The 1st International Conference of the Faculties of Sciences
19- 20 Dec 2021

AN EXPOSITIONOF GRAPHS RELATEDTO FINITE COMMUTATIVE RINGS

Hamza Daoub
University of Zawia /Faculty of Science / Libya / h.daoub@zu.edu.ly

ABSTRACT

In this paper, we investigates the relation between the ring-theoretic properties of $R$and the graph-theoretic properties of $G(R)$, where $R$is a finite commutative ring with unity, and $G(R)$ is a simple undirected graph associated to R such that two deferent vertices $u, v \in V(G) = R$ are adjacent if $u^2 = v^2$. Rings of interest are $R = \mathbb{Z}/n\mathbb{Z}$.

Keywords*:Commutative ring, Simple graphs, Vertex degree, Regular graphs, Quadratic polynomial.*

الملخص

في هذا البحث، نحقق في العلاقة بين الخصائص النظرية للحلقة لـRوالخصائص النظرية للرسم البياني لـ$G(R)$ ، حيثRعبارة عن حلقة تبديلية منتهية ذاتعنصر محايد ،و$G(R)$هو رسم بياني بسيط غير موجه مرتبط بـ Rبحيث يكون الرأسان المختلفان $u, v \in V(G) = R$متجاوران إذا كان$u^2 = v^2$. الحلقات ذات الأهمية هي$R = \mathbb{Z}/n\mathbb{Z}$.

الكلمات المفتاحية :الحلقات التبديلية، الرسوم البيانية البسيطة، درجة الرأس، الرسوم البيانية المنتظمة، الحدوديات التربيعية.

Author Correspondent:h.daoub@zu.edu.ly

1. INTRODUCTION

Let n be a positive integer, the set of all congruence classes of integers for a modulo n is called the ring of integers modulo n and is denoted $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Since $\mathbb{Z}_n$ is finite, it has integer characteristic $char\mathbb{Z}_n = n$. If n is not a prime number, then $\mathbb{Z}_n$ has zero-divisors and $\mathbb{Z}_n[x]$ is not a unique factorization ring, that is, if $\alpha, \beta \neq 0$, then $(x-\alpha)(x+\alpha) = (x-\beta)(x+\beta)$,are two distinct, non-associated factorizations of

$$x^2 = amodn, \tag{1}$$

where $a = (\pm\alpha)^2 = (\pm\beta)^2$. If $n = p$ is a prime, then $\mathbb{Z}_n$don't havezero-divisors. However, if $\mathbb{Z}_n$ is a domain, then it is a field, and $\mathbb{Z}_n\ [x]$ is a unique factorization domain.

Given anintegern$n$, consider the graph $G(\mathbb{Z}_n)$ with vertex set $\mathbb{Z}_n$, where two deferent vertices u and $v$are adjacent exactly when $u^2 = v^2$.The graph presentedby $G(\mathbb{Z}_n)$ is a disconnected simple graph.

This article aims to expose the most recent developments in describing the structural properties of the graph $G(\mathbb{Z}_n)$of the finite commutative ring $\mathbb{Z}_n$.

For the sake of completeness some basic algebraic and number-theoretic notions, one can refer to[1, 2, 3].

2. PRELIMINARIES

Definition 2.1.*An integer a is called a* ***quadratic residue*** *of $n$if$(a,n) = 1$, and the congruence $x^2 \equiv a\ (modn)$ has a solution. Otherwise, a is called a* ***quadratic nonresidue****of n.*

Since the derivative of x^2 is 2x, and $2\mathrm{x} \equiv 0 \pmod 2$ we have to distinguish between the cases $\mathrm{p} = 2$ and p odd prime.

Theorem 2.1.*Let p be an odd prime, and $(a,p) = 1$. Then there is a solution of $x^2 = a(modp^e),\ e > 1$, if and only if there is a solution of $x^2 = a\ (modp)$.*

Theorem 2.2.*Let $n = p_1^{e^1} p_2^{e^2} \dots p_r^{e^r}$. Then the number a is a square $modn$ iff there are numbers $x_1, x_2, \dots, x_r$ such that*

$$x_1^2 \equiv a\ (modp_1^{e^1})$$

$$x_2^2 \equiv a\ (modp_2^{e^2})$$

$$\vdots$$

$$x_r^2 \equiv a\ (modp_r^{e^r})$$

Let $\mathrm{N}(n)$ denote the number of solutions of $x^2 - a = 0\ \ modn$. If $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ is the prime decomposition of n, then $\mathrm{N}(n) = \mathrm{N}(p_1^{n_1})\mathrm{N}(p_2^{n_2}) \dots \mathrm{N}(p_k^{n_k})$.

