Quadratic Residues of Commutative Rings

Shakila Banu P
Assistant professor of Mathematics
Vellalar College for Women,Thindal,
Erode, India
shakimeeran10@gmail.com

Suganthi T
B.T.Assistant of Mathematics
Govt.Hr.Sec.School,Vadugam
Namakkal , Tamilnadu
sugan1306thi@gmail.com

ABSTRACT

The organization of the quadratic residues and non-residues of a ring is introduced in this study as $Z_P+wZ_p+w^2Z_p+\ldots+w^{k-1}Z_p$,$w^k=1$,p=2,3. We discover the universal formula for the ring's total number of quadratic residues. By integrating graph theory with algebraic concepts, certain complete graphs were discovered in the ring.

Keywords: Commutative ring, Quadratic Residues, Complete graph

I. INTRODUCTION

The concept of algebraic integers and polynomial rings are the roots of ring theory research. Zahlring was first used by David Hilbert in 1897. A ring that performs two binary operations and satisfies certain requirements is known as a set.If multiplication is commutative, then the ring is as well. Rings that are commutative are simpler to comprehend than those that are not. David S.Dummit investigated rings and commutative rings [1]. In [1-4], many number kinds and their characteristics were examined.In the seventeenth and eighteenth century, Fermat, Euler, Lagrange, and Legendre investigated the quadratic residues of an integer. For factoring big numbers and acoustical engineering, quadratic residues are used. Finding quadratic residues of an integer and counting them is simple. However, it is not possible to count the quadratic residues of a commutative ring in the same way as an integer. We utilised residue properties of commutative chain or non-chain rings to graphs in order to put the transition from ring theory to graph theory. In [7], graphs and their byproducts, such as cartesian, lexiographic, tensor, and strong products, were investigated. If the squares of vertices x and y under mod n are the same, Rezaei [6] constructed graphs whose points x and y belong to two different sorts nearby and whose vertex set is a reduced residue system mod n. In [8], graphic code structures were found. The quadratic residues and non-residues from a commutative ring $Z_P+wZ_p+w^2Z_p+\ldots+w^{k-1}Z_p$,$w^k=1$,p=2,3 are studied in this article. We discover the generic formula to count the ring's quadratic residues.We learned about various regular graphs from the ring's residue feature.

II. PRELIMINARIES

In this section, we look into certain basic ring theory and graph theory ideas.

- The mathematical equivalent of a collection of unique objects is a set. Any sort of mathematical object, including numbers, symbols, lines, points in space, other geometric structures, variables, or even other sets, can be one of a set's elements or members.

- • A group is a nonempty set S with the binary operation: $*$: S×S → S satisfying the axioms listed below:
  (i) Closure: if $s_1,s_2 \in S$, then $s_1 * s_2 \in S$.
  (ii) Associativity: $s_1 * (s_2 * s_3) = (s_1 * s_2) * s_3$for all $s_1, s_2, s_3 \in S$.
  (iii) Identity: there is an element $e \in S$, like that $s_1 * e = e * s_1 = s_1$ for all $s_1 \in S$.
  (iv) Inverse: for each element $s_1 \in S$, there is an element $s_2 \in S$ like that $s_1 * s_2 = e = s_2 * s_1$.
- A group S is alleged to be abelian (or commutative) if $s_1 * s_2 = s_2 * s_1$ for all $s_1, s_2 \in S$.

Example: 2.1

$\mathbb{Z}$ is an addition-based abelian group.

Having the binary operations + and ×, a ring is a nonempty set R that satisfies the following operations:
A group that is abelian is (i)(R, +).
It is monoid in (ii)(R, ×).
Addition is governed by distributive laws in (iii)(R, ×).
If ring R maintains commutativity when multiplied, it is referred to as a commutative ring.
If every element of R has a multiplicative inverse, then R is a field of a unity-containing commutative ring.

To have the ability to able to obtain graphs from commutative ring ,we must to know certain fundamentals of graph theory.

