a^2 - b^2 = a - b$$

$$b^2 - 2ab = -b,$$

which proves that $\bar{z}$ is a loop.

***Corollary** 1: Loops in $G(\mathbb{Z}_n[\xi])$ correspond to 0, 1, and idempotent vertices and their conjugates.*

***Corollary** 2: If $z = a + b\xi$ is a loop in $G(\mathbb{Z}_n[\xi])$ with $z \neq 0,\ z \neq 1$ then $\mathbb{Z}_n[\xi]$ is not an integral domain.*

Proof: Suppose that $z = a + b\xi$ is a loop in $G(\mathbb{Z}_n[\xi])$ with $z \neq 0,\ z \neq 1$ then $\bar{z} = a - b + (-b)\xi$ is a loop as well, but $z\bar{z} = [a + b\xi][a - b + (-b)\xi] = [a(a-b) - (-b^2)] + [(-ab) + b(a-b) - (-b^2)]\xi = [a^2 - ab + b^2] + [-ab + ab - b^2 + b^2]\xi = N(Z) = 0$, so z and $\bar{z}$ are a zero divisors in $\mathbb{Z}_n[\xi]$. Hence, $\mathbb{Z}_n[\xi]$ is not integral domain.

***Remark** 2:*

(i) *The vertices $z = 1$, and $z = 0$ form loops for any $n > 1$.*

(ii) *The vertex $z = -1$ is a vertex incident to $v = 1$ for any $n > 1$.*

(iii) *In $G\big(\mathbb{Z}_p[\xi]\big)$ for any prime number $p > 2$, $z = 0$ is an isolated loop.*

(iv) *For any* $n > 1$ *there exists a cycle of length 2, it corresponds to* $\xi \to n - 1 + (n-1)\xi \to \xi$ ↺.

(v) *every 2-cycle with unit vertices consists of a vertex and its inverse.*

For any prime number $p > 2$, suppose that $z = a + b\xi$ be a vertex in $V(G)$, such that z is an element in a cycle of length two. Then $(z^2)^2 = z$, and

$$a = a^4 - 6a^2b^2 + 4ab^3$$
$$b = 4a^3b - 6a^2b^2 + b^4$$

If $a = 0\,,\ b \neq 0$, then $b = b^4$ or $b^3 = 1$

If $a \neq 0\,,\ b = 0$, then $a = a^4$ or $a^3 = 1$

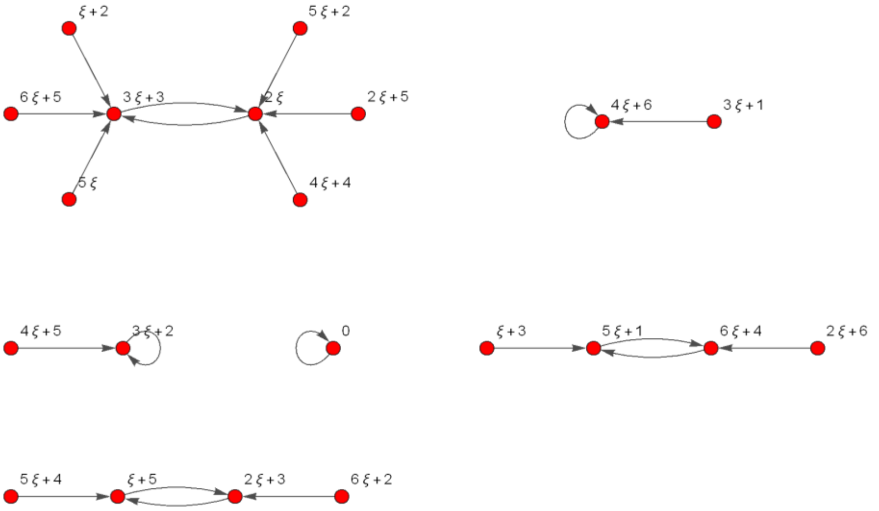


Figure 2: Part of $G(\mathbb{Z}_7[\xi])$

Note that, the norm of any vertex $z \neq 0$ in any cycle of length $r \geq 2$ may satisfies:

$$N(z) = \begin{cases} 0 & \mathit{if\ z\ is\ an\ idempotent} \\ k & \mathit{if\ z\ isn't\ idempotent} \end{cases}$$

For instance, in *Figure 2*, there exist 2-cycles with idempotent vertices different from zero and others not idempotent.