Theorem 2.3. *If p is an odd prime, $(a,p) = 1$ and a is a quadratic residue of p, then the congruence $x^2 \equiv a\ (mod p)$ has exactly two roots.*

Proof: See [3].

Corollary 2.1. *Let p be prime, the congruence*

$$x^2 \equiv 1\ (mod p)$$

has only the solutions $x = \pm 1\ (mod p)$.

Theorem 2.4. *Let p be an odd prime. Then there are exactly $(p-1)/2$ incongruent quadratic residues of p and exactly $(p-1)/2$ quadratic non-residues of p.*

Corollary 2.2. *The equation $x^2 \equiv a\ (mod p)$ has no solution if and only if $a^{\frac{(p-1)}{2}} \equiv -1\ (mod p)$.*

An element x of R is called ***nilpotent*** if there exists an integer $m \geq 0$ such that $x^m = 0$.

In graph theory, a ***complete*** graph is a simple undirected graph in which every pair of distinct vertices is connected by a unique edge. A ***regular*** graph is a graph where each vertex has the same number of neighbors; i.e. every vertex has the same degree ($\deg(v)$ is used to refer to the degree of a vertex v).

3. MAIN RESULTS

One notice that if n is an odd prime then according to **Theorem 2.3**, there are only two solutions of the quadratic polynomial (1), which means that $deg(v) = 1$ for all $v \in \mathbb{Z}_n$. Furthermore, the vertex $v = 0$ is omitted in this case, because $\mathbb{Z}_n$ is a field. Therefore, $\mathbb{Z}_n$ doesn't contain nilpotent elements that are adjacent to $v = 0$. If n is not a prime number, then $\deg(v) > 1$ in some components up to the deferent factorization of $x^2 - a = 0\ mod n$.

Since the degree of a vertex v depends on the number of roots of the quadratic polynomial (1), then we have the following.

Proposition 3.1. Let m be *the number of distinct roots of the quadratic polynomial (1), and v is a solution of this quadratic polynomial. Then, $deg(v) = m - 1$.*

Proof: Suppose that $x^2 - a = 0\ mod n$ is reducible quadratic polynomial, and v is one of its solutions, consequently $-v$ is also a root. As stated in Theorem 1.2, the polynomial (1) has $m > 1$ deferent factorization, which give us m deferent solutions. Thus, $deg(v) = m - 1$.■

The degree of a vertex v in G by definition is the number of arrows adjacent to this vertex. Since the solution of the polynomial (1) relies on the integer number n, then the degree of v can be determined as follows:

Theorem 3.1. *Let $p_1, p_2, \ldots, p_k$ be the prime component of the number n. Then the highest degree of a vertex v in the graph $G(\mathbb{Z}_n)$ equals to $2^k - 1$.*

Proof. Let $x^2 - a = 0 mod n$ be a reducible quadratic polynomial over $\mathbb{Z}_n$. From **Theorem 2.3** for each prime number p_i, we have

$$N(n) = 2 \times 2 \times \ldots \times 2 \ (k times) = 2^k.$$

Since v is considered as one of these solutions, thus $\deg(v) = 2^k - 1$. ■

In general, we can say that if $p_1^{n_1}, p_2^{n_2}, \ldots, p_r^{n_r}$ be the prime component of the number n. Then the highest degree of a vertex v in the graph $G(\mathbb{Z}_n)$ equals to $N(p_1^{n_1})N(p_2^{n_2})\ldots N(p_r^{n_r}) - 1$. For instance, in the graph shown in Figure 7the highest degree of a vertex v is $deg(v) = 6$.

Consider $n = p_1 p_2 \ldots p_k$, all solutions of quadratic polynomials $x^2 - a_i = 0 \ mod n$is a connected component in $G(\mathbb{Z}_n)$. When $k = 1$we have a 1-regular graph(every two vertices are connected separately with an edge). Therefore, from Theorem 2.4 we find that the number of components $c_n = \frac{p-1}{2}$.If$k > 1$, some quadratic polynomials $x^2 - a_i = 0 \ mod n$ will have more than two solutions. Thus, the number of components c_n will be less than $\frac{p-1}{2}$.

Consider $x^2 - b = 0 \ mod n$ is a quadratic polynomial with $\pm b_i$ solutions such that $1 < i < l$ for some positive integers $i$and l. The solutions $\pm b_i$ perform a simple completesubgraph (that is a componentin G)and this subgraph is a*k-regular* graph in G, where $k = deg\ (b_i)$ for some i.

