APPROVAL PAGE FOR GRADUATE THESIS OR PROJECT

GS-13

SUBMITTED IN PARTIAL FULFILLMENT OF REQUIREMENTS FOR DEGREE OF MASTER OF SCIENCE AT CALIFORNIA STATE UNIVERSITY, LOS ANGELES BY

Edward K. Voskanian
Candidate

Mathematics
Department

TITLE: **THE KAZHDAN CONSTANT OF** $(\mathbb{Z}_p, \Gamma_p)$

APPROVED:

Anthony Shaheen Committee Chairperson	Signature
Mike Krebs Faculty Member	Signature
Gary Brookfield Faculty Member	Signature
Grant A. Fraser Department Chairperson	Signature

DATE: **June 03, 2013**

THE KAZHDAN CONSTANT OF $(\mathbb{Z}_p, \Gamma_p)$

A Thesis

Presented to

The Faculty of the Department of Mathematics

California State University, Los Angeles

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

By

Edward K. Voskanian

June 2013

To my loving family:

Anahid, Edward, Shushan, Armen

Cindy, Derek, Lilia, Arpi

and my beautiful fiancé Lilit

Abstract

The Kazhdan Constant of $(\mathbb{Z}_p, \Gamma_p)$

By

Edward K. Voskanian

Let p be any prime number greater than 2 and let Γ_p be the set consisting of all squares in the group $\mathbb{Z}_p^\times$. From [2], the Kazhdan constant of the pair $(\mathbb{Z}_p, \Gamma_p)$ denoted $\kappa(\mathbb{Z}_p, \Gamma_p)$, is bounded below by a formula involving the second largest eigenvalue of the Paley graph $\mathrm{Cay}(\mathbb{Z}_p, \Gamma_p)$, which gives $\sqrt{2}$ as its best estimate as p tends to infinity. The main work of this thesis is providing another formula for the lower bound that tends to 2 as p tends to infinity. And because the Kazhdan constant is bounded above by 2, we get the best possible lower bound in the limit. We use the Chinese Remainder Theorem to obtain explicit formulas for $\kappa(\mathbb{Z}_p, \Gamma_p)$ that are valid for particular classes of primes. However, we do not obtain a generalized formula for any prime. Instead we use a result by Peralta to get a lower bound on $\kappa(\mathbb{Z}_p, \Gamma_p)$. We then take the limit over p to get our main theorem.

Contents

List of Tables

Table

List of Figures

Figure

Chapter 1

The Kazhdan Constant

In this chapter, we define the Kazhdan constant for a finite group/subset pair and then ultimately fix our attention to the pair $(\mathbb{Z}_p, \Gamma_p)$. For a given odd prime, the irreducible unitary representations of the group $\mathbb{Z}_p$ allow us to determine the value of $\kappa(\mathbb{Z}_p, \Gamma_p)$ as the distance of a chord on the unit circle. From this perspective, we obtain new results on the Kazhdan constant, one of which is obtaining a formula valid for any prime number congruent to 3 modulo 4.

1.1 Representation Theoretic Invariant

We begin by defining the Kazhdan constant for a given pair consisting of a finite group G and a nonempty subset $\Gamma \subset G$. As we will see in the definition, to obtain the Kazhdan constant of the pair (G, Γ), we must have a complete set of inequivalent, nontrivial, unitary, irreducible representations of the group G, all of which will be defined in this section. Note that we will call this collection the *unitary irreps* of G, not to be confused with the shorthand for an irreducible representation. Equipped with the *unitary irreps* of the groups $\mathbb{Z}_n$ and S_3, we will demonstrate how to calculate a Kazhdan constant for pairs involving these groups.

Definition 1.1. *Let G be a finite group. A representation of G is a group homomorphism $\rho : G \to GL(V)$, where V is a finite dimensional vector space, and $GL(V)$ is the general linear group consisting of all bijective linear transformations from V to*

itself with function composition as the group operation.

From the definition above, a given representation of a group G comes with a finite dimensional vector space V. For our purposes, we only want to consider representations that correspond to *unitary* operators. That is, we want the induced vector space V to be equipped with a G invariant inner product.

Definition 1.2. *If $\rho : G \to GL(V)$ is a representation of G with*

$$\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$$

for all $g \in G$ and $v, w \in V$, we say that ρ is unitary.

Definition 1.3. *Let G be a finite group and $\rho : G \to GL(V)$ a representation of G. Given a subspace W of V, if $\rho(g)w \in W$ for all $g \in G$ and $w \in W$, we say that the representation restricted to vectors in W is a subrepresentation. A representation is said to be irreducible if the only subrepresentations are those restricted to the trivial subspaces V and $\{0\}$.*

We will define the Kazhdan in two parts.

