Algebra and Discrete Mathematics
Volume **28** (2019). Number 1, pp. 44–59
© Journal "Algebra and Discrete Mathematics"
RESEARCH ARTICLE

Paley-type graphs of order a product of two distinct primes*

Angsuman Das

Communicated by D. Simson

Abstract. In this paper, we initiate the study of Paley-type graphs Γ_N modulo $N = pq$, where p, q are distinct primes of the form $4k + 1$. It is shown that Γ_N is an edge-regular, symmetric, Eulerian and Hamiltonian graph. Also, the vertex connectivity, edge connectivity, diameter and girth of Γ_N are studied and their relationship with the forms of p and q are discussed. Moreover, we specify the forms of primes for which Γ_N is triangulated or triangle-free and provide some bounds (exact values in some particular cases) for the order of the automorphism group $\mathrm{Aut}(\Gamma_N)$ of the graph Γ_N, the chromatic number, the independence number, and the domination number of Γ_N.

1. Introduction

The Paley graph, named after Raymond Paley, forms an infinite family of self-complementary, strongly regular graphs. Paley graph is a special type of Cayley graph with a finite field $\mathbb{F}_q, q = p^n$ where p is a Pythagorean prime i.e., primes of the form $4k+1$ as the additive group and the set of non-zero quadratic residues in $\mathbb{F}_q$ as the connection set. Since its inception, due to its connection with number theoretic properties of quadratic residues, a lot of research has been done on Paley graphs [3],[4], [12] and its generalized versions [1], [2], [7], [11], [16]. However, as far as our knowledge, Paley-type

*Preliminary version of this work appears in proceedings of ICMC 2015 [5].
2010 MSC: 05C30, 05C69.
Key words and phrases: Cayley graph, quadratic residue, Pythagorean prime.

graphs on modulus of the form pq, where p and q are distinct primes remained unexplored till date.

In this paper, we study Paley-type graphs Γ_N modulo $N = pq$, where p, q are distinct Pythagorean primes. The main goal of this paper is to study the properties of the proposed Paley-type graphs and their deviation from Paley graphs in terms of various graph parameters. It is shown that Γ_N is an edge-regular, Eulerian, Hamiltonian and arc-transitive graph. Also, the vertex connectivity, edge connectivity, diameter and girth of Γ_N are studied. Moreover, the conditions under which Γ_N is triangulated and triangle-free are discussed. We also provide some bounds (exact value in some particular cases) for the order of the automorphism group $\mathrm{Aut}(\Gamma_N)$ of Γ_N, the domination number, the chromatic number, and the independence number of Γ_N.

2. Preliminaries

In this section, for convenience of the reader and also for later use, we recall some definitions and notations concerning integers modulo N and quadratic residues in elementary number theory. For undefined terms and concepts in graph theory the reader is referred to [8] and [15]. Throughout this paper, graphs are undirected, simple and without loops.

An odd prime p is called a Pythagorean prime if $p \equiv 1 (\mathrm{mod}\ 4)$. Throughout this paper, even if it is not mentioned, a prime p always means a Pythagorean prime and $N = pq$ means the product of two distinct Pythagorean primes. By $\mathbb{Z}_N, \mathbb{Z}_N^*, \mathcal{QR}_N, \mathcal{QNR}_N, \mathcal{J}_N^{+1}, \mathcal{J}_N^{-1}$, we mean the set of all integers modulo N, the set of all units in integers modulo N, the set of all quadratic residues and non-quadratic residues which are also units in integers modulo N, the set of all units in integers modulo N with Jacobi symbol $+1$ and -1 respectively. For the sake of convenience, $a \equiv b (\mathrm{mod}\ N)$ is sometimes written as $a = b$, in places where the modulus is clear from the context. We can conclude the following lemma from the results which can be found in any elementary number theory book e.g., [14].

Lemma 1. *If $N = pq$, then the following are true:*

- *$\mathcal{J}_N^{+1}$ is a subgroup of $\mathbb{Z}_N^*$ and $\mathcal{QR}_N$ is a subgroup of $\mathcal{J}_N^{+1}$.*
- *$|\mathbb{Z}_N^*| = \phi(N) = (p-1)(q-1), |\mathcal{J}_N^{+1}| = |\mathcal{J}_N^{-1}| = \frac{(p-1)(q-1)}{2}$ and $|\mathcal{QR}_N| = \dfrac{(p-1)(q-1)}{4}$, where ϕ denotes the Euler's Phi function.*
- *$x \in \mathcal{QR}_N \iff x \in \mathcal{QR}_p \cap \mathcal{QR}_q$.*

- $x \in \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N \iff x \in \mathcal{QNR}_p \cap \mathcal{QNR}_q$.
- $x \in \mathcal{J}_N^{-1} \iff x \in \mathcal{QNR}_p \cap \mathcal{QR}_q$ *or* $x \in \mathcal{QR}_p \cap \mathcal{QNR}_q$. □

Lemma 2. *If p, q are two distinct primes of the form $p \equiv q \equiv 1(mod\ 4)$, then -1 is a quadratic residue in $\mathbb{Z}_N$.*

Proof. To show that -1 is a quadratic residue in $\mathbb{Z}_N$, we need to show that $x^2 \equiv -1(\text{mod } N)$ has a solution. But,

$$x^2 \equiv -1(\text{mod } N) \Leftrightarrow x^2 \equiv -1(\text{mod } p) \text{ and } x^2 \equiv -1(\text{mod } q)$$

Now, as p and q are Pythagorean primes, -1 is a square in both $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Thus, $x^2 \equiv -1(\text{mod } N)$ have a solution in $\mathbb{Z}_N$. □

3. Paley-type graph modulo *N*

We now define the Paley-type graphs Γ_N modulo $N = pq$ and study some of their basic properties.

Definition 1 (Paley-type Graph modulo N)**.** For $N = pq$, Paley-type Graph modulo N, Γ_N is given by $\Gamma_N = (V, E)$, where $V = \mathbb{Z}_N$ and $(a, b) \in E \Leftrightarrow a - b \in \mathcal{QR}_N$.