4. GRAPHS FOR SOME INTEGERSn

In this section, we introduce the graphs $G(\mathbb{Z}_n)$ for some primes and composite integer $n = 7, 8, 15, 16, 24, 25, 36$.We observe that the highest degree of a vertex in $G(\mathbb{Z}_n)$ depends on deferent factorization of the integer n. For instance, inFigure 1,the shown graph $G(\mathbb{Z}_7)$ is 2-regular, while inFigure 2, Figure 3, and Figure 4 there are *3-regular* subgraphs. In Figure 7, we have two*5-regular*subgraphs and six 3-regular subgraphs. In Figure 5 there is a unique 7-regular subgraph and three 3-regular subgraphs. In Figure 6, the shown graph $G(\mathbb{Z}_{16})$ includes a unique subgraph with vertex degree greater than one.

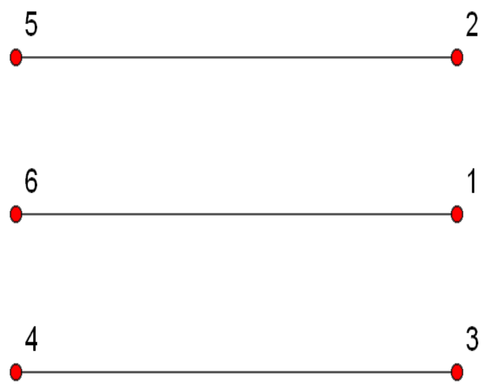

Figure 1: Shown is the graph $\mathbf{G}(\mathbb{Z}_7)$

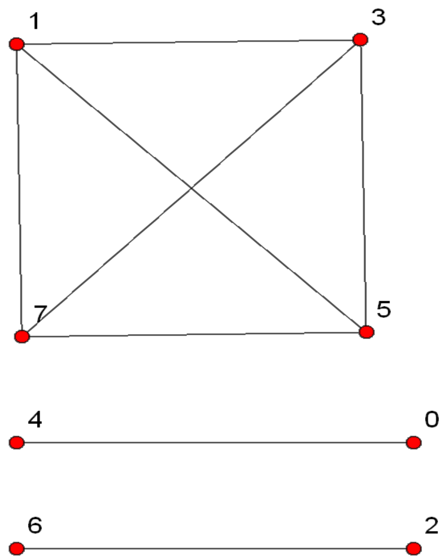