Definition 1.4. *Let G be a finite group, and let Γ be a nonempty subset of G. Let ρ be a unitary representation of G. We define*

$$\kappa(G, \Gamma, \rho) = \min_{\|v\|=1} \max_{\gamma \in \Gamma} \|\rho(\gamma)v - v\|$$

.

Definition 1.5. *Let G be a finite nontrivial group, and let Γ be a nonempty subset of G. Define*

$$\kappa(G, \Gamma) = \min_{\rho} \{\kappa(G, \Gamma, \rho)\}$$

where the minimum is over all irreducible, nontrivial, unitary representations ρ of G. The number $\kappa(G,\Gamma)$ is called the Kazhdan constant for the pair (G,Γ).

The *unitary irreps* associated with calculating $\kappa(\mathbb{Z}_p,\Gamma_p)$ allow us to take our problem into a geometrical setting, and they are given in the following theorem, which is taken from $[2, p.173]$.

Theorem 1.6. *The irreducible representations of $\mathbb{Z}_n$ are given by $\rho_a(k) : \mathbb{C} \to \mathbb{C}$ defined as*

$$\rho_a(k)z = e^{\frac{2\pi iak}{n}}z,$$

where $a = 0, 1, 2, ..., n-1$.

Moreover, $\rho_0, \rho_1, \rho_2, ..., \rho_{n-1}$ form a complete set of inequivalent, unitary, irreducible, representations of $\mathbb{Z}_n$.

In the following example, we see how the *unitary irreps* of the group $\mathbb{Z}_n$ simplify things. Because of how the maps are defined, we can factor out the vector v in Definition 1.3 and thus ignore the minimum.

Example 1.1.1. Let $G = \mathbb{Z}_6$ and let $\Gamma = \{1\}$. We have that

$$\begin{aligned}\|\rho_a(1)z - z\| &= \|e^{\frac{2\pi i(a)(1)}{6}}z - z\| \\ &= \|z\| \cdot \|e^{\frac{\pi i(a)}{3}} - 1\|.\end{aligned}$$

Hence,

$$\begin{aligned}\kappa(\mathbb{Z}_6,\{1\}) &= \min_{a=1,2,...,5}\left\{\min_{\|z\|=1}\|z\| \cdot \|e^{\frac{\pi i(a)}{3}} - 1\|\right\} \\ &= \min_{a=1,2,...,5}\left\{\|e^{\frac{\pi i(a)}{3}} - 1\|\right\}\end{aligned}$$

$$= \min\left\{\|e^{\frac{\pi i}{3}} - 1\|, \|e^{\frac{2\pi i}{3}} - 1\|, \|e^{\pi i} - 1\|, \|e^{\frac{4\pi i}{3}} - 1\|, \|e^{\frac{5\pi i}{3}} - 1\|\right\}$$

$$= 2 - 2\cos\frac{\pi}{3} = 1.$$

The following proposition generalizes Example 1.1.1 to any natural number n.

Proposition 1.7. *Let n be a natural number with $n \geq 2$. The Kazhdan constant for the pair $(\mathbb{Z}_n, \{1\})$ is given by the formula*

$$\kappa(\mathbb{Z}_n, \{1\}) = 2\sin\frac{\pi}{n}.$$

Moreover,

$$\lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 0.$$

Proof. Let $\theta \in \mathbb{R}$ with $0 \leq \theta \leq 2\pi$. We get

$$|e^{i\theta} - 1| = \sqrt{2}\sqrt{1 - \cos\theta} = 2\sqrt{\frac{1-\cos\theta}{2}} = 2\sin\frac{\theta}{2}.$$

Using this identity, we get

$$\begin{aligned}
\kappa(\mathbb{Z}_n, \{1\}) &= \min_{\rho}\{\kappa(\mathbb{Z}_n, \{1\}, \rho)\} \\
&= \min_{a=1,2,\ldots,n-1}\left\{\min_{\|z\|=1}\max_{\gamma\in\{1\}}\|e^{\frac{2\pi i a\gamma}{n}}z - z\|\right\} \\
&= \min_{a=1,2,\ldots,n-1}\left\{\min_{\|z\|=1}\|z\|\cdot\|e^{\frac{2\pi i a}{n}} - 1\|\right\} \\
&= \min\left\{\|e^{\frac{2\pi i}{n}} - 1\|, \|e^{\frac{4\pi i}{n}} - 1\|, \|e^{\frac{6\pi i}{n}} - 1\|, \ldots, \|e^{\frac{2(n-1)\pi i}{n}} - 1\|\right\}. \\
&= \min\left\{2\sin\frac{\pi}{n}, 2\sin\frac{2\pi}{n}, 2\sin\frac{3\pi}{n}, \ldots, 2\sin\left((n-1)\frac{\pi}{n}\right)\right\}.
\end{aligned}$$