Remark 1. Γ_N is a Cayley Graph (G, S) where $G = (\mathbb{Z}_N, +)$ and $S = \mathcal{QR}_N$. Observe that as $-1 \in \mathcal{QR}_N$ and $\mathcal{QR}_N$ is a group with respect to modular multiplication, $\mathcal{QR}_N$ is also closed with respect to additive inverse, i.e., $S = -S$ and $0 \notin S$.

Theorem 1. *Γ_N is Hamiltonian and hence connected.*

Proof. Since, $1 \in \mathcal{QR}_N$, the vertex set $\{0, 1, 2, \ldots, N-1\}$, taken in order, can be thought of as a Hamiltonian path. Hence, the theorem is proved. □

Theorem 2. *Γ_N is regular with valency $\phi(N)/4$ and hence Eulerian.*

Proof. Let $x \in \mathbb{Z}_N$. By $N(x)$, we mean the set of vertices in Γ_N which are adjacent to x, i.e., $N(x) = \{z \in \mathbb{Z}_N : x - z \in \mathcal{QR}_N\}$. If possible, let $\exists z_1, z_2 \in N(x)$ with $z_1 \neq z_2$ such that $x - z_1 = x - z_2$. But, $x - z_1 = x - z_2 = s$ (say) $\in \mathcal{QR}_N \Rightarrow z_1 = x - s = z_2$, a contradiction. Thus, $\forall s \in \mathcal{QR}_N, \exists$ a unique $z \in \mathbb{Z}_N$ such that $x - z = s$. Thus, degree or valency of $x = |N(x)| = |\mathcal{QR}_N| = \phi(N)/4$. Now, let $p = 4k+1, q = 4l+1$. Since, degree of each vertex $= \frac{\phi(N)}{4} = \frac{(p-1)(q-1)}{4} = \frac{4k \cdot 4l}{4} = 4kl$ is even, Γ_N is Eulerian. □

Note. The graph Γ_N is not strongly regular (See Remark 3).

Remark 2. Γ_N is not self-complementary: A necessary condition for a self - complementary graph G with n vertices is that number of edges in G equals $\frac{n(n-1)}{4}$. But, the number of edges in Γ_N with N vertices is $\frac{N\cdot\phi(N)}{8} < \frac{N(N-1)}{4}$. However, the next theorem shows that Γ_N has a homomorphic image of itself as a sub-graph of its complement graph.

Theorem 3. *Γ_N has a homomorphic image of itself as a sub-graph of its complement graph Γ_N^c.*

Proof. Let $n \in \mathbb{Z}_N^* \setminus \mathcal{QR}_N$. We define a function $\psi : \Gamma_N \to \Gamma_N^c$ given by $\psi(x) = nx$. For injectivity, $\psi(x_1) = \psi(x_2) \Rightarrow nx_1 = nx_2 \Rightarrow x_1 = x_2$, as n is a unit in $\mathbb{Z}_N$. For homomorphism, x, y adjacent in $\Gamma_N \Rightarrow x - y \in \mathcal{QR}_N \Rightarrow n(x-y) \notin \mathcal{QR}_N \Rightarrow nx$ and ny are not adjacent in Γ_N, i.e, $\psi(x)$ and $\psi(y)$ are adjacent in Γ_N^c. □

Theorem 4. *Γ_N is isomorphic to the direct product of Γ_p and Γ_q, the Paley graphs of prime order p and q respectively, i.e., $\Gamma_N \cong \Gamma_p \times \Gamma_q$.*

Proof. Consider the map $\Phi : \Gamma_N \to \Gamma_p \times \Gamma_q$ given by $\Phi(x) = (x \bmod p, x \bmod p)$. Clearly, this is a bijection. The fact that Φ preserves adjacency and non-adjacency follows from the result that $\mathcal{QR}_N$ is isomorphic to $\mathcal{QR}_p \times \mathcal{QR}_q$. □

4. Symmetricity of Γ_N

In this section, we study the action of the automorphism group $\mathrm{Aut}(\Gamma_N)$ on Γ_N and its consequences.

Theorem 5. *Γ_N is vertex-transitive.*

Proof. As Γ_N is a Cayley graph, it is vertex transitive. (by Theorem 3.1.2 in [8]) However, we show the existence of such automorphisms explicitly, which will be helpful later.

Choose $a \in \mathcal{QR}_N$ and $b \in \mathbb{Z}_N$ and define a function $\varphi : \mathbb{Z}_N \to \mathbb{Z}_N$ given by $\varphi(x) = ax+b, \forall x \in \mathbb{Z}_N$. We show that φ is an automorphism. φ is injective, for $\varphi(x_1) = \varphi(x_2) \Rightarrow ax_1+b = ax_2+b \Rightarrow a(x_1-x_2) = 0 \Rightarrow x_1 = x_2$ as $a \in \mathbb{Z}_N^*$ For surjectivity, $\forall y \in \mathbb{Z}_N, \exists x = a^{-1}y - a^{-1}b \in \mathbb{Z}_N$ such that $\varphi(x) = a(a^{-1}y - a^{-1}b) + b = y$. Moreover, φ is a graph homomorphism, as x and y are adjacent in $\Gamma_N \Leftrightarrow x - y \in \mathcal{QR}_N \Leftrightarrow a(x-y) + b - b \in \mathcal{QR}_N \Leftrightarrow (ax+b) - (ay+b) \in \mathcal{QR}_N \Leftrightarrow \varphi(x) - \varphi(y) \in \mathcal{QR}_N \Leftrightarrow \varphi(x)$ and $\varphi(y)$ are adjacent in Γ_N. Thus, $\varphi \in \mathrm{Aut}(\Gamma_N)$.

