International Journal of Pure and Applied Mathematics
Volume 113 No. 3 2017, 465-470
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v113i3.8

QUADRATIC RESIDUES GRAPHS

M. Rezaei[1], S.U. Rehman[2], Z.U. Khan[2], A.Q. Baig[2], M.R. Farahani[3] §

[1]Department of Mathematics
Buein Zahra Technical University
Buein Zahra, Qazvin, IRAN

[2]Department of Mathematics
COMSATS Institute of Information Technology
Attock, PAKISTAN

[3]Department of Applied Mathematics

Iran University of Science and Technology
IRAN

Abstract: We introduce and study the graphs whose vertex set is reduced residue system *mod n* such that two distinct vertices a and b are adjacent provided that $a^2 \equiv b^2 \ (mod\ n)$.

AMS Subject Classification: 13A15, 13F05.
Key Words: Quadratic residues, complete graphs, union of graph.

1. Introduction

Graphs can be used to model many types of relations and processes in physical, biological, social and information systems. Many practical problems can be represented by graphs to emphasize their application to real-world systems. Graph theory is the study of mathematical structures used to model pairwise relations between objects. A graph in this context is made up of vertices, nodes, or points which are connected by edges, arcs, or lines. A graph may be undirected, meaning that there is no distinction between the two vertices

Received: December 10, 2016
Revised: January 17, 2017
Published: March 28, 2017

§Correspondence author

associated with each edge, or its edges may be directed from one vertex to another. Graphs are one of the prime objects of study in discrete mathematics.

If G and H are disjoint graphs, their union $G \cup H$ is the graph with $V(G \cup H) = V(G) \cup V(H)$ and $E(G \cup H) = E(G) \cup E(H)$. Thus $G \cup H$ consist of a copy of G together with a copy of H.

In number theory, an integer q is called a quadratic residue modulo n if it is congruent to a perfect square modulo n; i.e., if there exists an integer x such that, $x^2 \equiv q \pmod{n}$ and $(q, n) = 1$. The trivial case $q = 0$ is generally excluded from lists of quadratic residues so that the number of quadratic residues $(mod\ n)$ is taken to be one less than the number of squares $(mod\ n)$. However, some source include 0 as a quadratic residue. Otherwise, q is called a quadratic non-residue modulo n. If p is an odd prime then no of quadratic and non-quadratic residues for $mod\ p$ is $\left(\frac{p-1}{2}\right)$.

Originally an abstract mathematical concept from the branch of number theory known as modular arithmetic, quadratic residues are now used in applications ranging from acoustical engineering to cryptography and the factoring of large numbers.

We recall the key definition of this paper.

Definition 1.1. Let $n \geq 2$ be a fixed positive integer. We call a simple graph is a quadratic residue graph modulo n if its vertex set is reduced residue system $mod\ n$ such that two distinct vertices a and b are adjacent provided that $a^2 \equiv b^2\ (mod\ n)$. We denote by ζ_n the quadratic residue graph modulo n, i.e., $V(\zeta_n) = \{a \in \mathbb{Z} \mid (a, n) = 1\ and\ a < n\}$ and $E(\zeta_n) = \{ab \mid a, b \in V(G)\ and\ a^2 \equiv b^2\ (mod\ n)\}$.

Example 1.2. Let $n = 7$, then

$$V(\zeta_7) = \{1, 2, 3, 4, 5, 6\} \text{ and } E(\zeta_7) = \{1\ 6, 2\ 5, 3\ 4\}.$$

So ζ_7 is as follows:

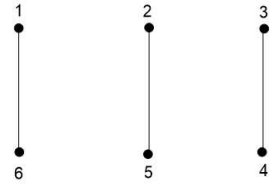

Fig. 1: ζ_7

Example 1.3. Let $n = 16$, then

$$V(\zeta_{16}) = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

and

$$E(\zeta_{16}) = \{1\ 7, 1\ 9, 1\ 15, 7\ 9, 7\ 15, 9\ 15, 3\ 5, 3\ 11, 3\ 13, 5\ 11, 5\ 13, 11\ 13\}.$$