Notice that we are minimizing $f(x) = 2\sin\frac{\pi}{n}x$ over integer values in the interval

[1,$n-1$]. See Figure 1.1. Therefore,

$$\kappa(\mathbb{Z}_n, \{1\}) = \min_{a=1,2,\ldots,n-1} \left\{ 2 \sin \frac{\pi a}{n} \right\}$$
$$= 2 \sin \frac{\pi}{n}.$$

Having acquired a formula for $\kappa(\mathbb{Z}_n, \{1\})$, we simply take a limit to get the second result. □

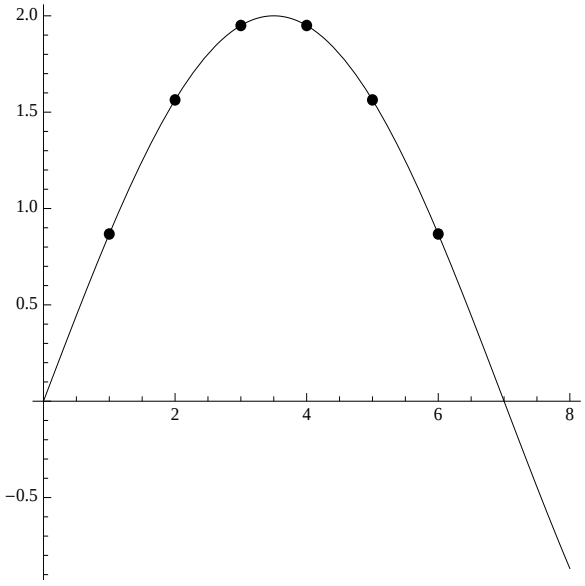

Figure 1.1: Minimum value from the graph.

Remark 1.8. *We present an alternate proof for Proposition 1.7.*

We have that

$$\kappa(\mathbb{Z}_n, \{1\}) = \min \left\{ \|e^{\frac{2\pi i}{n}} - 1\|, \|e^{\frac{4\pi i}{n}} - 1\|, \|e^{\frac{6\pi i}{n}} - 1\|, ..., \|e^{\frac{2(n-1)\pi i}{n}} - 1\| \right\},$$

which is just a minimum among $n-1$ chords on the unit circle.

Using the distance formula, we obtain the Kazhdan constant as the length of the shortest chord. Therefore,

$$d = \sqrt{(\cos \frac{2\pi}{n} - 1)^2 + (\sin \frac{2\pi}{n} - 0)^2} = 2 \sin \frac{\pi}{n}.$$

Consider the symmetric group S_3. Theorem 1.10 gives all the *unitary irreps* for S_3 for which we will need to calculate $\kappa\left(S_3, \{(2,3),(1,2)\}\right)$ in Example 1.1.2. See [2] for a proof.

Definition 1.9. *Consider the homomorphism sgn* : $S_n \to \{-1, 1\}$ *where*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, \text{ if } \sigma \text{ is an even permutation} \\ \\ -1, \text{ if } \sigma \text{ is an odd permutation} \end{cases}$$

The unitary matrix representation $\pi : S_n \to GL(1, \mathbb{C})$ *given by* $\pi(\sigma) = (sgn(\sigma))$ *is called the alternating representation of* S_n.

Theorem 1.10. *The only unitary irreps of* S_3 *are the alternating representation* π_1 *and the representation* $\pi_2 : S_3 \to GL(\mathbb{C}^2)$ *defined as follows:*

$$\pi_2(()) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \pi_2((1,2)) = \begin{pmatrix} 0 & e^{\frac{4\pi i}{3}} \\ e^{\frac{2\pi i}{3}} & 0 \end{pmatrix} \qquad \pi_2((1,3)) = \begin{pmatrix} 0 & e^{\frac{2\pi i}{3}} \\ e^{\frac{4\pi i}{3}} & 0 \end{pmatrix}$$

$$\pi_2((2,3)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \pi_2((1,2,3)) = \begin{pmatrix} e^{\frac{4\pi i}{3}} & 0 \\ 0 & e^{\frac{2\pi i}{3}} \end{pmatrix} \quad \pi_2((1,3,2)) = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}} \end{pmatrix}$$