The study of mathematical models used to depict pairwise relationships between objects is known as graph theory. A graph is a mathematical structure made up of a set of lines linking various pairs of vertices, some of which may be empty, and a collection of points called vertices. It's possible that the edges will be directed or oriented. The lines are referred to as arcs or edges depending on whether they are directed or undirected.Let G=(V,E) being a graph,where V the collection of all vertices and E={(x is close to y /x and y are vertices of V}.

A graph that is simple is one in which there is only one edge connecting any two vertices., and no edge begins or finishes at the same vertex. To put it another way, a simple graph is one that has few loops and edges. Two vertices are considered to be close by if an edge (arc) links them.. Each vertex in a directed graph has a direction attached to it, in addition to the vertices have connections by edges.

Edges are typically shown by arrows pointing in the direction that the graph can be traversed. The edges of an undirected graph are bidirectional and have no corresponding orientation. As a result, there are two ways to examine the graph. The graph is undirected because there isn't an arrow in it.Every pair of vertices in a graph must be connected by exactly one edge for it to be considered complete.

- • A complete graph with exactly 'n' vertices contains exactly nC_2 edges.
- K_n stands for a complete graph with 'n' vertices.
- **Example:2.2**

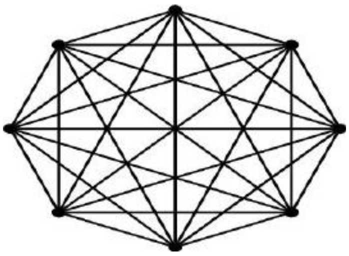

Figure:1 K_8

III. QUADRATIC RESIDUES

In this section, we examine the ring's component parts' structural details $\dot{R}=Z_P+wZ_p+w^2Z_p+\ldots.+w^{k1}Z_p$,$w^k=1,p=2,3$. The ring's quadratic residues and quadratic non-residues were identified.If there is an integer x such that $x^2 \equiv q(\text{mod } n)$, then an integer q is referred to as a quadratic residue of n in number theory.Otherwise, q is referred to as a quadratic n-residue.

Example:2.3

Let $Z_7=\{0,1,2,3,4,5,6\}$.

Since all the elements of commutative ring Z_7 has multiplicative inverse , Z_7 is a field.

$1^2=1(\text{mod } 7)$, $2^2=4(\text{mod } 7)$

$3^2=2(\text{mod } 7)$, $4^2=2(\text{mod } 7)$, $5^2=4(\text{mod } 7)$, $6^2=1(\text{mod } 7)$. Therefore, quadratic residues of $Z_7=\{1,2,4\}$

A.Quadratic Residues over ₿$_k$= $Z_2+\alpha Z_2+\alpha^2 Z_2+\ldots.+\alpha^{k-1}Z_2$, $\alpha^k=1$

Consider ₿$_k$= $Z_2+\alpha Z_2+\alpha^2 Z_2+\ldots.+\alpha^{k-1} Z_2$, $\alpha^k=1$ where $Z_2=\{0,1\}$.

Every element ҕ of ₿$_k$, it looks like $a+b\alpha+c\alpha^2+\ldots.+z\alpha^{k-1}$,Here $a,b,c,z \in Z_2$.

An element of ₿ referred to as a quadratic residue. if ҕ$^2 \equiv$ ꞑ (mod $\alpha^k=1$)

Take over the ring,₿$_2$.= $Z_2+\alpha Z_2=\{0,1, \alpha,1+\alpha\}$, $\alpha^2=1$.since ₿$_2$ satisfy the commutative ring properties, ₿$_2$ is a commutative ring.The set of all quadratic residue of ₿$_2$ is $\dot{r}_2=\{1,0\}$ and the set of all quadratic non-residues $=\{\alpha,1+\alpha\}$. Let ₿$_3$= $Z_2+\alpha Z_2+\alpha^2 Z_2$, $\alpha^3=1$ is a commutative ring .₿$_3$= $\{0,1, \alpha,1+\alpha, \alpha^2,1+\alpha^2, \alpha+\alpha^2,1+\alpha+\alpha^2\}$

Quadratic residues $\dot{r}_3$ =₿$_3$.Let ₿$_4$= $Z_2+\alpha Z_2+\alpha^2 Z_2+\alpha^3 Z_2$, $\alpha^4=1$.