Now, let $u, v \in \mathbb{Z}_N$ be two vertices of Γ_N. We take $a = 1 \in \mathcal{QR}_N$ and $b = v - u \in \mathbb{Z}_N$. Then the map $\varphi : \mathbb{Z}_N \to \mathbb{Z}_N$ given by $\varphi(x) = ax + b$ is an automorphism on Γ_N such that $\varphi(u) = v$. Thus, $\mathrm{Aut}(\Gamma_N)$ acts transitively on $\mathbb{Z}_N$ i.e., $V(\Gamma_N)$. □

Theorem 6. Γ_N *is arc-transitive and hence edge transitive.*

Proof. Let $\{u_1, v_1\}, \{u_2, v_2\}$ be two edges (considered as having a direction) in Γ_N. Therefore, $u_1 - v_1, u_2 - v_2 \in \mathcal{QR}_N$. We take $a = (u_2 - v_2)(u_1 - v_1)^{-1} \in \mathcal{QR}_N$ and $b = u_2 - au_1 \in \mathbb{Z}_N$ and construct the automorphism $\varphi(x) = ax + b$ as in Theorem 5. Since $\varphi(u_1) = u_2$ and $\varphi(v_1) = v_2$, Γ_N is arc transitive, and hence edge transitive. □

Corollary 1. $|\mathrm{Aut}(\Gamma_N)| \geqslant \frac{N\phi(N)}{4}$.

Proof. In Theorem 5, it was shown that $\varphi : \mathbb{Z}_N \to \mathbb{Z}_N$ given by $\varphi(x) = ax + b, \forall x \in \mathbb{Z}_N$ is an automorphism for $a \in_R \mathcal{QR}_N$ and $b \in_R \mathbb{Z}_N$. Thus, $|\mathrm{Aut}(\Gamma_N)| \geqslant \frac{N\phi(N)}{4}$. □

Corollary 2. *Edge connectivity of* Γ_N *is* $\phi(N)/4$.

Proof. Since Γ_N is connected and vertex-transitive, by Lemma 3.3.3 in [8], its edge connectivity is equal to its valency. □

Lemma 3. *[8] The vertex connectivity of a connected edge transitive graph is equal to its minimum valency.* □

Corollary 3. *Vertex connectivity of* Γ_N *is* $\phi(N)/4$.

Proof. Since, Γ_N is a connected edge-transitive graph with valency $\frac{\phi(N)}{4}$, by Lemma 3, Γ_N has vertex connectivity $\phi(N)/4$. □

5. Diameter, girth and triangles of Γ_N

In this section, we find out the diameter and girth of Γ_N. It is noted that Γ_N has dual nature when it comes to diameter and girth. To be more specific, it depends on whether 5 is a factor of N or not. If 5 is one of the two factors of N, we call it Γ_N of Type-I and else call it Γ_N of Type-II. First, we prove two lemmas which will be used later.

Lemma 4. *Let p be a prime of the form $4k + 1$ and $c \in \mathbb{Z}_p$. Then, the number of ways in which c can be expressed as difference of two quadratic residues in $\mathbb{Z}_p^*$ are*

(1) $\frac{p-1}{2}$ *if* $c \equiv 0(mod\ p)$*;*
(2) $\frac{p-5}{4}$ *if* $c \in \mathcal{QR}_p$*;*
(3) $\frac{p-1}{4}$ *if* $c \in \mathcal{QNR}_p$*.*

Proof. (1) If $c \equiv 0(\text{mod } p)$, then for all $r \in \mathcal{QR}_p$, c can be expressed as $r - r$. Thus, the number in this case, is equal to number of elements in $\mathcal{QR}_p$, i.e., $\frac{p-1}{2}$.

(2) For this case, assume that $c \not\equiv 0(\text{mod } p)$, i.e., $c \in \mathbb{Z}_p^*$. Let $c = a^2 - b^2 = (a+b)(a-b)$, where $a, b \in \mathbb{Z}_p^*$. Now, for all $p-1$ values of $d \in \mathbb{Z}_p^*$, letting $a + b = d; a - b = \frac{c}{d}$, we get all possible solutions of the equation $c = a^2 - b^2$. From this, we get $a = \frac{1}{2}\left(d + \frac{c}{d}\right)$ and $b = \frac{1}{2}\left(d - \frac{c}{d}\right)$. However, we need to ensure that $a, b \in \mathbb{Z}_p^*$, i.e., $d \pm \frac{c}{d} \not\equiv 0(\text{mod } p)$, i.e, $d^2 \not\equiv \pm c(\text{mod } p)$.

Now, if $c \in \mathcal{QR}_p$, then $-c \in \mathcal{QR}_p$. (as -1 is a quadratic residue in $\mathbb{Z}_p^*$). In this case, there exist two square roots of c and two other square roots of $-c$. Thus, we loose 4 possible values of d. Thus, the number of solutions is reduced to $p-5$. Moreover, it is observed that the 4 solutions of $(a+b, a-b)$, namely $(d, \frac{c}{d}), (-d, \frac{c}{-d}), (\frac{c}{d}, d), (\frac{c}{-d}, -d)$ lead to the same solution

$$a^2 = \frac{1}{4}\left(d + \frac{c}{d}\right)^2; b^2 = \frac{1}{4}\left(d - \frac{c}{d}\right)^2$$

(As p is odd, $d \neq -d$). Thus, the number of distinct solutions is reduced to $\frac{p-5}{4}$.

(3) The proof for $c \in \mathcal{QNR}_p$ follows exactly using same arguments except the fact that in this case, we do not loose those four solutions as $c \not\equiv \pm d^2$. Thus, the number of ways c can be expressed as difference of quadratic residues is $\frac{p-1}{4}$. □

Lemma 5. *Let $N = pq$, where p, q are Pythagorean primes. Then*

1) *If $c \in \mathcal{QR}_N$, then the number of ways in which c can be expressed as difference of two quadratic residues, i.e., $c = x^2 - y^2, x, y \in \mathbb{Z}_N^*$ is $\frac{(p-5)(q-5)}{16}$.*
2) *If $c \in \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$, then the number of ways in which c can be expressed as difference of two quadratic residues is $\frac{(p-1)(q-1)}{16}$.*
3) *If $c \in \mathcal{J}_N^{-1}$, then the number of ways in which c can be expressed as difference of two quadratic residues is either $\frac{(p-1)(q-5)}{16}$ [if $c \in \mathcal{QR}_q$, but $c \notin \mathcal{QR}_p$] or $\frac{(p-5)(q-1)}{16}$ [if $c \in \mathcal{QR}_p$, but $c \notin \mathcal{QR}_q$].*
4) *If $c(\neq 0) \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$ i.e., c is a non-zero, non-unit in $\mathbb{Z}_N$, then*

(a) *If* $c \equiv 0(mod\ q)$ *and* $c \in \mathcal{QR}_p$*, then the number of ways in which* c *can be expressed as difference of two quadratic residues is* $\frac{(p-5)(q-1)}{8}$.