For any vertex $v = (a, b) \in V(G)$, we have

1. If $a = 2b$, then

$$a + b\xi \to b^2\xi \to -b^4 + -b^4\xi \to b^8\xi \to -b^{16} + -b^{16}\xi \to b^{32}\xi \to \cdots \to -b^{2^k} + -b^{2^k}\xi \to b^{2^{k+1}}\xi \qquad (15)$$

This path closes at a vertex (c, d) which depends on the order of $3b$.

2. If $b = 2a$, then

$$a + b\xi \to -3a^2 \to 9a^4 \to 81a^8 \to \cdots \to 3^k a^{2^{\mathrm{k}}} \qquad (16)$$

This path gets closed at a vertex $3^m \mathrm{a}^{2^m}$ for some $1 \leq m < k$.

3. If $a = 0$, the path will follow the procedure in (15).

4. If $b = 0$. the path will follow the procedure in (16).

5. If $a = b$, the path will follow the procedure in (15).

6. If $ab = 0$, then

$$a + b\xi \to a^2 - b^2 - b^2\xi \to a^4 + b^4\xi \to a^8 - b^8 - b^8\xi \to a^{16} + b^{16}\xi \to \cdots \to a^{2^k} - b^{2^k} - b^{2^k}\xi \to a^{2^{k+1}} + b^{2^{k+1}}\xi \to \cdots \qquad (17)$$

This path closes at a vertex $c + d\xi$ which depends on the orders of a and b. Furthermore, we get cycles of this form in $G(\mathbb{Z}_n[\xi])$ when n is not a prime number.

7. If b is a nilpotent element, that is $b^2 = 0$, then

$$a + b\xi \to a^2 + 2ab\xi \to a^4 + 4a^3b\xi \to a^8 + 8a^7b\xi \to a^{16} + 16a^{15}b\xi \to a^{32} + 32a^{31}b\xi \to a^{64} + 64a^{63}b\xi \to \cdots \to a^{2^k}, 2^k a^{2^k - 1}b\xi \qquad (18)$$

This path closes at a vertex $(a^{2^m}, 2^m a^{2^m - 1}b)$ for some $1 \leq m < k$.

8. If a, b are nilpotent elements, i.e., $a^2 = b^2 = 0$, then

$$a + b\xi \rightarrow\ 2ab\xi \rightarrow 0 \circlearrowleft \tag{19}$$

The vertices are incident to the vertex $z = 0$ have the form $(0, ab)$, where a and b are nilpotent elements, (See case 8 above).

We can say if $v = 0$ is not an isolated loop, then we have nilpotent elements, which means $\mathbb{Z}_n[\xi]$ is not an integral domain.

The presence of idempotent element in the graph $G(\mathbb{Z}_n[\xi])$ relies on the choice of the integer number n. If n is a prime satisfies $n \equiv 2\ mod\ 3$ then $a^2 + b^2 \neq ab$ for any non-zero elements $a, b \in \mathbb{Z}_n$, which means $N(z) \neq 0$ for any non-zero $z \in \mathbb{Z}_n[\xi]$. Thus, we have $n^2 - 1$ units in $\mathbb{Z}_n[\xi]$ and the only appeared loops are $v = 0$ or $v = 1$.