So ζ_{16} is as follows:

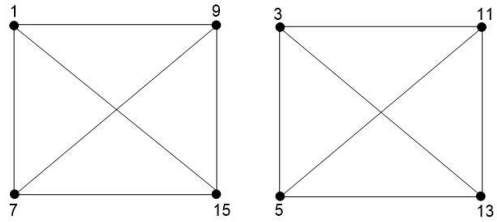

Fig. 2: ζ_{16}

Example 1.4. Let $n = 24$, then

$$V(\zeta_{24}) = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

and

$$E(\zeta_{24}) = \{1\ 5, 1\ 7, 1\ 11, 1\ 13, 1\ 17, 1\ 19, 1\ 23, 5\ 7, 5\ 11, 5\ 13, 5\ 17, 5\ 19, 5\ 23,$$
$$7\ 11, 7\ 13, 7\ 17, 7\ 19, 7\ 23, 11\ 13, 11\ 17, 11\ 19, 11\ 23, 13\ 17, 13\ 19, 13\ 23,$$
$$17\ 19, 17\ 23, 19\ 23\}.$$

So ζ_{24} is as follows:

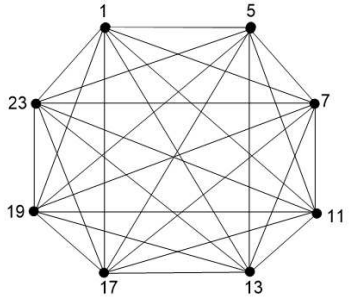

Fig. 3: ζ_{24}

2. Main Results

We denote by $G \oplus H$, the disjoint union of the graphs G and H and by $nG = G \oplus G \oplus \cdots \oplus G$, the disjoint union of the n copies of the graph G.

Theorem 2.1. *Let ζ_n be a quadratic residue graph.*

1. *If $n = 2$ then ζ_n is empty graph.*
2. *If $n = 2^2$, then $\zeta_n = K_2$.*
3. *If $n = 2^r$, where $r \geq 3$ is any integer, then $\zeta_n = 2^{k-3}K_4$.*
4. *If n is an odd prime then $\zeta_n = \dfrac{n-1}{2}K_2$.*
5. *If $n = p^r$ where p is an odd prime and r is positive integer then $\zeta_n = \dfrac{p^{r-1}(p-1)}{2}K_2$.*

Proof. The assertions (1) and (2) are straightforward.

(3): Note that the graph ζ_n has $\phi(2^r) = 2^{r-1}$ number of vertices. We compute the least positive residue of the square of the integers which are less than n and relatively prime with n. Since there are $\phi(n) = 2^{r-1}$ squares to be considered and since the congruence $x^2 \equiv a \ (mod\ 2^r)$ has either no solution or exactly 4 incongruent solutions, cf. [1, Exercise 9.1, Problem 18], there must be $\phi(n)/4 = 2^{r-1}/4 = 2^{r-3}$ number of quadratic residues among all the vertices. Hence $\zeta_n = 2^{r-3}K_4$.

(4): We compute the least positive residue of the square of the integers $1, 2, 3, .., n-1$. Since there are $\phi(n) = n-1$ squares to be considered and since the congruence $x^2 \equiv a \ (mod\ n)$ has either no solution or exactly 2 incongruent solutions, there must be $\phi(n)/2 = (n-1)/2$ number of quadratic residues among all the vertices. Hence $\zeta_n = \frac{n-1}{2}K_2$.

(5): Note that the graph ζ_n has $\phi(p^r) = p^{r-1}(p-1)$ number of vertices. We compute the least positive residue of the square of the integers which are less than n and relatively prime with n. Since there are $\phi(n) = p^{r-1}(p-1)$ squares to be considered and since the congruence $x^2 \equiv a \ (mod\ p^r)$ has either no solution or exactly 2 incongruent solutions, cf. [1, Exercise 9.1, Problem 16], there must be $\phi(n)/2 = p^{r-1}(p-1)/2$ number of quadratic residues among all the vertices. Hence $\zeta_n = \frac{p^{r-\mathbf{1}}(p-1)}{2}K_2$.