(b) *If* $c \equiv 0(mod\ q)$ *and* $c \in \mathcal{QNR}_p$*, then the number of ways in which* c *can be expressed as difference of two quadratic residues is* $\frac{(p-1)(q-1)}{8}$.

(c) *If* $c \equiv 0(mod\ p)$ *and* $c \in \mathcal{QR}_q$*, then the number of ways in which* c *can be expressed as difference of two quadratic residues is* $\frac{(q-5)(p-1)}{8}$.

(d) *If* $c \equiv 0(mod\ p)$ *and* $c \in \mathcal{QNR}_q$*, then the number of ways in which* c *can be expressed as difference of two quadratic residues is* $\frac{(q-1)(p-1)}{8}$.

Proof. 1) If $c \in \mathcal{QR}_N$, then $c \in \mathcal{QR}_p$ and $c \in \mathcal{QR}_q$. Thus, the result follows from Chinese Remainder Theorem and second part of Lemma 4.

2) If $c \in \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$, then $c \in \mathcal{QNR}_p$ and $c \in \mathcal{QNR}_q$. Thus, the result from Chinese Remainder Theorem and third part of Lemma 4.

3) If $c \in \mathcal{J}_N^{-1}$, then either of two cases may arise, namely $c \in \mathcal{QR}_q;\ c \in \mathcal{QNR}_p$ or $c \in \mathcal{QR}_p;\ c \in \mathcal{QNR}_q$.

If $c \in \mathcal{QR}_q;\ c \in \mathcal{QNR}_p$, then by applying second part of Lemma 4 for q and third part of Lemma 4 and Chinese Remainder Theorem, we get the count as $\frac{(p-1)(q-5)}{16}$. Similarly, the case $c \in \mathcal{QR}_p;\ c \in \mathcal{QNR}_q$ follows.

4) As $c \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$, either $p \mid c$ or $q \mid c$ [not both, as that would imply $c \equiv 0(\text{mod } N)$].

If $q \mid c$ and $p \nmid c$, two cases arises, namely (a) $c \equiv 0(\text{mod } q)$ and $c \in \mathcal{QR}_p$, and (b) $c \equiv 0(\text{mod } q)$ and $c \in \mathcal{QNR}_p$. In both the cases, the lemma follows from Chinese remainder Theorem and Lemma 4.

Similarly, if $q \nmid c$ and $p \mid c$, two cases arises, namely (c) $c \equiv 0(\text{mod } p)$ and $c \in \mathcal{QR}_q$ and (d) $c \equiv 0(\text{mod } p)$ and $c \in \mathcal{QNR}_q$. Again, these cases follows similarly. □

5.1. Γ_N of Type-I

Lemma 6. *If* $N = 5q$*, then* $x, y \in \mathcal{QR}_N \Rightarrow x - y \notin \mathcal{QR}_N$.

Proof. Since $x, y \in \mathcal{QR}_N, \exists a, b \in \mathbb{Z}_N^*$ such that $x \equiv a^2(\text{mod } N)$ and $y \equiv b^2(\text{mod } N)$. If possible, let $x - y \in \mathcal{QR}_N$. Then, $\exists c \in \mathbb{Z}_N^*$ such that $x - y \equiv c^2(\text{mod } N)$. Therefore, $a^2 - b^2 \equiv c^2(\text{mod } N) \Rightarrow a^2 \equiv b^2 + c^2(\text{mod } N) \Rightarrow a^2 \equiv b^2 + c^2(\text{mod } 5)$. Now, as $a, b, c \in \mathbb{Z}_N^*, a, b, c$ are relatively prime to 5. But $a^2 \equiv b^2 + c^2(\text{mod } 5)$ has no solution in $\mathbb{Z}_5^*$, which is a contradiction. □

Theorem 7. *If $N = 5q$, then Γ_N is triangle-free.*

Proof. If possible, let $x, y, z \in \mathbb{Z}_N$ be vertices of a triangle in Γ_N. Then, $x - y, z - y, x - z \in \mathcal{QR}_N$. However, $x - z \equiv (x - y) - (z - y)(\text{mod } N)$, a contradiction to Lemma 6. Thus, Γ_N is triangle-free. □

Corollary 4. *Γ_N of Type-I is an edge-regular graph with parameters $v = 5q, k = q - 1, \lambda = 0$.* □

Lemma 7. *[8] If G is an abelian group and S is an inverse-closed subset of $G \setminus \{e\}$ with $|S| \geqslant 3$, then the Cayley graph (G, S) has girth at most 4.* □

Corollary 5. *If $N = 5q$, then $girth(\Gamma_N) = 4$.*

Proof. Since, Γ_N is triangle-free, $girth(\Gamma_N) \geqslant 4$. However, as Γ_N is a Cayley graph with $G = \mathbb{Z}_N$ and generating set $S = \mathcal{QR}_N$ such that $|S| = q - 1 \geqslant 3$, by Lemma 7, $girth(\Gamma_N)$ is at most 4. Thus, $girth(\Gamma_N) = 4$. □

Now, with the help of the following two lemmas, we prove that if $N = 5q$, where q is a Pythagorean prime, then $diam(\Gamma_N) = 3$.

Lemma 8. *If $N = 5q$, where q is a Pythagorean prime, then the number of vertices at distance 2 from the vertex $0 \in \Gamma_N$ is $3q - 1$.*

Proof. Let x be a vertex at distance 2 from 0. Clearly, $x \neq 0$. Since, $d(0, x) \neq 1$, it follows that $x \notin \mathcal{QR}_N$. Also, as $d(0, x) = 2$, $\exists u \in \Gamma_N$ such that $0, u$ are adjacent and u, x are adjacent i.e., $u, u - x \in \mathcal{QR}_N$, i.e., $x = u - (u - x)$ can be expressed as difference of two quadratic residues modulo N. Thus, number of vertices x at distance 2 from the vertex 0 is equal to the number of $x \notin \mathcal{QR}_N$ which can be expressed as difference of two quadratic residues. Now, we finish the proof by appeal to Cases 2,3 and 4 of Lemma 5 with $p = 5$.

