Cayley Graphs.

Definition. A group Γ is a set with a map $*: \Gamma \times \Gamma \to \Gamma$ so that

1) For all $a, b, c \in \Gamma$,

$$(a * b) * c = a * (b * c)$$

2) There exists some $e \in \Gamma$ so that for all $a \in \Gamma$ we have

$$a * e = e * a = a$$

3) For each $a \in \Gamma$, there exists some $a^{-1} \in \Gamma$ so that

$$a * a^{-1} = a^{-1} * a = e.$$

Definition. If $S \subset \Gamma$ is closed under inverses, or for every $s \in S$ the element s^{-1} is also in S, then we say S is a set of generators.

Definition. The Cayley graph generated by S is the graph with vertex set Γ and $u \bullet\!\!-\!\!\bullet v \iff \exists$ some $s \in S$ so $u * s = v$.

Example. $\mathbb{Z}/n\mathbb{Z}$ is the group with elements $0, 1, \ldots, n-1$ and group operation $u * v = u + v \pmod{n}$. $S = \{1, n-1\}$.

The Cayley graph is

$$1 \bullet\!\!-\!\!\bullet 2 \bullet\!\!-\!\!\bullet 3 \bullet\!\!-\!\!\bullet \cdots \bullet\!\!-\!\!\bullet n-1 \bullet\!\!-\!\!\bullet 1$$

or the cycle graph C_n.

Example. $(\mathbb{Z}/2\mathbb{Z})^d$ is the group with elements given by bit strings $b_1 \ldots b_d$ (each $b_i \in \{0,1\}$). and group operator

$$(b_1 \ldots b_d) * (c_1 \ldots c_d) = (b_1 \text{ xor } c_1) \ldots (b_d \text{ xor } c_d)$$

$$= (b_1 + c_1 \bmod 2) \ldots (b_d + c_d \bmod 2).$$

S is the set $(10\ldots0), (010\ldots0), \ldots, (0\ldots01)$ of strings with a single 1. The Cayley graph is the hypercube.

We now study

Definition. The Paley graph is the Cayley graph with group $\mathbb{Z}/p\mathbb{Z}$ (under addition) with p a prime number congruent to $1 \bmod 4$, and $S = \{ s \in \mathbb{Z}/p\mathbb{Z} \mid s = x^2 \bmod p \}$.

We recall:

$\mathbb{Z}/p\mathbb{Z}$ is a field (a group both additively and multiplicatively).

Proposition. $S = \{ s \in \mathbb{Z}/p\mathbb{Z} \mid s = x^2 \bmod p \}$ is closed under inverses if $p = 1 \bmod 4$ and p is prime.

We first observe that it suffices to show that $-1 = i^2 \bmod 4$ for some $i \in 1, \ldots, p$. since $s = x^2 \iff -s = (ix)^2$.

We recall that

Proposition. The finite field $\mathbb{Z}/p\mathbb{Z}$ contains at least one primitive element $g \in 1, \ldots, p-1$. The primitive element generates $1, \ldots, p-1$ by taking powers $g, g^2, g^3, \ldots, g^{p-1} \bmod p$.

Corollary. $g^{p-1} \equiv 1 \bmod p$, and no smaller power of g is equal to $1 \bmod p$.

Now we know $(p-1)/4$ is an integer, since $p \equiv 1 \bmod 4$. Take any primitive element g and let

$$i = g^{(p-1)/4} \bmod p.$$

We claim $i^2 = -1$. First, we know that $i^4 = g^{p-1} = 1$, and that $i^2 = g^{(p-1)/2} \neq 1$. Next, we know that since $\mathbb{Z}/p\mathbb{Z}$ is a field, it is an "integral domain", and $ab \equiv 0 \bmod p \Rightarrow a = 0$ or $b = 0 \bmod p$. (This also follows from the fact that p is prime.) Thus if $i^4 =_p 1$, then

$$(i^2 - 1)(i^2 + 1) =_p i^4 - 1 =_p 0$$

so $i^2 =_p +1$ or $i^2 =_p -1$. Since $i^2 \neq_p +1$, we

conclude that $i^2 = -1$, as desired. □ (7)

Now we also know:

Lemma. If p is a prime and $p \equiv 1 \bmod 4$, then there are $\frac{p-1}{2}$ elements in S.

Proof. Take any primitive g. The even powers of g are certainly squares. If $g^{2K+1} \equiv x^2 \bmod p$, then

$$g = g^{2K+1} \cdot g^{-2K} = (x \cdot g^{-K})^2,$$

so g is itself a square. Now if $g = y^2$, then $g^{\frac{p-1}{2}} = y^{p-1} = 1$, which is false. So these are the only squares in $\mathbb{Z}/p\mathbb{Z}$. □

We can conclude:

Proposition. The Paley graph with prime p is regular with degree $\frac{p-1}{2}$.