Figure 2: Shown is the graph $\mathbf{G}(\mathbb{Z}_8)$

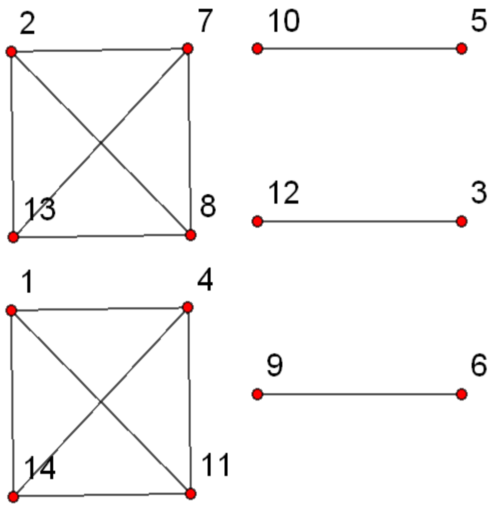

Figure 3: Shown is the graph $\mathbf{G}(\mathbb{Z}_{15})$

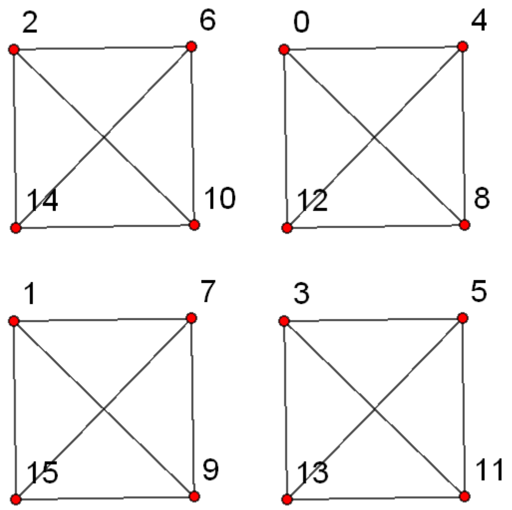

Figure 4: Shown is the graph $\mathbf{G}(\mathbb{Z}_{16})$

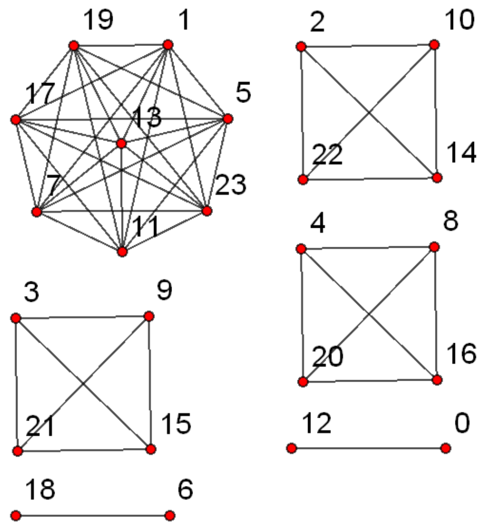

Figure 5: Shown is the graph $\mathbf{G}(\mathbb{Z}_{24})$

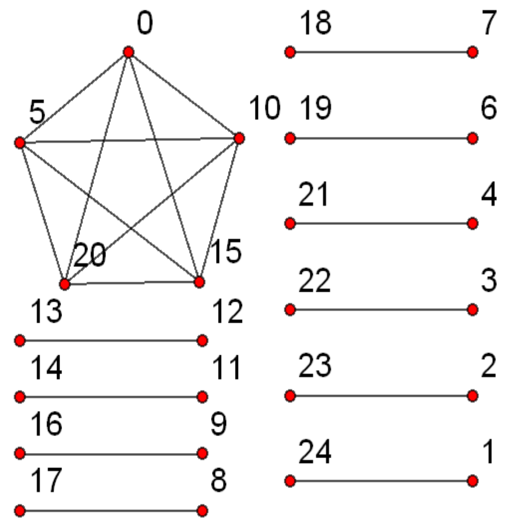

Figure 6: Shown is the graph $\mathbf{G}(\mathbb{Z}_{25})$

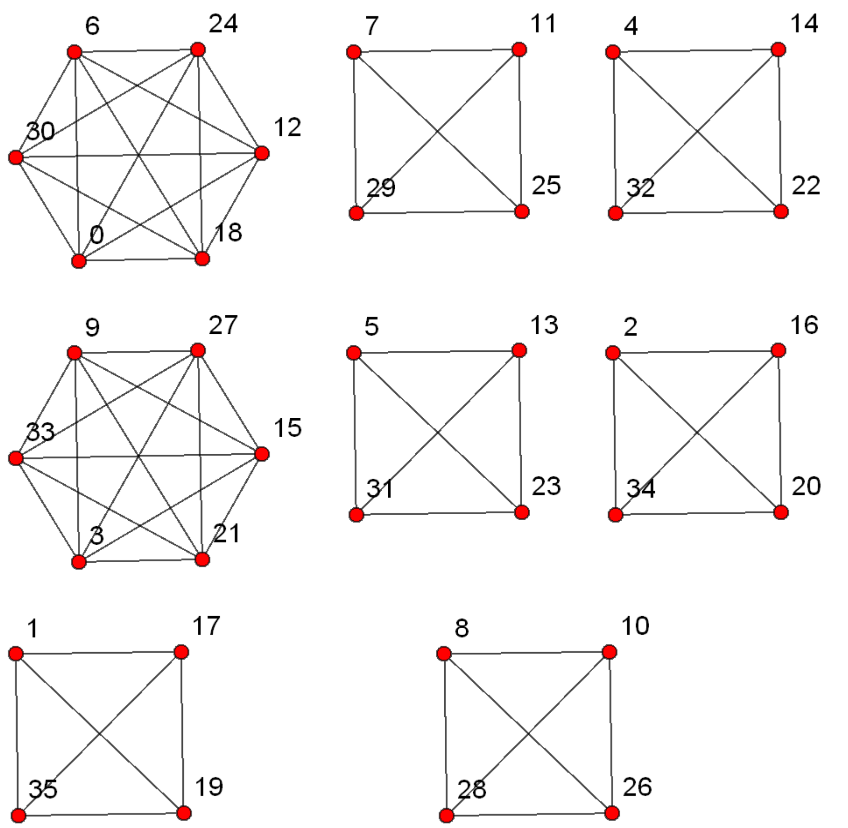

Figure 7: Shown is the graph $\mathbf{G}(\mathbb{Z}_{36})$

REFERENCES

[1] Childs, Lindsay N. (2009). A concrete introduction to higher algebra. New York: Springer.

[2] Kraft, James S., and Lawrence C. (2016). Washington. An introduction to number theory with cryptography. CRC Press.

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