Case 2: The number of such $x \in \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$, i.e., $|\mathcal{J}_N^{+1} \setminus \mathcal{QR}_N|$ is $\frac{(p-1)(q-1)}{4} = q - 1$.

Case 3: In $\mathcal{J}_N^{-1}$, only those x's, for which $x \in \mathcal{QR}_q$ but $x \notin \mathcal{QR}_5$, can be expressed as difference of two quadratic residues. Note that the other type of x's can not be expressed as difference of quadratic residues as $p = 5$. Thus, the number of $x \in \mathcal{J}_N^{-1}$ which can be expressed as difference of two quadratic residues is $|\{x \in \mathcal{J}_N^{-1} : x \in \mathcal{QR}_q \ \& \ x \notin \mathcal{QR}_5\}| = \left(\frac{q-1}{2}\right) 2 = q - 1$.

Case 4: If x is a non-zero, non-unit element in $\mathbb{Z}_N$, out of the four cases in Lemma 5, the last three cases are applicable. Note that in the first case x can not be expressed as difference of quadratic residues as $p = 5$. Thus, the number of x which can be expressed as difference of two squares in this category is

$$\begin{aligned}
&|\{x : x \equiv 0 (\text{mod } q) \ \& \ x \in \mathcal{QNR}_5\}| \ + \ |\{x : x \equiv 0 (\text{mod } 5) \ \& \ x \in \mathcal{QR}_q\}| \\
&\qquad + |\{x : x \equiv 0 (\text{mod } 5) \ \& \ x \in \mathcal{QNR}_q\}| \\
&\qquad = \frac{5-1}{2} + \frac{q-1}{2} + \frac{q-1}{2} = q + 1
\end{aligned}$$

Combining all these cases, we get the total number of vertices at a distance 2 from the vertex 0 as $(q-1) + (q-1) + (q+1) = 3q - 1$. □

Lemma 9. *If $N = 5q$, where q is a Pythagorean prime, then the number of vertices at distance 3 from the vertex $0 \in \Gamma_N$ is $q + 1$.*

Proof. From the proof of Lemma 8, it is evident that x's which are not at a distance 1 or 2 from the vertex 0 fall under either of the two categories: (i) $x \in \mathcal{J}_N^{-1}$, with $x \in \mathcal{QR}_5$, but $x \notin \mathcal{QR}_q$ or (ii) x is a non-zero, non-unit in $\mathbb{Z}_N$ such that $x \equiv 0 (\text{mod } q)$ and $x \in \mathcal{QR}_5$. Observe that in both the cases, $x \in \mathcal{QR}_5$.

We now construct a path of length 3 from 0 to x. Consider the vertex 1 and x. Now, $x - 1 \notin \mathcal{QR}_5$, otherwise, we get two consecutive integers $x, x-1 \in \mathcal{QR}_5$, which is a contradiction. Thus, by Lemma 5, $d(x, 1) = d(x-1, 0) = 2$ or 1. Also, $d(1, x) \neq 1$ as that would give a path $0, 1, x$ of length 2 from 0 to x, a contradiction. Hence, $d(1, x) = 2$. Let the shortest path from 1 to x be $1, u, x$. Then, $0, 1, u, x$ is a path from 0 to x and hence, $d(0, x) \leqslant 3$. On the other hand, $d(0, x) \neq 1, 2$. Thus, $d(0, x) = 3$.

Now, the number of such x's at a distance 3 from 0 is

$$\begin{aligned}
&|\{x \in \mathcal{J}_N^{-1} : x \in \mathcal{QR}_5; x \notin \mathcal{QR}_q\}| \\
&\qquad + |\{x \in \mathbb{Z}_N : x \equiv 0 (\text{mod } q); x \in \mathcal{QR}_5\}| \\
&\qquad = 2\left(\frac{q-1}{2}\right) + \frac{5-1}{2} = (q-1) + 2 = q + 1.
\end{aligned}$$
□

Theorem 8. *If $N = 5q$, with q a Pythagorean prime, then $diam(\Gamma_N) = 3$.*

Proof. Since, Γ_N is regular with degree $\phi(N)/4 = q-1$, number of vertices adjacent to 0, i.e., at distance 1 from 0 is $q - 1$. By Lemma 8, Lemma 9 and counting the point 0 itself, we get the number of all points at distance $0, 1, 2, 3$ from the vertex 0 as $1 + (q-1) + (3q-1) + (q+1) = 5q = N$. Thus, it exhausts all the vertices in Γ_N, i.e., all the points, apart from 0 itself, are at either distance 1, 2 or 3 from 0. Since, Γ_N is symmetric, the maximum distance between any two vertex is 3, i.e., $diam(\Gamma_N) = 3$. □

5.2. Γ_N of Type-II

Theorem 9. *If $N = pq$ where $5 \nmid N$, then Γ_N is triangulated and girth*$(\Gamma_N) = 3$.

Proof. Let $x \in \mathbb{Z}_N$ be any vertex in Γ_N. Consider $x, x+3^2, x+5^2 \in \mathbb{Z}_N$. These three vertices form a triangle as $9, 16, 25$ are relatively prime to N and belongs to $\mathcal{QR}_N$. Thus, every vertex $x \in \Gamma_N$ is a vertex of a triangle in Γ_N. Hence, Γ_N is triangulated. Now, existence of triangle in Γ_N ensures its girth to be 3. □

Lemma 10. *Let $N = pq$ where $5 \nmid N$. If $0, x \in \mathbb{Z}_N$ be non-adjacent vertices in Γ_N, then $\exists u \in \mathbb{Z}_N$ such that 0 and u are adjacent and u and x are adjacent.*

Proof. Since, $0, x \in \mathbb{Z}_N$ be non-adjacent vertices in Γ_N, x is not a quadratic residue in $\mathbb{Z}_N$. Also, $N = pq$ with $5 \nmid N$ implies $p, q > 5$. Therefore, by Lemma 5, x can always be expressed as difference of two quadratic residues, say $u, v \in \mathcal{QR}_N$ such that $x = u - v$. Since, $u \in \mathcal{QR}_N$, 0 and u are adjacent in Γ_N. Also, $u - x = v$ is a quadratic residue, i.e., u and x are adjacent in Γ_N. □

Theorem 10. *If $N = pq$ where $5 \nmid N$, then diam*$(\Gamma_N) = 2$.

