Spectral Graph Theory: Cuts and diameter - exercise 2

[redacted]

2-) The Paley graph $Pay(p)$ is defined as follows. Take a prime p with $p \cong 1$(mod 4). Consider the graph with vertex set the integers modulo p and two vertices i, j form an edge if $i - j$ is a square in $(\mathbb{Z}/p\mathbb{Z})^*$. Give upper and lower bounds for the isoperimetric number of Pay(p) and give asymptotic expressions for this number when $p \to \infty$.

First, see that the Paley graph is well defined: If $i \sim j$, $i - j = t^2$ for some $t \in (\mathbb{Z}/p\mathbb{Z})^*$. Then $j - i = -t^2$ which is a square in $(\mathbb{Z}/p\mathbb{Z})^*$ if and only if -1 is a square, which is true due to the fact that $p \cong 1 \pmod 4$. So the adjacency relation is symmetric. Moreover $i \nsim i$ because $i - i = 0$, and $0 \notin (\mathbb{Z}/p\mathbb{Z})^*$.

The isoperimetric number of G is defined as $i(G) = \min\{\frac{e(A,V\setminus A)}{|A|}, A \subset V, 0 < |A| \leq n/2\}$ and can be bounded by $\frac{\mu_2}{2} \leq i(G) \leq \delta(G)$ where μ_2 is the second smallest eigenvalue of the Laplacian matrix of G.
The first inequality was proved in class. For the second inequality, restrict A to be a single vertex v. Then $i(G) = \min_{A \subset V} \frac{(e(A, V \setminus A)}{|A|} \leq \min_{v \in V} e(\{v\}, V \setminus \{v\}) \leq \delta(G)$. So our aim is to compute $\delta(G)$ and μ_2.

Now, we will discuss some properties of the Paley graph. The first one is that the Paley graph is a $\frac{p-1}{2}$-regular graph. In order to prove it, we see that the number of quadratic residues in $(\mathbb{Z}_p)^*$ is $\frac{p-1}{2}$. This is due to the fact that $i^2 \cong (p-i)^2 \pmod p$ so there are $p-1$ different elements in $\mathbb{Z}_p$ that yield to $\frac{p-1}{2}$ quadratic residues different from 0.
Take a vertex $i \in \mathbb{Z}/p\mathbb{Z}$. Then $\forall z \neq 0$ quadratic residue, define $j = i + z \pmod p$. By definition, $i \sim j$. In particular, $d(i) = \frac{p-1}{2}, \forall i \in \mathbb{Z}/p\mathbb{Z}$, Pay(p) is $\frac{p-1}{2}$-regular.
Here, we already have an upper bound $i(G) \leq \frac{p-1}{2}$.

For the lower bound, we need to compute μ_2. As the Paley graph is regular, the Laplacian matrix can be written as

$$L(G) = \frac{p-1}{2} Id - A(G)$$

So $\mu_2 = \frac{p-1}{2} - \lambda_2$.

In order to compute λ_2, notice that A(G) is circulant. Suppose $i \sim j$, for $i, j \in \mathbb{Z}_p$. Then $i + 1 \sim j + 1$ because the difference between these 2 numbers is the same. So the adjacency matrix is circulant.
Since A is circulant, the spectra can be computed easily. For λ_2:

$$\lambda_2 = \sum_{j=1}^{n} a_j (w_n^2)^{j-1}$$

where w is a primitive n–th root of unity.

In this sum, $a_j = 1 \iff j \sim 1 \iff j-1$ is a quadratic residue different from 0. Hence, the sum can be written in terms of the quadratic residues:

$$\lambda_2 = \sum_{t=1}^{\frac{p-1}{2}} (e^{\frac{4i\pi}{p}})^{t^2} = \frac{\sum_{t=1}^{p-1} (e^{\frac{4i\pi}{p}})^{t^2}}{2} = \frac{\sum_{t=0}^{p-1} (e^{\frac{4i\pi}{p}})^{t^2} - 1}{2}$$

where we have used the fact that $t = i$ and $t = p - i$ lead to the same quadratic residue. Now, we use that the sum $\sum_{t=0}^{p-1} (e^{\frac{4i\pi}{p}})^{t^2}$ is a well-known sum called Quadratic Gauss Sum and its result is $\sqrt{p}$ for $p \cong 1 \bmod(4)$ (see [1]).
It follows that $\lambda_2 = \frac{\sqrt{p}-1}{2}$ and $\mu_2 = \frac{p-1}{2} - \frac{\sqrt{p}-1}{2} = \frac{p-\sqrt{p}}{2}$.

Substituting in $\frac{\mu_2}{2} \leq i(G) \leq \delta(G)$, the bounds for $i(G)$ are:

$$\frac{p-\sqrt{p}}{4} \leq i(G) \leq \frac{p-1}{2}$$

so dividing by p and asymptotically:

$$\frac{1}{4} \leq \lim_{p\to\infty} \frac{i(G)}{p} \leq \frac{1}{2}$$

References

[1] Ireland K. and Rosen M. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 1990.