Paley graphs and Paley tournaments

László Babai

Last updated 2021 May 21 at 0:20

1 Congruences

$\mathbb{Z}$ denotes the set of integers.

Definition 1.1. Let $a, b \in \mathbb{Z}$. We say that a **divides** b (notation: $a \mid b$) if $(\exists x)(ax = b)$. (Here x is also an integer.)

Exercise 1.2. Note that $0 \mid 0$.

Definition 1.3. Let $a, b, m \in \mathbb{Z}$. We say that a is **congruent** to b modulo m if $m \mid a - b$. Notation: $a \equiv b \pmod{m}$.

Exercise 1.4. Let $a \equiv b \pmod{m}$. Prove: $\gcd(a, m) = \gcd(b, m)$.

Exercise 1.5. Prove: for a fixed m, the relation $a \equiv b \pmod{m}$ is an equivalence relation on $\mathbb{Z}$.

Terminology 1.6. The equivalence classes of this relation are called **mod** m **residue classes**.

Exercise 1.7. Observe: $a \equiv b \pmod{0}$ if and only if $a = b$.

Notation 1.8. Let $[i]_m$ denote the residue class of i mod m. We call i a *representative* of this residue class.

Exercise 1.9. $[i]_m = [j]_m$ if and only if $i \equiv j \pmod{m}$.

Exercise 1.10. Let $m \neq 0$. Then the number of mod m residue classes is $|m|$.

Exercise 1.11. $\gcd([i]_m, m) := \gcd(i, m)$ is well-defined (it does not depend on the particular choice of representative i).

Definition 1.12. [Arithmetic of residue classes] Let p be a prime number. We define $[a]_m + [b]_m := [a + b]_m$ and $[a]_m \cdot [b]_m := [ab]_m$.

Exercise 1.13. Prove that these definitions are sound. What you need to prove is the following. If $a \equiv x \pmod{m}$ and $b \equiv y \pmod{m}$ then

(i) $a + b \equiv x + y \pmod{m}$

(ii) $ab \equiv xy \pmod{m}$.

Notation 1.14. We write $\mathbb{Z}_m$ to denote the set of residue classes mod m.

Exercise 1.15. Prove that $\mathbb{Z}_m$ is a *commutative ring* under the operations just defined, i. e., each operation is commutative and associative, multiplication is distributive over addition, there is a zero element, and every element has an additive inverse. There is also a multiplicative identity element.

Notation 1.16. The zero element of $\mathbb{Z}_m$ is $[0]_m$ and the identity element is $[1]_m$. Below we shall omit the brackets and write 0_m and 1_m, and we omit m if its value is clear from the context.

Definition 1.17. We say that $b \in \mathbb{Z}_m$ is the multiplicative inverse of $a \in \mathbb{Z}_m$ if $ab = 1_m$. In this case we write $b = a^{-1}$.

Exercise 1.18. Prove: $a \in \mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

Notation 1.19. It follows that if $m = p$ is a prime number then every nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse. In other words, $\mathbb{Z}_p$ is **field**. In recognition of this fact, we change the notation from $\mathbb{Z}_p$ to $\mathbb{F}_p$. So $\mathbb{F}_p$ is the field of residue classes mod p. We refer to $\mathbb{F}_p$ as the **finite field of order** p.

2 Quadratic residues

Definition 2.1. Let p be a prime number and $a \in \mathbb{Z}$. We say that a is a **quadratic residue mod** p if $a \not\equiv 0 \pmod{p}$ (i. e., $p \nmid a$), and $(\exists x \in \mathbb{Z})(a \equiv x^2 \pmod{p})$. We say that $b \in \mathbb{Z}$ is a **quadratic non-residue mod** p if $(\forall x \in \mathbb{Z})(b \not\equiv x^2 \pmod{p})$. Instead of "quadratic non-residue" we often simply say "non-residue."