□

Theorem 2.2. *Let $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_m}^{\alpha_m}$; p_i are distinct odd primes and α_i are positive integers. Then:*

$$\zeta_n = \frac{\phi(n)}{2^m} K_{2^m}$$

Proof. Since the congruence $x^2 \equiv a \ (mod\ p_i^{\alpha_i})$ has either no solution or exactly 2 incongruent solutions, cf. [1, Exercise 9.1, Problem 16], therefore, by Chinese remainder theorem, there are exactly 2^m incongruent solutions of the congruence $x^2 \equiv a \ (mod\ n)$. There must be $\phi(n)/2^m$ number of quadratic residues among all the vertices. Hence $\zeta_n = \frac{\phi(n)}{2^m} K_{2^m}$. □

Theorem 2.3. *Let $n = 2^r \cdot {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_m}^{\alpha_m}$; p_i are distinct odd primes and α_i and r are positive integers. Then:*

$$\zeta_n = \begin{cases} \frac{\phi(n)}{2^m} K_{2^m} \ if\ r = 0 \ or\ 1 \\ \frac{\phi(n)}{2^{m+1}} K_{2^{m+1}} \ if\ r = 2 \\ \frac{\phi(n)}{2^{m+2}} K_{2^{m+2}} \ if\ r \geq 3 \end{cases}$$

Proof. Note that the congruence $x^2 \equiv a \ (mod\ 2^r)$ has either no solution or exactly 4 incongruent solutions, if $r \geq 3$, cf. [1, Exercise 9.1, Problem 18]. Also $x^2 \equiv a \ (mod\ 2^2)$ has two solutions and $x^2 \equiv a \ (mod\ 2)$ has one solution. Moreover, as mentioned in the proofs above, the congruence the congruence $x^2 \equiv a \ (mod\ p_i^{\alpha_i})$ has either no solution or exactly 2 incongruent solutions if p is an odd prime, cf. [1, Exercise 9.1, Problem 16]. By applying Chines remainder theorem we get that $x^2 \equiv a \ (mod\ n)$ has either no solution or 2^m solutions if $r = 0$ *or* 1. Also $x^2 \equiv a \ (mod\ n)$ has either no solution or 2^{m+1} solutions if $r = 2$. And finally, $x^2 \equiv a \ (mod\ n)$ has either no solution or 2^{m+2} solutions if $r \geq 3$. Hence the result. □

Theorem 2.4. *ζ_n is a complete graph K_n if and only if n is a divisor of* 24.

Proof. Suppose ζ_n is a complete graph K_n. Then $a^2 \equiv 1 \ (mod\ n)$ for every a in reduced residue system *mod* n. Suppose $n = 2^k m$ where m is odd and k is an integer ≥ 1. Then $a^2 \equiv 1 \ (mod\ 2^k)$ for all a in reduced in reduced residue system *mod* 2^k and $a^2 \equiv 1 \ (mod\ m)$ for all a in reduced residue system *mod* m.

In particular, $2^2 \equiv 1 \ (mod\ m)$ and $3^2 \equiv 1 \ (mod\ 2^k)$. Therefore, m divides 3 and 2^k divides 8. This implies that n divides 24. Conversely, if n is a divisor of 24, then $\zeta_n : \ n = 2, 3, 4, 6, 8, 12, 24$ is a complete graph K_n. □

Remark 2.5. The quadratic residue graph ζ_n is either a complete graph or disjoint union of complete graphs.

References

[1] Kenneth H. Rosen, Elementry Number Theory and its Application, *Addison-Wesley Publishing company* (1984).

[2] Hardy, G. H.; Wright, E. M., An Introduction to the Theory of Numbers (fifth ed.), *Oxford: Oxford University Press* (1980)

[3] Ireland, Kenneth; Rosen, Michael, A Classical Introduction to Modern Number Theory (second ed.), *New York: Springer* (1990)

[4] Lemmermeyer, Franz, Reciprocity Laws: from Euler to Eisenstein, Berlin: *Springer* (2000)