Example 1.1.2. Let $G = S_3$, and let $\Gamma = \{(1,2),(1,2,3)\}$. We will calculate the Kazhdan constant of the pair (S_3, Γ). And so we must first calculate $\kappa(S_3, \Gamma, \pi_1)$.

$$\begin{aligned} \kappa(S_3, \Gamma, \pi_1) &= \min_{\|v\|=1} \max_{\gamma \in \Gamma} \left\| \pi_1(\gamma)v - v \right\| \\ &= \min_{\|v\|=1} \max \left\{ \|\pi_1((1,2))v - v\|, \|\pi_1((1,2,3))v - v\| \right\} \\ &= \max\{2, 0\} = 2. \end{aligned}$$

Now we calculate $\kappa(S_3, \Gamma, \pi_2)$ Let $(a, b)^t$ be a unit vector in $\mathbb{C}^2$. Then

$$\begin{aligned}
\left\|\pi_2((1,2,3)) \cdot (a,b)^t - (a,b)^t\right\|^2 &= \left\|(ae^{\frac{4\pi i}{3}} - a, be^{\frac{2\pi i}{3}} - b)^t\right\|^2 \\
&= \left\|e^{\frac{4\pi i}{3}} a - a\right\|^2 + \left\|e^{\frac{2\pi i}{3}} b - b\right\|^2 \\
&= \left\| - e^{\frac{4\pi i}{3}}\right\|^2 \cdot \left\| - a + ae^{\frac{-4\pi i}{3}}\right\|^2 + \left\|e^{\frac{2\pi i}{3}} b - b\right\|^2 \\
&= \left\|e^{\frac{2\pi i}{3}} a - a\right\|^2 + \left\|e^{\frac{2\pi i}{3}} b - b\right\|^2 \\
&= \left\|e^{\frac{2\pi i}{3}} - 1\right\|^2 \left(\left\|a\right\|^2 + \left\|b\right\|^2\right) \\
&= 3.
\end{aligned}$$

So, $\|\pi_2((1,2,3)) \cdot (a,b)^t - (a,b)^t\| = \sqrt{3}$ for any unit vector in $\mathbb{C}^2$.

Therefore, $\kappa(S_3, \Gamma, \pi_2) \geq \sqrt{3}$. One can compute that

$$\left\|\pi_2((1,2)) \cdot (1,0)^t - (1,0)^t\right\| = \sqrt{2}.$$

Hence

$$\max_{\gamma \in \Gamma} \left\|\pi_2(\gamma) \cdot (1,0)^t - (1,0)^t\right\| = \sqrt{3},$$

so $\kappa(S_3, \Gamma, \pi_2) \leq \sqrt{3}$. Therefore, $\kappa(S_3, \Gamma, \pi_2) = \sqrt{3}$. So,

$$\kappa(S_3, \Gamma) = \min\{2, \sqrt{3}\} = \sqrt{3}.$$

1.2 The Kazhdan Constant of $(\mathbb{Z}_p, \Gamma_p)$

From this point on we will only be concerned with calculating the Kazhdan constant for the pair $(\mathbb{Z}_p, \Gamma_p)$.

Definition 1.11. *Let p be a prime number. We define*

$$\Gamma_p = \{k^2 | k \in \mathbb{Z}_p^\times\}.$$

We denote the complement of this set in $\mathbb{Z}_p^\times$ as $\overline{\Gamma}_p$.

Example 1.2.1. Here we calculate the Kazhdan constant for the pair $(\mathbb{Z}_5, \Gamma_5)$. Note that $\Gamma_5 = \{1^2, 2^2, 3^2, 4^2\} = \{1, 4\}$.

From definition 1.3, we must minimize the value

$$\kappa(\mathbb{Z}_5, \Gamma_5, \rho_a) = \min_{\|v\|=1} \max_{k \in \Gamma_5} \|e^{\frac{2\pi i a k}{5}} v - v\| = \max_{k \in \Gamma_5} \|e^{\frac{2\pi i a k}{5}} - 1\|$$

over all the *unitary irreps* ρ_a of $\mathbb{Z}_5$. That is, we compute the value above for $a = 1, 2, 3, 4$ and take the minimum.