₿$_4$=$\{0,1, \alpha,1+\alpha, \alpha^2,1+\alpha^2, \alpha+\alpha^2,1+\alpha+\alpha^2, \alpha^3, 1+\alpha^3, \alpha+\alpha^3,1+\alpha+\alpha^3, \alpha^2+\alpha^3,1+\alpha^2+\alpha^3, \alpha+\alpha^2+\alpha^3,1+\alpha+\alpha^2+\alpha^3\}$

Residues of ₿$_4$ is $\dot{r}_4=\{0,1+\alpha^2, 1+\alpha+\alpha^2, 1+\alpha+\alpha^3\}$

Let ₿$_5$= $Z_2+\alpha Z_2+\alpha^2 Z_2+\alpha^3 Z_2+\alpha^4 Z_2$, $\alpha^5=1$.In this ring $\dot{r}_5$= ₿$_5$.

By proceeding in this manner, we are able to obtain the commutative ring's elements and quadratic residues $Z_2+\alpha Z_2+\alpha^2 Z_2+\ldots.+\alpha^{k-1}Z_2$ where , $\alpha^k=1$.

Theorem:3.1

Let ₿$_k$= $Z_2+\alpha Z_2+\alpha^2 Z_2+\ldots.+\alpha^{k-1} Z_2$, $\alpha^k=1$ be a commutative ring.Then the number of quadratic residues of ₿$_k$

$$= \begin{cases} k, \alpha^k = 1 \text{ and } k \text{ is even number} \\ 2^k, \alpha^k = 1 \text{ and } k \text{ is odd number} \end{cases}$$

B. Quadratic Residues over Ꜩ$_k=Z_3+\beta Z_3+\beta^2Z_3+\ldots.+\beta^{k-1}Z_3$, $\beta^k=1$

We investigate the structural features of the ring's constituent pieces in this section.$Z_3+\beta Z_3+\beta^2Z_3+\ldots.+\beta^{k-1}Z_3$, $\beta^k=1$.

Consider Ꜩ$_k= Z_3+\beta Z_3+\beta^2Z_3+\ldots.+\beta^{k-1}Z_3$, $\beta^k=1$ where $Z_3=\{0,1,2\}$.

Every element ꜩ of Ꜩ$_k$ is of the form $a+b\beta+c\beta^2 +\ldots.+z\beta^{k-1}$,Here a,b,c,..z $\in Z_3$.

Consider the ring, Ꜩ$_2=Z_3+\beta Z_3$, $\beta^2=1$.

Ꜩ$_2=\{0,1, \beta,1+\beta,2\beta,1+2\beta,2,2+\beta,2+2\beta \}$

since Ꜩ$_2$ satisfy the commutative ring properties,Ꜩ$_2$ is a commutative ring.The set of all quadratic residue of the ring is ẗ$_2 =\{1,2+2\beta,2+\beta \}$and the set of all quadratic non-residues $=\{0, \beta,1+\beta,2\beta,1+2\beta,2 \}$.

Let Ꜩ$_3 = Z_3+ \beta Z_3+ \beta^2Z_3$, $\beta^3=1$ is a commutative ring.

$=\{0,1,2,\beta,2\beta,1+\beta,2+\beta,1+2\beta,2+2\beta,\beta^2,1+\beta^2,2+\beta^2,\beta+\beta^2,2\beta+\beta^2,1+\beta+\beta^2,2+\beta+\beta^2,1+2\beta+\beta^2,2+2\beta+\beta^2,2\beta^2, 1+2\beta^2,2+2\beta^2,\beta+2\beta^2,2\beta+2\beta^2,1+\beta+2\beta^2,2+\beta+2\beta^2,1+2\beta+2\beta^2, 2+2\beta+2\beta^2 \}$

Quadratic residues ẗ$_3 =\{ 0,1,\beta^2,1+2\beta+\beta^2,2\beta+2\beta^2,2+2\beta, 2+2\beta^2,1+\beta+\beta^2,\beta,2+\beta+\beta^2,1+\beta+2\beta^2 \}$.