Exercise* 2.2. -1 is a quadratic residue mod p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Terminology 2.3. Note that $a \in \mathbb{Z}$ is a quadratic residue mod p if and only if $[a]_p \neq 0_p$ and $[a]_p$ is the square of some element in $\mathbb{F}_p$, and $b \in \mathbb{Z}$ is a non-residue mod p if and only if $[b]_p$ is not the square of any element in $\mathbb{F}_p$. For this reason, we also use the terms "quadratic (non-)residue" in relation to $\mathbb{F}_p$: we say that an element $a \in \mathbb{F}_p$ is a quadratic residue if $a \neq 0_p$ and $(\exists x \in \mathbb{F}_p)(a = x^2)$, and we say that an element $b \in \mathbb{F}_p$ is a non-residue if $(\forall x \in \mathbb{F}_p)(b \neq x^2)$.

Exercise 2.4. Prove that (a) the number of quadratic residues in $\mathbb{F}_p$ is $(p-1)/2$ and (b) the number of non-residues in $\mathbb{F}_p$ is $(p-1)/2$.

Exercise 2.5. Let us represent the elements of $\mathbb{F}_{13}$ by the numbers $\{-6, -5, \ldots, 5, 6\}$. Verify that the quadratic residues are $\{\pm 1, \pm 3, \pm 4\}$. Accordingly, the non-residues are $\{\pm 2, \pm 5, \pm 6\}$.

Exercise 2.6. Prove: (a) if a, b are quadratic residues in $\mathbb{F}_p$ then so is ab (b) if a is a q. residue and b is a non-residue in $\mathbb{F}_p$ then ab is a non-residue (c) if a and b are non-residues then ab is a q. residue. (Only part (c) is non-trivial.)

Let p be an odd prime. We define the *quadratic character* $\chi_2 : \mathbb{F}_p \to \{0, 1, -1\}$ by setting, for $a \in \mathbb{F}_p$,

$$\chi_2(a) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \text{ and } a \text{ is a square in } \mathbb{F}_p \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_p \end{cases}$$

A common notation for the quadratic character mod p is the **Legendre symbol** $\left(\frac{a}{p}\right) := \chi_2(a)$. In these notes we shall not use the Legendre symbol.

Exercise 2.7. Prove: the quadratic character is multiplicative, i. e., $(\forall a, b \in \mathbb{F}_p)(\chi_2(ab) = \chi_2(a)\chi_2(b))$.

Exercise 2.8. Let p be an odd prime (i. e., $p \neq 2$). Prove: $\sum_{a \in \mathbb{F}_p} \chi_2(a) = 0$.

Exercise 2.9. Prove: $\chi_2(a) \equiv a^{(p-1)/2} \pmod{p}$.

Exercise 2.10. [Multiplicativity] Prove: $\chi_2(ab) = \chi_2(a)\chi_2(b)$.

Exercise 2.11. Prove: $\left|\sum_{a \in \mathbb{F}_p} \chi_2(a)\chi_2(a-1)\right| = 1$.

3 Paley graphs

In this section, p is a prime number and $p \equiv 1 \pmod{4}$.

Definition 3.1. The **Paley graph of order** p, denoted $\mathrm{PGr}(p)$, is defined as follows. The vertices of $\mathrm{PGr}(p)$ are the elements of the field $\mathbb{F}_p$. Vertices i and j are adjacent if $j - i$ is a quadratic residue in $\mathbb{F}_p$.

Exercise 3.2. Show that this definition is sound: it indeed defines a graph. You need to show that the adjacency relation is symmetric. Show where you use the assumption that $p \equiv 1 \pmod{4}$.

Exercise 3.3. What is the graph $\mathrm{PGr}(5)$?

Exercise 3.4. Show that $\mathrm{PGr}(p)$ is (a) vertex-transitive (all vertices are equivalent under automorphisms) (b) edge-transitive (all edges are equivalent under automorphisms) (c) arc-transitive (all ordered pairs of adjacent vertices are equivalent under automorphisms).

Exercise 3.5. Show that $\mathrm{PGr}(p)$ is self-complementary (isomorphic to its complement).

Exercise 3.6. Show that every vertex of $\mathrm{PGr}(p)$ has degree $(p-1)/2$.

Exercise 3.7. Show that $\mathrm{PGr}(p)$ has diameter 2.