For $a = 1$ and $a = 2$, we get the following:

$$\kappa(\mathbb{Z}_5, \Gamma_5, \rho_1) = \min_{\|v\|=1} \max_{k \in \Gamma_5} \|e^{\frac{2\pi i k}{5}} v - v\| = \max_{k \in \Gamma_5} \|e^{\frac{2\pi i k}{5}} - 1\| = \|e^{\frac{2\pi i}{5}} - 1\| \approx 1.1756$$

$$\kappa(\mathbb{Z}_5, \Gamma_5, \rho_2) = \min_{\|v\|=1} \max_{k \in \Gamma_5} \|e^{\frac{4\pi i k}{5}} v - v\| = \max_{k \in \Gamma_5} \|e^{\frac{4\pi i k}{5}} - 1\| = \|e^{\frac{4\pi i}{5}} - 1\| \approx 1.902$$

And for $a = 3$ and $a = 4$, we get the following:

$$\kappa(\mathbb{Z}_5, \Gamma_5, \rho_3) = \min_{\|v\|=1} \max_{k \in \Gamma_5} \|e^{\frac{6\pi i k}{5}} v - v\| = \max_{k \in \Gamma_5} \|e^{\frac{6\pi i k}{5}} - 1\| = \|e^{\frac{6\pi i}{5}} - 1\| \approx 1.902$$

$$\kappa(\mathbb{Z}_5, \Gamma_5, \rho_4) = \min_{\|v\|=1} \max_{k \in \Gamma_5} \|e^{\frac{8\pi i k}{5}} v - v\| = \max_{k \in \Gamma_5} \|e^{\frac{8\pi i k}{5}} - 1\| = \|e^{\frac{8\pi i}{5}} - 1\| \approx 1.1756$$

And so, $\kappa(\mathbb{Z}_5, \Gamma_5, \rho) = \|e^{\frac{2\pi i}{5}} - 1\| \approx 1.1756$

Notice how $\kappa(\mathbb{Z}_5, \Gamma_5, \rho_a)$ is the same for $a = 1$ and $a = 4$, and that it is also the same for $a = 2$ and $a = 3$. In Lemma 1.13, we will show that in general, the value of $\kappa(\mathbb{Z}_p, \Gamma_p, \rho_a)$ is the same whenever $a \in \Gamma_p$, and that it is also the same whenever $a \in \overline{\Gamma}_p$. We will use this fact to simplify the calculation required for obtaining $\kappa(\mathbb{Z}_p, \Gamma_p)$.

Proposition 1.12. *Let p be an odd prime number. The set Γ_p is a multiplicative subgroup of $\mathbb{Z}_p^\times$. Moreover, Γ_p consists of exactly $\dfrac{p-1}{2}$ distinct elements.*

Proof. Let p be any odd prime number and consider the map

$$\phi : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$$

defined as $\phi(x) = x^2$ for all $x \in \mathbb{Z}_p^\times$.

Let $x, y \in \mathbb{Z}_p^\times$ be given. Then,

$$\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y).$$

Hence, ϕ is a group homomorphism. And since Γ_p is the image of ϕ, we have that Γ_p is a sugroup of $\mathbb{Z}_p^\times$. By the First Isomorphism Theorem, we get that

$$\Gamma_p = \phi(\mathbb{Z}_p^\times) \cong \mathbb{Z}_p^\times / \ker(\phi).$$

Since p is an odd prime, $\mathbb{Z}_p^\times$ has no zero divisors. So, the only solutions to $x^2 = 1$ are $x = \pm 1$. Thus,

$$\ker(\phi) = \{1, -1\}.$$

And because we are dealing with finite groups, we get that

$$\left|\Gamma_p\right| = \frac{\left|\mathbb{Z}_p^\times\right|}{\left|\ker(\phi)\right|} = \frac{p-1}{2}.$$ □

Lemma 1.13. *Let p be an odd prime number, and let $a \in \mathbb{Z}_p^\times$. Then,*

$$a\Gamma_p = \begin{cases} \Gamma_p, & \text{if } a \in \Gamma_p \\ \\ \overline{\Gamma}_p, & \text{if } a \in \overline{\Gamma}_p \end{cases}$$

Proof. Let $a \in \Gamma_p$. In Proposition 1.13, we showed that Γ_p is a multiplicative subgroup of $\mathbb{Z}_p^\times$. Hence, because $a\Gamma_p$ is a coset,

$$a\Gamma_p = \Gamma_p.$$

Now, suppose that $a \in \overline{\Gamma}_p$. Then,

$$|a\Gamma_p| = |\Gamma_p| = \frac{p-1}{2}.$$

Note that $a\Gamma_p$ and Γ_p are disjoint cosets both with $\frac{p-1}{2}$ elements. Hence,

$$a\Gamma_p = \overline{\Gamma}_p.$$

This completes the proof. □

Theorem 1.14. *Let p be an odd prime number. Then,*

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \min\left\{ \max_{k\in\Gamma_p} \|e^{\frac{2\pi ik}{p}} - 1\|, \max_{k\in\overline{\Gamma}_p} \|e^{\frac{2\pi ik}{p}} - 1\| \right\}.$$