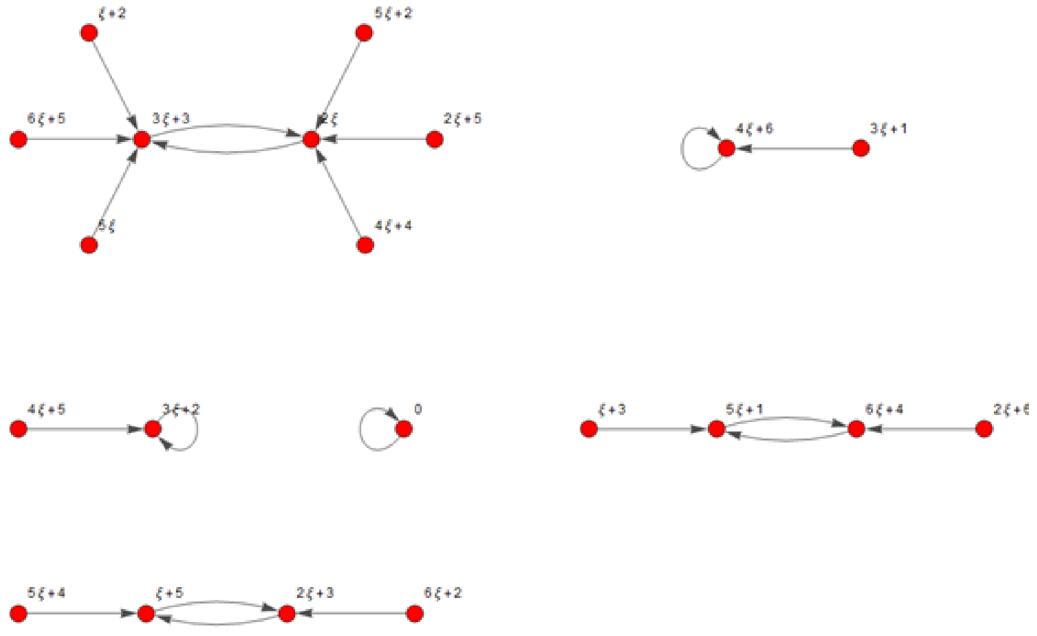
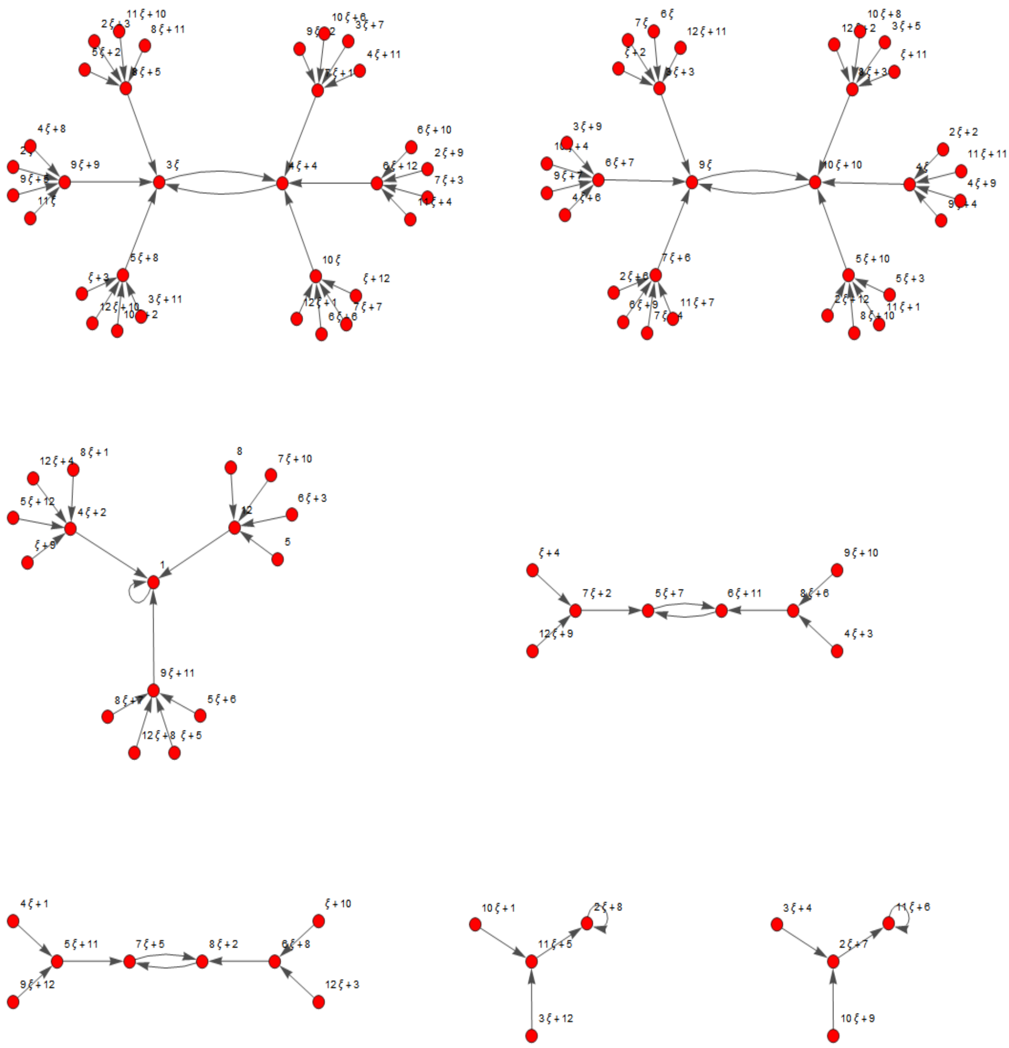