Let Ꜩ$_4 = Z_3+\beta Z_3+\beta^2Z_3+ \beta^3 Z_3$, $\beta^4=1$.

Ꜩ$_4 =\{0,1,2,\beta,2\beta,1+\beta,2+\beta,1+2\beta,2+2\beta,\beta^2,1+\beta^2,2+ \beta^2, \beta+ \beta^2,2\beta+ \beta^2,1+\beta+\beta^2,2+\beta+\beta^2,1+2\beta+\beta^2,2+2\beta+ \beta^2,2\beta^2,1+2 \beta^2,2+2\beta^2,\beta+2\beta^2,2\beta+2\beta^2,1+\beta+2\beta^2,2+\beta+2\beta^2,1+2\beta+2\beta^2,2+2\beta+2\beta^2,\beta^3,1+\beta^3,2+\beta^3,\beta+\beta^3,2\beta+\beta^3,1+\beta+\beta^3,2+\beta+\beta^3,1+2\beta +\beta^3,2+2\beta+\beta^3,\beta^2+\beta^3,1+\beta^2+\beta^3,2+\beta^2+\beta^3,\beta+\beta^2+\beta^3,2\beta+\beta^2+\beta^3,1+\beta+\beta^2+\beta^3,2+\beta+\beta^2+\beta^3,1+2\beta+\beta^2+\beta^3,2+2\beta+\beta^2+\beta^3,2\beta^2+ \beta^3,1+2\beta^2+\beta^3,2+2\beta^2+\beta^3,\beta+2\beta^2+\beta^3,2\beta+2\beta^2+\beta^3,1+\beta+2\beta^2+\beta^3,2+\beta+2\beta^2+\beta^3,1+2\beta+2\beta^2+\beta^3,2+2\beta+2\beta^2+\beta^3,2\beta^3,1+2\beta^3,2 +2\beta^3,\beta+2\beta^3,2\beta+2\beta^3,1+\beta+2\beta^3,,2+\beta+2\beta^3,1+2\beta+2\beta^3,2+2\beta+2\beta^3,\beta^2+2\beta^3,1+\beta^2+2\beta^3,2+\beta^2+2\beta^3,\beta+\beta^2+2\beta^3,2\beta+ \beta^2+2\beta^3,1+\beta+ \beta^2+2\beta^3,2+\beta+ \beta^2+2\beta^3,1+2\beta+ \beta^2+2\beta^3,2+2\beta+ \beta^2+2\beta^3,2\beta^2+2\beta^3,1+2 \beta^2+2\beta^3,2+2 \beta^2+2\beta^3,\beta+2 \beta^2+2\beta^3,2\beta+2 \beta^2+2\beta^3,1+\beta+2 \beta^2+2\beta^3,2+\beta+2 \beta^2+2\beta^3,1+2\beta+2 \beta^2+2\beta^3,2+2\beta+2\beta^2+2\beta^3 \}$

Residues of Ꜩ$_4$ is ẗ$_4=\{\beta^2,2+2\beta^2,1+2\beta^2,1,1+\beta^2+2\beta^3,1+\beta^2+\beta^3,1+2\beta+\beta^2,2\beta+2\beta^2+2\beta^3,2+2\beta+2\beta^2+\beta^3,1+\beta+\beta^2, \beta+2\beta^2+\beta^3,2+\beta^2,\beta+2\beta^3,2\beta+\beta^3,1+2\beta+\beta^2,2+2\beta+2\beta^3,1+2\beta+\beta^2+2\beta^3,2+\beta+\beta^3,1+\beta+\beta^2+\beta^3,2+\beta+2\beta^2+2\beta^3\}$

By proceeding in this manner, we are able to obtain the commutative ring's elements and quadratic residues $Z_3+\beta Z_3+\beta^2 Z_3+\ldots.+\beta^{k-1}Z_3$,$\beta^k=1$.