Proof. Let $x, y \in \mathbb{Z}_N$. If $x - y \in \mathcal{QR}_N$, then $d(x, y) = 1$. If $x - y$ is not a quadratic residue, then 0 and $x - y$ are non-adjacent vertices in Γ_N. Therefore, by Lemma 10, $\exists u \in \mathbb{Z}_N$ such that 0 is adjacent to u and u is adjacent to $x - y$. So using a translation of y, we get y is adjacent to $u + y$ and $u + y$ is adjacent to x in Γ_N. Thus, $d(x, y) = 2$ and hence *diam*$(\Gamma_N) = 2$. □

Theorem 11. *Let $N = pq$, where $p, q > 5$ are primes with $p = 4k+1, q = 4l+1$. If x, y are two adjacent vertices in Γ_N, then there are exactly $(k-1)(l-1)$ vertices in Γ_N which are adjacent to both x and y.*

Proof. Since x, y are two adjacent vertices in Γ_N, $x - y \in \mathcal{QR}_N$. By Lemma 5, the number of ways in which $x - y$ can be expressed as difference of two quadratic residues is $\frac{(p-5)(q-5)}{16} = \frac{(4k-4)(4l-4)}{16} = (k-1)(l-1)$. Let $x - y = u - v$ where $u, v \in \mathcal{QR}_N$. Therefore, $0, u$ are adjacent (as $u \in \mathcal{QR}_N$) and $u, x - y$ are adjacent (as $u - (x - y) = v \in \mathcal{QR}_N$) in Γ_N. Thus, by using a translation by y and symmetricity of Γ_N, $y, u + y$ are adjacent and $u + y, x$ are adjacent. Hence, there are exactly $(k-1)(l-1)$ vertices in Γ_N which are adjacent to both x and y. □

Corollary 6. *Γ_N of Type-II is edge-regular with parameters $v = pq, k = \frac{(p-1)(q-1)}{4}$, $\lambda = \frac{(p-5)(q-5)}{16}$.* □

Remark 3. By Theorem 2 and Theorem 11, it follows that Γ_N of Type-II is regular and any two neighbours in Γ_N have equal number of common neighbours. However, any two non-adjacent vertices may not have equal number of common neighbours. Thus, Γ_N is not strongly regular.

In Theorem 9, it was shown that Γ_N of Type-II is triangulated. Now, by using Theorem 11, we count the number of triangles in Γ_N of Type-II.

Theorem 12. *If $N = pq$ with $p = 4k+1, q = 4l+1$ being primes > 5, then number of triangles in Γ_N is $\frac{2}{3}Nk(k-1)l(l-1)$.*

Proof. Let x be a vertex in Γ_N. The number of vertices adjacent to x is $\phi(N)/4$. Let y be one of those vertices adjacent to x. Now, by Theorem 11, there are $(k-1)(l-1)$ vertices z_i's in Γ_N which are adjacent to both x and y, thereby forming a triangle. Thus, the count of triangles with x as a vertex, comes to $\frac{\phi(N)}{4}(k-1)(l-1)$. However, this number is twice the actual number of triangles with x as a vertex, since we could have also started with choosing z_i instead of y and get y as the common neighbour of x and z_i. Thus, the actual number of triangles with x as a vertex is $\frac{\phi(N)}{8}(k-1)(l-1)$. Now, varying x over the vertex set of Γ_N, the count becomes $\frac{\phi(N)}{8}N(k-1)(l-1)$. Again, this count is to be divided by 3, as if x, y, z are vertex of a triangle, then the triangle is counted thrice once with respect to each vertex. Thus, the actual number of triangles in Γ_N is

$$\begin{aligned}\frac{\phi(N)}{24}N(k-1)(l-1) &= \frac{(p-1)(q-1)}{24}N(k-1)(l-1)\\ &= \frac{4k\cdot 4l}{24}N(k-1)(l-1) = \frac{2}{3}Nk(k-1)l(l-1).\end{aligned}$$ □

Remark 4. Note that one of $k-1, k, k+1$ is divisible by 3. But as $p = 4k+1 = 3k+(k+1)$, $k+1$ is not divisible by 3, thus $k(k-1)$ is divisible by 3. As a result, the number of triangles is a positive integer.

6. Independence number of Γ_N

In this section, we find the independence number of Γ_N of Type-I and provide both lower and upper bounds for that of Γ_N of Type-II. We first state a result which will be crucial in deducing these bounds.

Proposition 1. *[17] If G and H are vertex-transitive graphs, then independence number of their direct product $G \times H$ is given by $\alpha(G \times H) = \max\{\alpha(G) \cdot |H|, \alpha(H) \cdot |G|\}$.*

Theorem 13. *If $N = pq$ with $p < q$, then $2q \leqslant \alpha(\Gamma_N) \leqslant q[\sqrt{p}]$.*

Proof. Since, Paley graphs are self complementary, clique number of Γ_p= independence number of Γ_p, i.e., $\omega(\Gamma_p) = \alpha(\Gamma_p)$. Also, it is known that clique number of a prime-order Paley graph $\omega(\Gamma_p) < \sqrt{p}$ (See [4]). Now, as $p < q$ and p, q are primes of the form 1 mod 4, $\exists k \in \mathbb{N}$ such that $q = 4k + p$. Thus,

$$p^2 q = p^2(p + 4k) = p^3 + 4p^2 k < p^3 + 8p^2 k + 16pk^2 = p(p + 4k)^2 = pq^2$$

i.e., $p\sqrt{q} < q\sqrt{p}$. Since $\Gamma_N \cong \Gamma_p \times \Gamma_q$ and Paley graphs are vertex-transitive, by Proposition 1 we get $\alpha(\Gamma_N) = \max\{q \cdot \alpha(\Gamma_p), p \cdot \alpha(\Gamma_q)\} < \max\{p\sqrt{q}, q\sqrt{p}\} = q\sqrt{p}$. In fact, as $\omega(\Gamma_p)$ is a positive integer, $\alpha(\Gamma_N) \leqslant q[\sqrt{p}]$.