Figure 3: part of $G(\mathbb{Z}_7[\xi])$

If n is a prime satisfies $n \equiv 1\ \ mod\ 3$, then $a^2 + b^2 = ab$ for some non-zero elements $a, b \in \mathbb{Z}_n$, which means $N(z) = 0$ for some non-zero $z \in \mathbb{Z}_n[\xi]$. Therefore, we have $(n-1)^2$ units in $\mathbb{Z}_n[\xi]$ (see [3]), which means there are $2n$ non-units represented as loops and cycles. For instance, in $G(\mathbb{Z}_7[\xi])$ there are twelve non-unit elements as they appear in *Figure 3*.

Let $H(\mathbb{Z}_n)$ refer to the digraph of square mapping of $\mathbb{Z}_n$ as it is defined in [9]. According to the definition of the norm function, we know that N is a multiplicative function, i.e., $N(z^2) = N(z)N(z)$ for any $z \in \mathbb{Z}_n[\xi]$, also $N(z)$ is a positive integer number in $\mathbb{Z}_n$. Therefore, we can say that the mapping $N: V(G) \rightarrow V(H)$ is a homomorphism, that is, $N(uv) \in H(\mathbb{Z}_n)$ for any $uv \in G(\mathbb{Z}_n[\xi])$ and $N(0) = 0$. From Chinese remainder theorem we note (get, have, ….) that all cycles (including loops) are assigned to cycles or loops in $H(\mathbb{Z}_n)$. Thus, any component with a unit vertex cannot include nilpotent vertex. In addition, by getting the norm of one vertex we can determine the rest of the vertices in their component.



Corollary 3: *If* $\boldsymbol{N(z) = 0}$ *for some* $\boldsymbol{z \in V(G)}$*, then the norm of every vertex that connected to* $\boldsymbol{v}$ *in their component equals to zero.*

Proof: Trivial

In خطأ! المرجع الذاتي للإشارة المرجعية غير صحيح., we observed that vertices which are representing units and non-units form different loops and cycles. Since $N(z)$ is a multiplicative function, so all the vertices of any component are units or non-units.

Proposition 4: Let $z = a + b\xi$ be a vertex incident to α such that $N(z) = 0$, then z and $-z$ are the only two vertices incident to α.

Proof: Let the vertex $z = a + b\xi$ has norm zero and z is a root of the polynomial

$$x^2 - \alpha = 0, \tag{20}$$

then z and $-z$ are two roots of the polynomial (20).

Suppose that there is another root w different from z and $-z$, then

$$w^2 = \alpha \quad mod\, p$$

Let $w = c + d\xi$, then the following are hold.

$$\boldsymbol{a^2 - b^2 = c^2 - d^2,} \tag{21}$$

$$\boldsymbol{2ab - b^2 = 2cd - d^2,} \tag{22}$$

also,

$$\boldsymbol{a^2 + b^2 = ab,} \tag{23}$$

$$\boldsymbol{c^2 + d^2 = cd,} \tag{24}$$

Subtract (22) from (21) gives

$$\boldsymbol{a^2 - 2ab = c^2 - 2cd,} \tag{25}$$

By substitution of (23) and (24) in (25), we get

$$a^2 - 2(a^2 + b^2) = c^2 - 2(c^2 + d^2)$$

$$\boldsymbol{a^2 + 2b^2 = c^2 + 2d^2,} \tag{26}$$

Subtract (21) from (26) gives

$$3b^2 = 3d^2$$
$$d^2 = b^2$$

$$\boldsymbol{d = \pm b} \qquad (27)$$

By substitution of (27) in (21), we get

$$a^2 - b^2 = c^2 - b^2$$
$$a^2 = c^2$$
$$c = \pm a$$

Thus, the only roots of the polynomial (20) are z and $-z$.