Proof. Let p be a prime number. Then,

$$\begin{aligned}\kappa(\mathbb{Z}_p, \Gamma_p) &= \min_{a=1,2,\ldots,p-1} \left\{ \min_{\|z\|=1} \max_{k\in\Gamma_p} \|e^{\frac{2\pi iak}{p}} z - z\| \right\} \\ &= \min_{a=1,2,\ldots,p-1} \left\{ \max_{k\in\Gamma_p} \|e^{\frac{2\pi iak}{p}} - 1\| \right\}.\end{aligned}$$

The rest follows follows immediately from Lemma 1.13. □

Definition 1.15. *Let p be an odd prime number. An integer $a \not\equiv 0 \pmod{p}$ is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p defined as follows:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \text{ divides } a \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a nonquadratic residue modulo } p \end{cases}$$

Remark 1.16. *Let p be an odd prime number. From Definition 1.15, Γ_p is the set consisting of every quadratic residue modulo p of the group $\mathbb{Z}_p^\times$, and so $\overline{\Gamma}_p$ is the set consisting of all nonquadratic residues.*

Definition 1.17. *Let p be any given odd prime number, and let $\mathcal{P}_p$ denote the p^{th} roots of unity except for z=1. Define the function $\Phi : \mathcal{P}_p \to \{1, -1\}$ as:*

$$\Phi(\zeta_p^k) = \begin{cases} 1, & \text{if } \left(\frac{k}{p}\right) = 1 \\ -1, & \text{if } \left(\frac{k}{p}\right) = -1 \end{cases}$$

where $\zeta_p^k = e^{\frac{2\pi ik}{p}}$. If $\Phi(\zeta_p^k) = 1$ we call ζ_p^k a square and say that it has positive quadratic character, otherwise we call it a nonsquare and say that it has negative quadratic character.

We know that any prime number greater than 2 is congruent to either 1 or 3 modulo 4. In the case where $p \equiv 3 \pmod 4$, we can use Definition 1.17 to write an explicit formula for $\kappa(\mathbb{Z}_p, \Gamma_p)$. To do this, we will need Euler's criterion. We reformulate the theorem so that it fits to our needs, the proof is in [4].

Theorem 1.18. *Euler's criterion. If p is an odd prime and $a \in \mathbb{Z}_p^\times$, then*

$$a^{(p-1)/2} = \begin{cases} 1, \text{ if } a \in \Gamma_p \\ -1, \text{ if } a \in \overline{\Gamma}_p \end{cases}$$

Proposition 1.19. *If p is a prime number congruent to 3 modulo 4, in the p^{th} roots of unity, $\Phi(\zeta_p^n) \neq \Phi(\zeta_p^{-n})$ for all $n = 1, 2, 3, ..., p-1$. And if p is a prime number congruent to 1 modulo 4, $\Phi(\zeta_p^n) = \Phi(\zeta_p^{-n})$ for all $n = 1, 2, 3, ..., p-1$.*

Proof. Let p be a prime with $p \equiv 3 \pmod 4$ and suppose without loss of generality that $\Phi(\zeta_p^n) = \Phi(\zeta_p^{-n}) = 1$ for some $n < p$. Then by Definition 1.17, $\left(\frac{n}{p}\right) = \left(\frac{-n}{p}\right) = 1$.

From Euler's criterion,

$$\begin{aligned} 1 \equiv (n)^{(p-1)/2} \equiv (-n)^{(p-1)/2} &\equiv (-1)^{(p-1)/2}(n)^{(p-1)/2} \\ &\equiv (-1)^{2k+1}(n)^{(p-1)/2} \\ &\equiv -(n)^{(p-1)/2} \equiv -1 \pmod{p}, \text{ for some integer k.} \end{aligned}$$

This is impossible, and so we get the first part. Now, suppose that p is a prime number congruent to 1 modulo 4. By the Law of Quadratic Reciprocity, see Theorem A.2 in Appendix A, we have that $\left(\frac{-1}{p}\right) = 1$. Now, if $\Phi(\zeta_p^n) \neq \Phi(\zeta_p^{-n})$ for some $n < p$, then $\left(\frac{n}{p}\right) \neq \left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{n}{p}\right)$. Which is again impossible, and so we are done. □

Theorem 1.20. *Let p be a prime number congruent to 3 modulo 4. Then,*

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \|\zeta_p^{(p-1)/2} - 1\|.$$

Proof. Let p be any given prime with $p \equiv 3 \pmod 4$. Note that we can write the statement in Theorem 1.14 as follows:

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \min\left\{ \max_{k \in \Gamma_p} \left\|\zeta_p^k - 1\right\|, \max_{k \in \overline{\Gamma}_p} \left\|\zeta_p^k - 1\right\| \right\}.$$

It follows from Theorem 1.19 that $\Phi(\zeta_p^{(p-1)/2}) \neq \Phi(\zeta_p^{(p+1)/2})$. And because the first and second maximum correspond to the points $\zeta_p^{(p-1)/2}$ and $\zeta_p^{(p+1)/2}$, we determine the Kazhdan constant as the minimum of the two line segments $\left\|\zeta_p^{(p-1)/2} - 1\right\|$ and $\left\|\zeta_p^{(p+1)/2} - 1\right\|$. Note that the points are distributed symmetrically about the real axis, and so the line segments have equal length, see Figure 1.2. And so we get a formula for $\kappa(\mathbb{Z}_p, \Gamma_p)$. □

Corollary 1.21. *Considering only prime numbers congruent to 3 modulo 4,*

$$\lim_{p \to \infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 2.$$

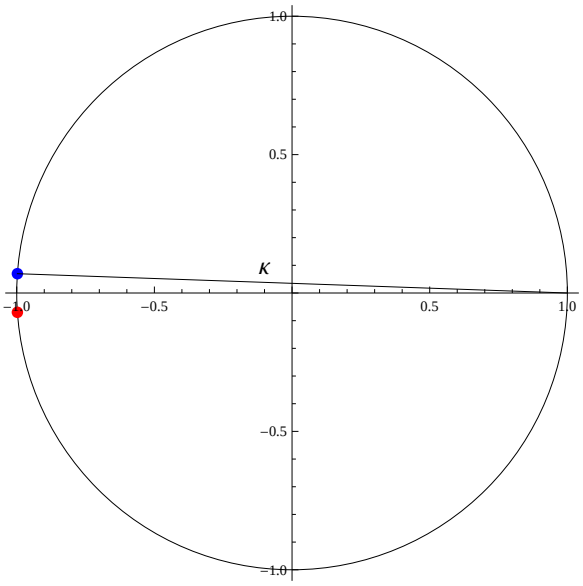

Figure 1.2: formula for $p \equiv 3 \pmod 4$.

Proof. By Theorem 1.20,

$$\begin{aligned}\lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) &= \lim_{p\to\infty} \|\zeta_p^{(p-1)/2} - 1\| \\ &= \lim_{p\to\infty} \|e^{2\pi i(p-1)/2p} - 1\| \\ &= \lim_{p\to\infty} \|e^{\pi i(1-1/p)} - 1\| \\ &= 2.\end{aligned}$$

□

Equipped with a formula, we now have the main result of this thesis nailed for the prime numbers congruent to 3 modulo 4. Whenever p is congruent to 1 modulo 4 however, we know from Proposition 1.19 that the two points $\zeta_p^{\frac{p-1}{2}}$ and $\zeta_p^{\frac{p+1}{2}}$ at maximal distance from 1 will have the same quadratic character, and so in this case, we won't be able to immediately determine the minimum like we did in the proof for Theorem 1.20. Using *Mathematica*, we developed a function that takes an odd prime number and displays $\kappa(\mathbb{Z}_p, \Gamma_p)$ as a line segment on the unit circle. After a few runs,

it became clear that the Kazhdan constant tends to 2 as p tends to infinity, which is all we really need anyway. And so, for the remainder of this thesis, every prime number is assumed to be congruent to 1 modulo 4.

Remark 1.22. *Let p be a given prime number, and let $\mathcal{U}_p$ be the set of all p^{th} roots of unity in the upper half plane. Consider the map*

$$P : \left\{1, 2, ..., \frac{p-1}{2}\right\} \to \mathcal{U}_p$$

defined as $P(n) = \zeta_p^{(p+1-2n)/2}$. Let n_0 be the smallest integer among the set $\{1, 2, 3, ..., \frac{p-1}{2}\}$ such that $\Phi(P(1)) \neq \Phi(P(n_0))$. We will often times refer to the point $P(n_0)$ as the first flip in quadratic character.

Using Proposition 1.19, when $p \equiv 1 \pmod 4$ we have that

$$\begin{aligned}\kappa(\mathbb{Z}_p, \Gamma_p) &= \min\left\{\max_{k\in\Gamma} \|\zeta_p^k - 1\|, \max_{k\in\overline{\Gamma}_p} \|\zeta_p^k - 1\|\right\} \\ &= \|P(n_0) - 1\|.\end{aligned}$$

Example 1.2.2. Using Mathematica, we calculate $(\mathbb{Z}_{17}, \Gamma_{17})$. The first flip is the point $P(2)$, so $\kappa(\mathbb{Z}_{17}, \Gamma_{17}) \approx 1.9237$. See Figure 1.2.