For the lower bound, choose $a \in \mathcal{QNR}_p$ and consider the following subset of $\mathbb{Z}_N$,

$$I = \{pk : 0 \leqslant k \leqslant q - 1\} \cup \{pl + a : 0 \leqslant l \leqslant q - 1\}$$

Claim: I is an independent subset of Γ_N of size $2q$.
Proof of the claim: As the difference of two elements of the form pk is a multiple of p, the difference does not belong to $\mathcal{QR}_p$ and as a result does not belong to $\mathcal{QR}_N$. Thus, two vertices of the form pk are non-adjacent in Γ_N. Similarly, two vertices of the form $pl + a$ are non-adjacent in Γ_N. Finally, as $(pl + a) - pk \equiv a \bmod p$, $(pl + a) - pk$ does not belong to $\mathcal{QR}_p$ and hence does not belong to $\mathcal{QR}_N$. Thus, a vertex of the form pk is not adjacent to a vertex of the form $pl + a$. Therefore the claim is true and it proves the required lower bound of $\alpha(\Gamma_N)$. □

In the next corollary, we show that the lower bound is tight.

Corollary 7. *For Γ_N of Type-I, $\alpha(\Gamma_N) = 2q$.*

Proof. As Γ_5 is a cycle of length 5, $\alpha(\Gamma_5) = 2$. Also for Paley graph Γ_q, $\alpha(\Gamma_q) < \sqrt{q}$. Thus,

$$\alpha(\Gamma_N) = \max\{q \cdot \alpha(\Gamma_5), 5 \cdot \alpha(\Gamma_q)\} \leqslant \max\{2q, 5\sqrt{q}\} = 2q.$$

The last equality follows as $2q > 5\sqrt{q}$ for all $q > \frac{25}{4}$ and the least value of q in Γ_N of Type-I is 13. Hence, $\alpha(\Gamma_N) \leqslant 2q$. Now, as demonstrated in Theorem 13, I is an independent set of size $2q$. Thus, $\alpha(\Gamma_N) = 2q$.

In fact, a maximal independent set in Γ_N is a collection of vertices of the form $\{x \in \mathbb{Z}_N : x = 5k \text{ or } x = 5l + 3 \text{ for } 0 \leqslant k, l \leqslant q - 1\}$. It is easy to check that this set contains $2q$ elements and independence of the set follows from the fact that 0 and 3 does not belong to $\mathcal{QR}_5$. □

7. Chromatic number of Γ_N

In this section, we find the chromatic number of Γ_N of Type-I and provide both lower and upper bounds for that of Γ_N of Type-II. Before that, we state two results which will be used in deducing these bounds.

Proposition 2. *(See [9]; p.22) For any graph G with vertex set V, $\chi(G) \cdot \alpha(G) \geqslant |V|$.*

Proposition 3. *For graphs G and H, $\chi(G \times H) \leqslant \min\{\chi(G), \chi(H)\}$.*

Proof. The proof follows from the existence of projection graph homomorphisms $G \times H \to G$ and $G \times H \to H$. □

Lemma 11. *For Γ_N of Type-I, $\chi(\Gamma_N) \geqslant 3$.*

Proof. Since, $N = 5q$ and q is a prime of the form $4k+1$, the minimum value of q is 13 and hence, the minimum value of N is 65. We now demonstrate a 5-cycle in Γ_N, as existence of such cycle will ensure $\chi(\Gamma_N) \geqslant \chi(C_5) = 3$.

Consider the vertices $0, 1, 17, 8, 4$ in Γ_N. They form a 5-cycle in Γ_N, taken in order, as $1, 4, 9, 16 \in \mathcal{QR}_N$, thereby proving the lemma. □

Theorem 14. *For Γ_N of Type-I, $\chi(\Gamma_N) = 3$.*

Proof. Since Paley graph of q vertices Γ_q for $q > 5$ is triangulated, $\chi(\Gamma_q) \geqslant 3$. Moreover, $\Gamma_5 \cong C_5$ and $\chi(C_5) = 3$. Therefore, from Theorem 3 it follows that $\chi(\Gamma_N) \leqslant \min\{\chi(\Gamma_5), \chi(\Gamma_q)\} = \min\{\chi(C_5), \chi(\Gamma_q)\} \leqslant 3$. Combining this with Lemma 11, the theorem follows. □

Remark 5. It is also possible to find an explicit 3-coloring for Γ_N of Type-I. Consider the sets $X_1 = \{x \in \mathbb{Z}_N : x \equiv 0 \bmod 5 \text{ or } x \equiv 2 \bmod 5\}$, $X_2 = \{x \in \mathbb{Z}_N : x \equiv 1 \bmod 5 \text{ or } x \equiv 3 \bmod 5\}$ and $X_3 = \{x \in \mathbb{Z}_N : x \equiv 4 \bmod 5\}$. We will show that X_1, X_2 and X_3 are independent sets whose union is $\mathbb{Z}_N$. As a result, they form color classes of Γ_N.

Let $a, b \in X_1$. If both are congruent to 0 mod 5 or 2 mod 5, then their difference is also 0 mod 5 and as a result does not belong to $\mathcal{QR}_5$ and hence does not belong to $\mathcal{QR}_N$. If $a \equiv 0 \bmod 5$ and $b \equiv 2 \bmod 5$, then $a - b \equiv 2 \bmod 5$. Thus $a - b \notin \mathcal{QR}_5$ and hence does not belong to

$\mathcal{QR}_N$. Thus, X_1 is an independent set. The proof for X_2 and X_3 follows similarly.