Corollary *4: The indegree of a component with a non-unit vertex is two.*

3.3 Computer Calculations

In this section, we introduce calculations produced by Mathematica Notebook for calculating prime omega functions $\Omega(n)$, $\omega(n)$ and Carmichael function $\lambda(n)$. If n ≥ 2 and the unique prime factorization of n has the form $n = \prod_{i=1}^{k} p_i^{r_i}$, for distinct primes p_i, where $p_1 < p_2 < \ldots < p_k$ and $r_1, r_2, \ldots, r_k$ are positive integers. Then the prime omega functions $\Omega(n)$ counts the total number of prime factors of n considering their multiplicity, i.e., $\Omega(n) = r_1 + r_2 + \ldots + r_k$. However, the prime omega function $\omega(n)$ gives the number of distinct primes. I.e., the number k.

The Carmichael function associates to every positive integer n, a positive integer $\lambda(n)$, defined as the smallest positive integer m such that $a^m \equiv 1 \ (mod\, n)$, for every integer a between 1 and n that is coprime to n. In algebraic terms, $\lambda(n)$ is the exponent of the multiplicative group of integers modulo n. By the unique factorization theorem, any $n > 1$ can be written in a unique way as defined above. Then $\lambda(n)$ is the least common multiple of the λ of each of its prime power factors i.e., $\lambda(n) = \mathrm{lcm}\left(\lambda(p_1^{r_1}), \lambda(p_2^{r_2}) \ldots \lambda(p_k^{r_k})\right)$, which can be proved using the Chinese remainder theorem.

Also, the calculations care of the number of components NC, length of longest cycles LLC and the number of longest cycles NLC for the graph $G(\mathbb{Z}_n[\xi])$, see *Table 1*.

The prime factor counting functions and Carmichael function have many important number theoretic relations. The results are anticipated to present interesting information that can be very useful for further and comparison studies of the graph under investigation.

From the results obtained by Mathematica algorithm,

1. The vertices with indegree greater than 2 satisfies $N(z) \neq 0$ for all z in their component. (left for further investigations)
2. In the ring $z_p[\xi]$ with $p \equiv 1\, mod\, 3$ the norm of all vertices in the components with indegree 2 is zero. (left for further investigations)

Table 1 : Computer calculations show prime omega functions $\Omega(n)$ and $\omega(n)$, Carmichael lambda function $\lambda(n)$, the number of components NC, length of longest cycles LLC and number of longest cycles NLC for the graph $G(\mathbb{Z}_n[\xi])$, n=2,3, 4, …, 100.

n	$\Omega(n)$	$\omega(n)$	$\lambda(n)$	NC	LLC	NLC
2	1	1	1	3	2	1
3	1	1	2	3	2	1
4	2	1	2	3	2	1
5	1	1	4	3	2	1
6	2	2	2	10	2	6
7	1	1	6	10	2	6
8	3	1	2	3	2	1

n	$\Omega(n)$	$\omega(n)$	$\lambda(n)$	NC	LLC	NLC
9	2	1	6	15	2	13
10	2	2	4	10	2	6
11	1	1	10	6	4	3
12	3	2	2	10	2	6
13	1	1	12	10	2	6
14	2	2	6	36	2	28
15	2	2	4	10	2	6
16	4	1	4	3	2	1
17	1	1	16	4	6	1
18	3	2	6	58	2	54
19	1	1	18	24	6	14
20	3	2	4	10	2	6
21	2	2	6	36	2	28
22	2	2	10	22	4	12
23	1	1	22	6	10	3
24	4	2	2	10	2	6
25	2	1	20	21	4	18
26	2	2	12	36	2	28
27	3	1	18	51	6	36
28	3	2	6	36	2	28
29	1	1	28	16	12	6
30	3	3	4	36	2	28
31	1	1	30	70	4	60
32	5	1	8	3	2	1
33	2	2	10	22	4	12
34	2	2	16	14	6	4
35	2	2	12	36	2	28
36	4	2	6	58	2	54
37	1	1	36	24	6	14
38	2	2	18	92	6	56
39	2	2	12	36	2	28
40	4	2	4	10	2	6
41	1	1	40	16	12	6
42	3	3	6	136	2	120
43	1	1	42	98	6	68

