

Paley graph and its clique number

Armanbyek Soltanmurat

January 9, 2025

Introduction

Definition

Let q and r be two positive integers with $\gcd(q, r) = 1$, then r is a *quadratic residue* of q if and only if $x^2 \equiv r \pmod{q}$ has a solution, and r is a *quadratic nonresidue* of q if and only if $x^2 \equiv r \pmod{q}$ has no solution.

Definition

Let p be an odd prime number and a is an integer. The Legendre symbol is a function of a and p , defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Properties of Legendre symbol

Lemma

If p is an odd prime, then the numbers $0^2, 1^2, 2^2, \dots, \left[\frac{p-1}{2}\right]^2$ are distinct modulo p .

Theorem

If p is an odd prime and $a, b \in \mathbb{Z}$, then:

- 1 $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- 2 If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$.
- 3 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$

Euler's criterion

Theorem

If p is an odd prime, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Proof.

If $p \mid a$, both sides are trivially zero.

If a is a quadratic residue, then $a \equiv b^2$ for some $b \in \mathbb{Z}_p^*$, so

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem.

Now consider the equation

$$y^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Proof continued...

Proof.

By Lagrange's Theorem, this equation has at most $\frac{p-1}{2}$ solutions. However, all $\frac{p-1}{2}$ quadratic residues (Lemma 3) are already solutions! Hence, a is a quadratic residue if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Finally, observe that Fermat's Little Theorem can be factored (uniquely modulo p) as

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) \pmod{p}.$$

We conclude that a is a non-residue if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Definition of Paley graph

Definition

Let q be a prime power such that $q \equiv 1 \pmod{4}$. The graph $P = (V, E)$, where

$$V(P) = \mathbb{F}_q \quad \text{and} \quad E(P) = \{\{x, y\} : x, y \in \mathbb{F}_q, x - y \in (\mathbb{F}_q^*)^2\},$$

is called the *Paley graph* of order q .

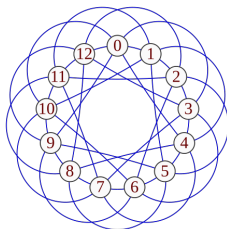


Figure: Paley graph of order 13

Proof of Self-Complementary Property

Theorem

Let P be the Paley graph of order $q = p^n$. Then P is a self-complementary graph.

Proof.

Let r be a quadratic nonresidue modulo q , and define the function $f : V(P) \rightarrow V(P)$ by $f(x) = rx$. To show f preserves adjacency, note that $\{x, y\} \in E(P) \iff (x - y) \in (\mathbb{F}_{p^n}^*)^2 \iff f(x) - f(y) = r(x - y) \iff r(x - y) \notin (\mathbb{F}_{p^n}^*)^2 \iff \{f(x), f(y)\} \notin E(P)$.

Thus, f preserves adjacency. Next, we prove f is a bijection: Suppose $f(x) = f(y)$. Then $rx = ry \implies r(x - y) = 0$. Since $r \neq 0$, it follows that $x = y$. Since $\gcd(r, q) = 1$, there exist integers $a, b \in \mathbb{Z}$ such that $1 = qa + rb \implies rb \equiv 1 \pmod{q}$. Thus, for any $x \in V(P)$, we can write $f(bx) = r(bx) = x$. □

Strong regularity of Paley graph

Theorem

Let P be the Paley graph of order $q = p^n$. Then P is a strongly regular graph with parameters $\text{srg}(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

Proof.

Let $x \in V(P)$ $d(x) = |N(x)| = |(\mathbb{F}_{p^n}^*)^2|$. By Lemma 3, $|(\mathbb{F}_{p^n}^*)^2| = \frac{q-1}{2}$. Consider two adjacent vertices x and y in P .

$$x - y = a^2.$$

Let z be a common neighbor of both x and y . Then we have:

$$x - z = b^2 \quad \text{and} \quad y - z = c^2.$$

To count the number of common neighbors of x and y we count the different solutions for z . We can get that $(b - c)(b + c) = a^2$.

Let $b - c = t$ then $b + c = t^{-1}a^2$



$$b = \frac{t + t^{-1}a^2}{2}, \quad c = \frac{t^{-1}a^2 - t}{2}.$$

We consider different cases for t :

- ① If $t = t$, then $t = 0$ and $c = 0$.
- ② If $t = -t$, then $t = 0$ and $c = 0$.
- ③ If $t = -a^2t^{-1}$, then $t = \pm ia$, and $b = 0$.
- ④ If $t = a^2t^{-1}$, then $t = \pm a$ and $c = 0$.

Hence, we exclude these five solutions which are $t = 0, \pm ia, \pm a$ from the set \mathbb{F}_q . We now count the number of common neighbors of nonadjacent x and y . Let $x - y = r, r \notin (\mathbb{F}_q^*)^2$. Similarly, we can get

$$b = \frac{t + t^{-1}r}{2}, \quad c = \frac{t^{-1}r - t}{2}.$$

$t = rt^{-1}$ and $t = -rt^{-1}$ are impossible because we get $r = t^2$ and $r = -t^2$. So we only exclude $t = 0$.

Upper bound for the clique number

Theorem

Let q be a prime power such that $q \equiv 1 \pmod{4}$ and P be Paley graph order of q . Then $\omega(P) \leq \sqrt{q}$

Proof.

Let $N = \omega(P)$, and let $C = \{v_1, v_2, \dots, v_N\} \subseteq \mathbb{F}_q$ be a clique of the maximum size in P . Let g be a primitive root of \mathbb{F}_q^* , and consider the set

$$W = \{v_i + gv_j : 1 \leq i, j \leq N\}.$$

If $v_i + gv_j = v_{i'} + gv_{j'}$, then $v_i - v_{i'} = g(v_{j'} - v_j)$, which is impossible unless $i = i'$ and $j = j'$. Thus, each element of W is distinct. This implies that $|W| = N^2 \leq q$, i.e.,

$$N \leq \sqrt{q}.$$