Proof. (Homework)

We are now going to compute the eigenvalues of the Paley graph.

Claim. If $1_{p\times p}$ is the $p\times p$ matrix of all 1's, and L is the Laplacian of the Paley graph based on p,

$$L^2 = pL + \frac{p-1}{4} 1_{p\times p} - \frac{p(p-1)}{4} I$$

To prove this, we start by defining

Definition. The quadratic character $\chi(a)$ of $a \in \mathbb{Z}/p\mathbb{Z}$ is given by

$$\chi(a) = \begin{cases} 1, & \text{if } a \text{ is a square mod } p \\ 0, & \text{if } a \text{ is } 0 \\ -1, & \text{otherwise} \end{cases}$$

Note that $\chi(ab) = \chi(a)\chi(b)$, for all $a, b \in \mathbb{Z}/p\mathbb{Z}$.

We let X be the $p \times p$ matrix defined by

$$X(a,b) = \chi(a-b)$$

Homework: $X = pI - 2L - 1_{p \times p}$.

We now prove:

Lemma. $X^2 = pI - 1_{p\times p}$.

Proof. Each column of X consists of $\chi(0-k), \chi(1-k), \ldots, \chi(p-1-k)$, which are the characters of all elements of $\mathbb{Z}/p\mathbb{Z}$. We know that $\frac{p-1}{2}$ of these are $+1$, $\frac{p-1}{2}$ are -1, and 1 is 0.

Now $\chi(a-b) = \chi(b-a)$ (because -1 is a square!) so X is symmetric. Thus $X^2 = X^T X$ and the entries in X^2 are dot products of columns of X.

On the diagonal, we sum the squares of $\frac{p-1}{2}$ ones, $\frac{p-1}{2}$ -ones and 1 zero to get $p-1$.

Off the diagonal,

$$X^2(a,b) = \sum_x X(a-x)X(b-x).$$

If we set $y = a-x$, we can r/w the sum

$$= \sum_y X(y)X(b-a+y)$$

Now set $w = b-a$ (for convenience). Since we are off the diagonal, $w \neq 0$.
Further, when $y=0$, $X(y)X(b-a+y) = 0$, so we can r/w as

$$= \sum_{y=1}^{p-1} X(y)X(w+y)$$

Now if $y = x^2$ then $\frac{1}{y} = \left(\frac{1}{x}\right)^2$, so $\chi(y) = \chi(1/y)$. Thus we can r/w as

$$= \sum_{y=1}^{p-1} \chi(1/y)\,\chi(\omega + y)$$

$$= \sum_{y=1}^{p-1} \chi(\omega/y + 1).$$

For any fixed ω, the set $\{\omega/1, \omega/2, \ldots, \omega/p-1\}$ is a rearrangement of $\{1, \ldots, p-1\}$. Thus $\{\omega/1 + 1, \ldots, \omega/p-1 + 1\}$ is a rearrangement of $\{2, \ldots, p\}$, so our sum is

$$= \sum_{y=2}^{p} \chi(y) = \underbrace{\sum_{y=0}^{p-1} \chi(y)}_{0} - \chi(1) = -1$$

This proves all off-diagonal entries are -1, completing the proof.

Homework: $X^2 = pI - 1_{p\times p}$ and

$$X = pI - 2L - 1_{p\times p} \Rightarrow L^2 = pL + \frac{p-1}{4} 1_{p\times p} - \frac{p(p-1)}{4} I$$

Now if $\vec{\varphi}$ is an eigenvector of L (orthogonal to $\vec{1}_p$), we know

$$L^2\vec{\varphi} = pL\vec{\varphi} + -\frac{p(p-1)}{4}\vec{\varphi}$$

or if $L\varphi = \lambda\varphi$,

$$\lambda^2\varphi = \left(p\lambda - \frac{p(p-1)}{4}\right)\varphi$$

so

$$\lambda^2 - p\lambda + \frac{p(p-1)}{4} = 0$$

and

$$\lambda = \frac{p \pm \sqrt{p^2 - 4\,\frac{p-(p-1)}{4}}}{2}$$

$$= \frac{p \pm \sqrt{p^2 - (p^2 - p)}}{2}$$

$$= \frac{p \pm \sqrt{p}}{2}.$$

Therefore the eigenvalues of the Paley graph are 0 (once), $\frac{p+\sqrt{p}}{2}$, and $\frac{p-\sqrt{p}}{2}$.

Since there are p vertices, these are very close to the eigenvalues of the complete graph K_p (always p-1).