Theorem 15. *For Γ_N of Type-II, if $p < q$, then*

$$\sqrt{p} < \chi(\Gamma_N) \leqslant \min\{\chi(\Gamma_p), \chi(\Gamma_q)\}.$$

Proof. From Theorem 13, $\alpha(\Gamma_N) < q\sqrt{p}$. Now, by Proposition 2, we have

$$\chi(\Gamma_N) \geqslant \frac{|\mathbb{Z}_N|}{\alpha(\Gamma_N)} > \frac{pq}{q\sqrt{p}} = \sqrt{p}.$$

Other part of the inequality follows from Proposition 3. □

8. Domination number of Γ_N

In this section, we provide some bounds for domination number of Γ_N. Before that, we state two results which will be used in deducing these bounds.

Proposition 4. *[10] Let G be a graph with n vertices.*

1) *If G has a degree sequence $d_1, d_2, \ldots, d_n$ with $d_i \geqslant d_{i+1}$, then*

$$\gamma(G) \geqslant \min\{k : k + (d_1 + d_2 + \ldots + d_k) \geqslant n\}.$$

2) *If G has no isolated vertex and has minimum degree $\delta(G)$, then*

$$\gamma(G) \leqslant \frac{n}{\delta(G)+1} \sum_{j=1}^{\delta(G)+1} \frac{1}{j}.$$

Theorem 16. *If $N = pq$, then $\gamma(\Gamma_N) \geqslant 5$. In particular, if $N = 5q$, then*

$$5 \leqslant \gamma(\Gamma_N) \leqslant 5 \sum_{j=1}^{q} \frac{1}{j}.$$

Proof. For the first part, we assume that $p = 4l + 1$. Since, Γ_N is regular with degree $\frac{\phi(N)}{4} = \frac{(p-1)(q-1)}{4} = l(q-1)$, we have $\gamma(\Gamma_N) \geqslant \min\{k : k + kl(q-1) \geqslant (4l+1)q\} = 5$.

For the second part, i.e., $N = 5q$, we put $l = 1$. Also, as Γ_N has no isolated vertex,

$$\gamma(\Gamma_N) \leqslant \frac{5q}{(q-1)+1} \sum_{j=1}^{q} \frac{1}{j} = 5 \sum_{j=1}^{q} \frac{1}{j}.$$ □

Remark 6. A similar upper bound could have been given for the general case, however the expression being messy, may not provide meaningful insight.

9. Conclusion and future work

In this paper, we introduced Paley-type graphs on composite modulus and proved some basic features of this family. These graphs, due to its connection with quadratic residuosity problem on modulus of the form pq, may find applications in topology-hiding cryptography [13]. However, a lot of questions are still unresolved, e.g., exact automorphism group of Γ_N, a tighter bound for the domination number of Γ_N etc.

Acknowledgement

The author is thankful to Avishek Adhikari of Department of Pure Mathematics, University of Calcutta, India for some fruitful suggestions and careful proofreading of the manuscript. The research is supported in part by National Board of Higher Mathematics, Department of Atomic Energy, Government of India (No 2/48(10)/2013/ NBHM(R.P.)/R&D II/695).

References

[1] W. Ananchuen: *On the adjacency properties of generalized Paley graphs*, Australas. J. Combin., 24, 129-147, 2001.

[2] W. Ananchuen and L. Caccetta: *Cubic and quadruple Paley graphs with the n-e.c. property*, Discrete Math., 306, 2954-2961, 2006.

[3] R.D. Baker, G.L. Ebert, J. Hemmeter and A. Woldar: *Maximal cliques in the Paley graph of square order*, J. Statist. Plann. Inference, 56(1), 33-38, 1996.

[4] S.D. Cohen: *Clique Numbers of Paley Graphs*, Quaest. Math., 11(2), 225-231, 1988.

[5] A. Das: *Quadratic Residue Cayley Graphs on Composite Modulus*, Mathematics and Computing, Springer Proceedings in Mathematics and Statistics, Vol. 139, 2015.

[6] A.N. Elsawy: *Paley graphs and their generalizations*, M.S. Thesis, Heinrich Heine University, Germany, 2009.

[7] R.E. Giudici and A.A. Olivieri: *Quadratic modulo 2^n Cayley graphs*, Discrete Math., 215, 73-79, Elsevier, 2000.

[8] C. Godsil and G. Royle: *Algebraic Graph Theory*, Graduate Texts in Mathematics, Springer, 2001.

[9] R. Hammack, W. Imrich and S. Klavzar: *Handbook of Product Graphs*, Second Edition, CRC Press, 2011.

[10] T.W. Haynes, S.T. Hedetniemi and P.J. Slater: *Fundamentals of Domination in Graphs*, Marcel Dekker Inc., 1998.

[11] T.K. Lim and C.E. Praeger: *On generalized Paley graphs and their automorphism groups*, Michigan Math. J., (58) 2009, 293-308.

[12] E. Maistrelli and D.B. Penman: *Some colouring problems for Paley graph*, Discrete Math., Vol. 306, Issue 1, 99-106, 2006.

[13] T. Moran, I. Orlov and S. Richelson: *Topology-Hiding Computation*, Cryptology E-print Archive, 2014. Available at http://eprint.iacr.org/2014/1022.pdf.

[14] K.H. Rosen: *Elementary Number Theory and Its Applications*, Addison-Wesley, 1984.

[15] D.B. West: *Introduction to Graph Theory*, Prentice Hall, 2001.

[16] K. Wu, W. Su, H. Luo and X. Xu: *A generalization of generalized Paley graphs and new lower bounds for $R(3, q)$*, The Electronic Journal of Combinatorics, 17 (2010).

[17] H. Zhang: *Independent Sets in Direct Products of Vertex-Transitive Graphs*, J. Combin. Theory Ser. B, Vol 102, Issue 3, pg. 832-838, 2012.

Contact information

Angsuman Das Department of Mathematics,
Presidency University, Kolkata.
86/1, College Street, Kolkata 700073, India
E-Mail(s): angsuman.maths@presiuniv.ac.in

Received by the editors: 02.02.2015
and in final form 27.08.2019.