Theorem:3.2

Let Ꜩ$_k = Z_3+\beta Z_3+\beta^2 Z_3+\ldots+\beta^{k-1} Z_3$,$\beta^k=1$ be a commutative ring.Then, the total number of quadratic residues of

$$\text{Ꜩ}_k= \begin{cases} 2^k-1, if\ \beta^k=1, k=2 \\ 2^k+1,\ \ if\ \beta^k=1, k>2\ and\ k\ is\ positive\ integer \end{cases}$$

IV.QUADRATIC RESIDUE GRAPH OVER $\dot{R}=Z_P+w\ Z_p+w^2\ Z_p+\ldots.+w^{k-1}\ Z_p$,$w^k=1$

A simple graph G is a graph with quadratic residues G_n [7] using an edge set E and a vertex set V where

$V(G_n)=\{x \in Z_n/(x,n)=1$ and $x<n\}$ and $E(G_n) =\{xy/x,y\in V(G_n)$ and $x^2\equiv y^2 \pmod{n}\}$

Let $Z_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

$V(G_{12})=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

Here,$1^2=5^2=7^2=11^2\equiv1$(mod 12),$2^2=4^2=8^2=10^2\equiv4$ (mod 12),$3^2= 9^2\equiv49$(mod 12), $0^2= 6^2\equiv0$(mod 12)

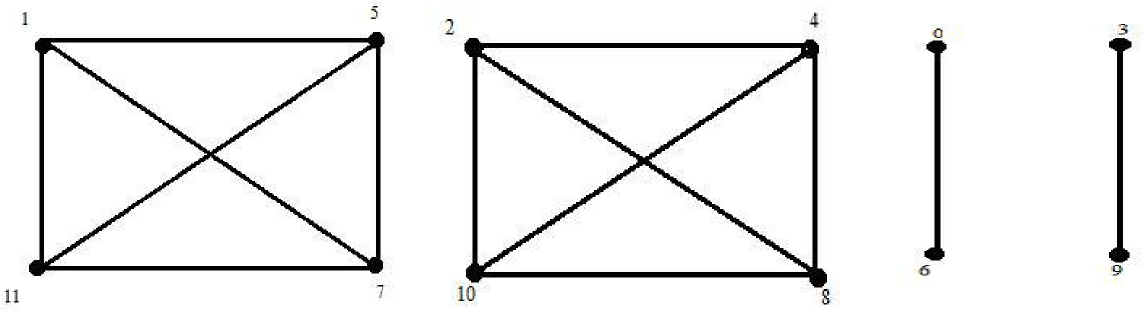

Figure 2: G(Z$_{12}$)

In this section ,we study about quadratic residue graph over $Z_P+w\ Z_p+w^2\ Z_p+\ldots.+w^{k-1}\ Z_p$,$w^k=1$, p=2 or 3.if their vertex sets are reduced residue systems mod $w^k=1$.

$V(G)=\{a \in \dot{R}\}$

$E(G)=\{x$ is adjacent to $y/x,y \in V(G)$ and $x^2=y^2$ (mod $w^k=1$)$\}$.Here,w ‘s are congruent under $w^k=1$ and element of Z_p are congruent under modulo p in the product and addition of polynomials over $\dot{R}$.

Throughout this paper,we consider G is undirected graph only.

Theorem:4.1

Let G(฿$_k$)=(V,E), be a quadratic residue graph where k is even .Then the graph is k types of complete graph and $|V|=2^k$.

Example:

Let ฿$_4= Z_2+\alpha Z_2+\alpha^2Z_2+ \alpha^3 Z_2$, $\alpha^4=1$.

This is commutative ring has four quadratic residues twelve quadratic non residues.