Exercise 3.8. (a) Show that every pair of adjacent vertices of $\mathrm{PGr}(p)$ has the same number of common neighbors. (b) Show that this number is $(p-5)/4$. (c) Show that every pair of distinct, non-adjacent vertices has the same number of common neighbors. (d) Show that this number is $(p-1)/4$.

Exercise 3.9. (a) Show that the adjacency matrix A of $\mathrm{PGr}(p)$ satisfies an equation of the form $A^2 + bA + cI = dJ$. Determine the coefficients b, c, d. (I is the identity matrix, J is the all-ones matrix.) (b) Find the eigenvalues of A. (c) Find the multiplicity of each eigenvalue of A.

4 Paley tournaments

In this section, p is a prime number and $p \equiv -1 \pmod 4$.

Definition 4.1. The **Paley tournament of order** p, denoted $\mathrm{PTr}(p)$, is defined as follows. The vertices of $\mathrm{PTr}(p)$ are the elements of the field $\mathbb{F}_p$. (i, j) is an edge (we draw the arrow $i \to j$) if $j - i$ is a quadratic residue in $\mathbb{F}_p$.

Exercise 4.2. Show that this definition is sound: it indeed defines a tournament. You need to show that this is an orientation of the complete graph, i. e., for every pair $\{a, b\}$ of vertices, exactly one of (a, b) and (b, a) is an edge. Show where you use the assumption that $p \equiv -1 \pmod 4$.

Exercise 4.3. (a) What is $\mathrm{PTr}(3)$? (b) Make a nice drawing of the tournament $\mathrm{PTr}(7)$.

Exercise 4.4. Show that $\mathrm{PTr}(p)$ is (a) vertex-transitive (b) edge-transitive (all edges are equivalent under automorphisms).

Exercise 4.5. Show that $\mathrm{PTr}(p)$ is self-converse (isomorphic to its converse, where every edge is reversed).

Exercise 4.6. Show that every vertex of $\mathrm{PTr}(p)$ has indegree $(p-1)/2$ and the same outdegree. Show that this follows from vertex-transitivity.

Exercise 4.7. Show that the directed diameter of $\mathrm{PTr}(p)$ is 2, i. e., if $a \neq b$ are vertices then b can be reached from a in at most two steps.

Exercise 4.8. (a) Show that for every edge (a, b) in $\mathrm{PTr}(p)$, the number of two-step walks from a to b is the same. (b) Show that this number is $(p-3)/4$. (c) Show that for every edge (a, b) in $\mathrm{PTr}(p)$, the number of two-step walks from b to a is the same. (d) Show that this number is $(p+1)/4$.

Definition 4.9. Let $G = ([n], E)$ be an oriented graph. This means that the adjacency relation is antisymmetric: if $(u, v) \in E$ then $(v, u) \notin E$. We define the **$\pm$-adjacency matrix** $A = (a_{ij})$ of G as follows:

$$a_{ij} = \begin{cases} 1 & \text{if } (i,j) \in E \\ -1 & \text{if } (j,i) \in E \\ 0 & \text{otherwise} \end{cases}$$

Note that this includes $a_{ii} = 0$. If G is a tournament then $a_{ij} = 0 \iff i = j$.

Exercise 4.10. Let G be an oriented graph and let A be its $\pm$-adjacency matrix.
(a) Observe that $A^T = -A$.
(b) Assume $(\forall i, j)(\deg^+(i) = \deg^-(j))$ (all indegrees and outdegrees are equal). Then the all-ones vector is an eigenvector of A. What is the corresponding eigenvalue?
(c) If G is vertex-transitive then the assumption in (b) holds.

Exercise 4.11. Let A be the $\pm$-adjacency matrix of the Paley tournament $\mathrm{PTr}(p)$.
(i) Prove that A^2 can be expressed as $A^2 = aI + bJ$. Determine the coefficients a and b.
(ii) Determine the eigenvalues of A^2 and their multiplicities.
(iii) Determine the eigenvalues of A and their multiplicities (over $\mathbb{C}$).