n	$\Omega(n)$	$\omega(n)$	$\lambda(n)$	NC	LLC	NLC
44	3	2	10	22	4	12
45	3	2	12	58	2	54
46	2	2	22	22	10	12
47	1	1	46	7	22	2
48	5	2	4	10	2	6
49	2	1	42	98	6	68
50	3	2	20	82	4	72
51	2	2	16	14	6	4
52	3	2	12	36	2	28
53	1	1	52	20	36	6
54	4	2	18	202	6	144
55	2	2	20	22	4	12
56	4	2	6	36	2	28
57	2	2	18	92	6	56
58	2	2	28	60	12	24
59	1	1	58	21	28	15
60	4	3	4	36	2	28
61	1	1	60	70	4	60
62	2	2	30	276	4	240
63	3	2	6	228	2	220
64	6	1	16	3	2	1
65	2	2	12	36	2	28
66	3	3	10	84	4	48
67	1	1	66	124	10	114
68	3	2	16	14	6	4
69	2	2	22	22	10	12
70	3	3	12	136	2	120
71	1	1	70	37	12	20
72	5	2	6	58	2	54
73	1	1	72	24	6	14
74	2	2	36	92	6	56
75	3	2	20	82	4	72
76	3	2	18	92	6	56
77	2	2	30	84	4	48
78	3	3	12	136	2	120

n	$\Omega(n)$	$\omega(n)$	$\lambda(n)$	NC	LLC	NLC
79	1	1	78	142	12	132
80	5	2	4	10	2	6
81	4	1	54	159	18	108
82	2	2	40	60	12	24
83	1	1	82	25	60	12
84	4	3	6	136	2	120
85	2	2	16	14	6	4
86	2	2	42	368	6	292
87	2	2	28	60	12	24
88	4	2	10	22	4	12
89	1	1	88	24	60	4
90	4	3	12	228	2	220
91	2	2	12	136	2	120
92	3	2	22	22	10	12
93	2	2	30	276	4	240
94	2	2	46	24	22	10
95	2	2	36	92	6	56
96	6	2	8	10	2	6
97	1	1	96	10	2	6
98	3	2	42	368	6	292
99	3	2	30	142	4	84
100	4	2	20	82	4	72

3. Conclusion

This study investigates the ring of Eisenstein integers modulo n under the mapping $\varphi(z) = \mathrm{z}^2, \ \mathrm{z} = \mathrm{a} + \mathrm{b}\xi$, where ξ is the primitive third root of unity. The mapping represents the directed graph $G(\mathbb{Z}_n[\xi])$. Many properties of the diagraph vertices, components and closed paths are studied. Our contribution introduced very interesting results in the field of graph theory. The study was supported by calculations obtained by applications of computer arithmetic using Wolfram Mathematica.

References

[1] Wright, Steve. Quadratic residues and non-residues. Springer International Publishing Switzerland, 2016.

[2] Karaivanov, Borislav, and Tzvetalin S. Vassilev. "On Certain Sums Involving the Legendre Symbol." Integers 16.2 (2016).

[3] Alkam, Osama, and Emad Abu Osba. "On Eisenstein integers modulo n." International Mathematical Forum. Vol. 5. No. 22. 2010.

[4] Buçaj, Valmir. "Finding Factors of Factor Rings over Eisenstein Integers." International Mathematical Forum. Vol. 9. No. 31. 2014.

[5] Alkam, Osama, and Emad Abu Osba. "Zero Divisor Graph for the Ring of Eisenstein Integers Modulo." Algebra 2014 (2014).

[6] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory,Springer, 1992.

[7] Jarvis, Katherine, and Monica Nevins. "ETRU: NTRU over the Eisenstein Integers." Designs, Codes and Cryptography 74.1 (2015): 219-242.

[8] T.D. Rogers, The graph of the square mapping on the prime fields, Discrete Math. 148 (1996) 317–324.

[9]L. Szalay, A discrete iteration in number theory (Hungarian) BDTF Tud. Kozl. VIII. Termeszettudomanyok 3, Szombathely, 1992, pp. 71–91.

[10] Daoub, Hamza. "On Digraphs Associated to Quadratic Congruence Modulo n." University Bulletin–ISSUE No. 19 3 (2017).