The graph generated by the ring ฿$_4$ is a Quadratic residue graph which has the following vertices and edges :

V(฿$_4$) $=\{0,1, \alpha,1+\alpha, \alpha^2,1+ \alpha^2, \alpha+\alpha^2,1+\alpha+\alpha^2, \alpha^3, 1+ \alpha^3, \alpha+ \alpha^3,1+\alpha+\alpha^3, \alpha^2+\alpha^3,1+ \alpha^2+\alpha^3, \alpha+ \alpha^2+\alpha^3,1+ \alpha+ \alpha^2+\alpha^3\}$

E(Ᵽ$_4$)=$\{(0,1+\boldsymbol{\alpha}^2),(0,1+\alpha+\alpha^2+\alpha^3),(1+\alpha^2,1+\alpha+\alpha^2+\alpha^3),(\alpha^2,\alpha+\alpha^2+\alpha^3)(1,1+\alpha+\alpha^3),(1,\alpha^2),(1,1+\alpha^2+\alpha^3),(\alpha+\alpha^2+\alpha^3,1+\alpha+\alpha^3),(\alpha^2,1+\alpha+\alpha^3),(\alpha,\alpha^3),(\alpha,1+\alpha^2+\alpha^3),(\alpha,1+\alpha+\alpha^2),(\alpha^3,1+\alpha^2+\alpha^3),(1+\alpha+\alpha^2,1+\alpha^2+\alpha^3),(\alpha^3,1+\alpha+\alpha^2),(\alpha+\alpha^2,\alpha+\alpha^3),(\alpha+\alpha^2,\alpha^2+\alpha^3),(1+\alpha^3,1+\alpha),(1+\alpha^3,\alpha^2+\alpha^3),(\alpha+\alpha^3,1+\alpha),(\alpha+\alpha^2,1+\alpha^3),(1+\alpha^3,\alpha+\alpha^3),(1+\alpha,\alpha^2+\alpha^3),(\alpha+\alpha^3,\alpha^2+\alpha^3),(\alpha+\alpha^2,1+\alpha)\}$

Quadratic binary Residue graph is given below:

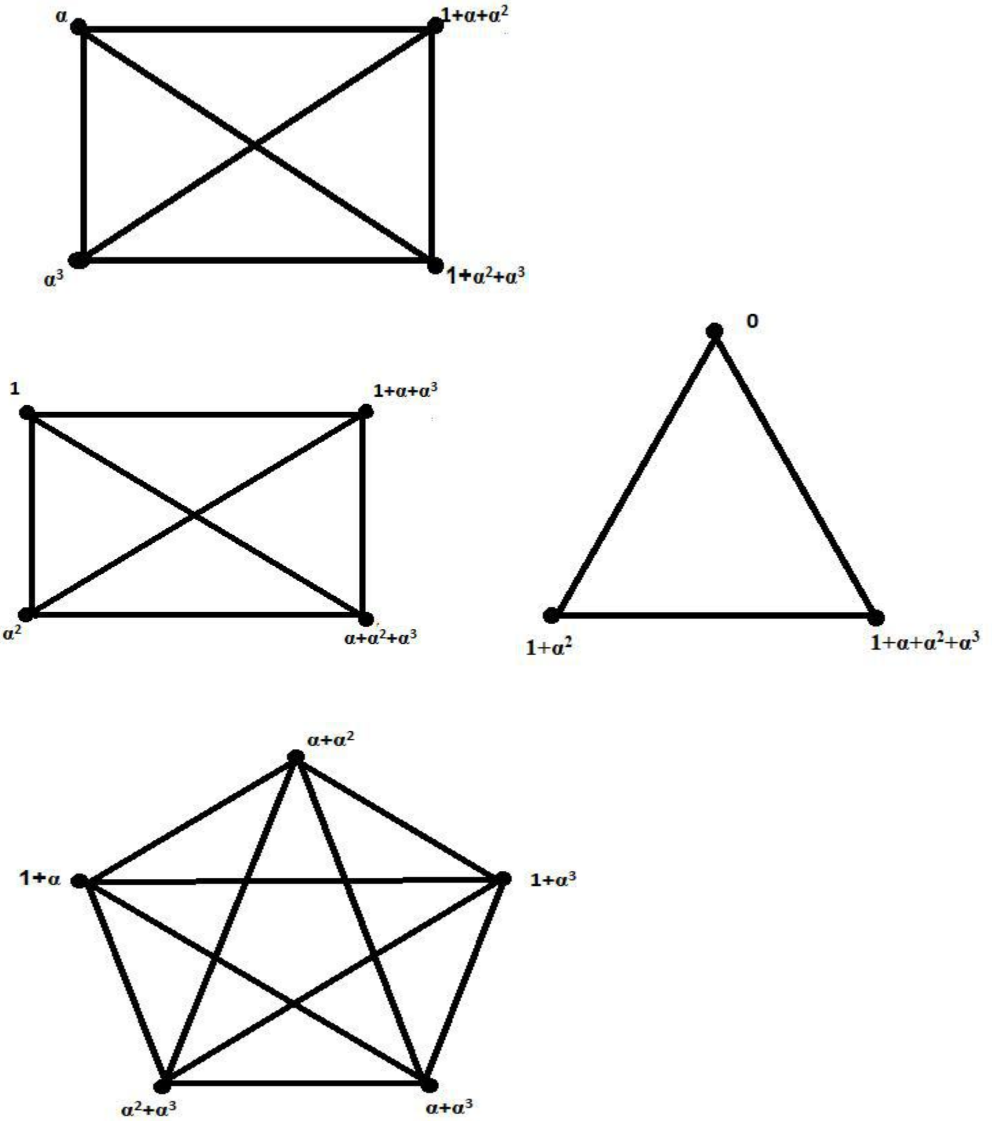

Figure 3: **G(Ᵽ$_4$)**

Theorem:4.2

Let G(Ŧk)=(V,E), be a graph of quadratic residue.The graph is then one of three types of complete graphs with |V|=3^k

Example:

Let Ꜩ $_4$ = $Z_3+\beta Z_3+\beta^2 Z_3+\beta^3 Z_3$, $\beta^4=1$.

It is a commutative ternary ring with eighty one elements .Quadratic residue graph obtained from the ring with the following vertices ..

V(Ꜩ $_4$) =$\{0,1,2,\beta,2\beta,1+\beta,2+\beta,1+2\beta,2+2\beta,\beta^2,1+\beta^2,2+\beta^2,\beta+\beta^2,2\beta+\beta^2,1+\beta+\beta^2,2+\beta+\beta^2,1+2\beta+\beta^2,2+2\beta+\beta^2,2\beta^2,1+2\beta^2,2+2\beta^2,\beta+2\beta^2,2\beta+2\beta^2,1+\beta+2\beta^2,2+\beta+2\beta^2,1+2\beta+2\beta^2,2+2\beta+2\beta^2\}$

Quadratic Ternary Residue graph over Ꜩ $_4$ is shown below:

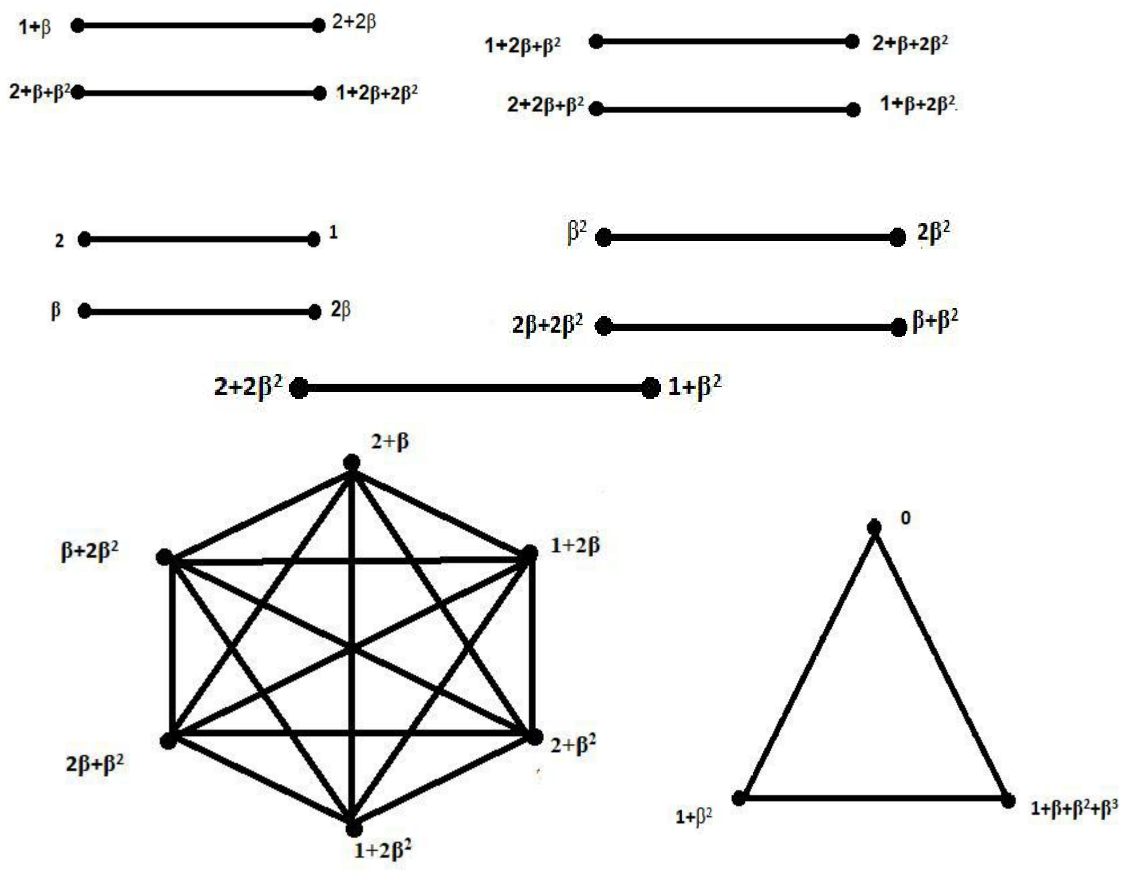

Figure 3: G(Ʒ 4)

Conclusion:

We describe the structure of quadratic residues in a commutative ring in this study. Complete graphs were found in the ring by using algebraic ideas to graph theory. The author hopes to expand the work to include the encoding and decoding of commutative rings in future research.

REFERENCES

[1] David S.Dummit,Richard M.Foote,Abstract algebra,third edition,Wiley India Pvt.Ltd.,Delhi,(2014).ISBN:978-81-265-3228-5.

[2] G. H.Hardy,E. M. Wright, An introduction to the theory of numbers (fifth ed,(1980).), Oxford: Oxford University Press.

[3] Ireland, Kenneth, Rosen, and Michael, A classical introduction to modern number theory,(second ed.), New York: Springer (1990).

[4] H. Kenneth, Rosen, Elementary number theory and its application, Addison-Wesley Publishing company,(1984).

[5] Lemmermeyer, Franz, Reciprocity laws: from Euler to Eisenstein, Berlin: Springer, (2000).

[6] F.J.Macwilliams,Theory of error correcting codes,North-Holland Mathematical library,(1983).

[7] Rezaei, Mehdi & Rehman, Shafiq & Khan, Zia & Baig,A, & Farahani, Mohammad, Quadratic residues graphs , International Journal of Pure and Applied Mathematics,βol.113. pp.465-470,DOI: 10.12732/ijpam.v113i3.8.(2017).

[8] F.Harray, Graph theory, Addison Wesley,(1969).

[9] El. Rouayheb,Salim &Geroghiades,Costas,Graph theorectic methods in coding Theory, vol.10,DOI: 1007/978-1-4419-6624-7-5,(2011).