We will now state Legendre's version of Quadratic Reciprocity from the Law of Quadratic Reciprocity. Combined with the power of the Chinese Remainder Theorem, we can obtain a formula for $\kappa(\mathbb{Z}_p, \Gamma_p)$ that is valid when p is among a specified congruence class.

Theorem 1.23. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), \text{ if } p \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right), \text{ if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

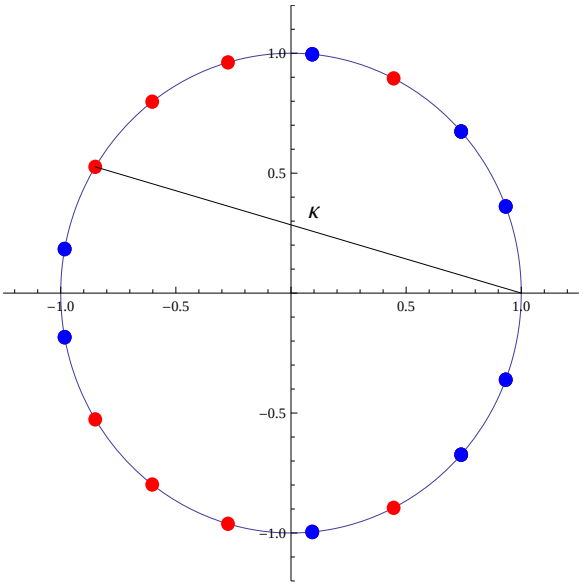

Figure 1.3: $\kappa(\mathbb{Z}_{17}, \Gamma_{17})$ displayed on the unit circle.

$p \equiv 1 \pmod 4$	$\|P(n_0) - 1\|$
5	$\|P(2) - 1\| \approx 1.1756$
13	$\|P(3) - 1\| \approx 1.6460$
17	$\|P(2) - 1\| \approx 1.9237$
29	$\|P(2) - 1\| \approx 1.9737$
37	$\|P(3) - 1\| \approx 1.9551$
41	$\|P(2) - 1\| \approx 1.9868$
53	$\|P(2) - 1\| \approx 1.9921$
57	$\|P(2) - 1\| \approx 1.9932$
61	$\|P(4) - 1\| \approx 1.9676$
73	$\|P(3) - 1\| \approx 1.9884$
89	$\|P(2) - 1\| \approx 1.9972$
97	$\|P(3) - 1\| \approx 1.9934$
101	$\|P(2) - 1\| \approx 1.9978$
109	$\|P(6) - 1\| \approx 1.9749$
113	$\|P(2) - 1\| \approx 1.9983$
137	$\|P(2) - 1\| \approx 1.9988$
149	$\|P(2) - 1\| \approx 1.9990$
157	$\|P(3) - 1\| \approx 1.9975$
173	$\|P(2) - 1\| \approx 1.9993$

Table 1.1: Table of values for the Kazhdan constant.

We now give formulas for $\kappa(\mathbb{Z}_p, \Gamma_p)$ for different classes of primes. In particular we give formulas when $p \equiv 17 \pmod{24}$ and $p \equiv 97 \pmod{120}$.

Example 1.2.3. We can write the formula for $\kappa(\mathbb{Z}_p, \Gamma_p)$ when $p \equiv 17 \pmod{24}$ as follows: Let us consider only those prime numbers for which we are guaranteed that $\Phi(P(1)) = 1$ and $\Phi(P(2)) = -1$. Consider the equation

$$\left(\frac{\frac{p-1}{2}}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right).$$

Since $p \equiv 1 \pmod{4}$, we know that $\left(\frac{-1}{p}\right) = 1$ by Theorem A.2. And so to guarantee that $\Phi(P(1)) = 1$, using Theorem A.2, we require that $p \equiv 1 \pmod{8}$ so that $\left(\frac{2}{p}\right) = 1$. At the same time we want $\Phi(P(2)) = -1$, that is, we want $\left(\frac{\frac{p-3}{2}}{p}\right) = -1$. So, we consider the equation

$$\left(\frac{\frac{p-3}{2}}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right).$$

Using Legendre's version of Quadratic Reciprocity, we get

$$\left(\frac{\frac{p-3}{2}}{p}\right) = \left(\frac{p}{3}\right).$$

Since the only quadratic nonresidue in $\mathbb{Z}_3$ is 2, we must also require that $p \equiv 2 \pmod{3}$. Now, by the Chinese Remainder Theorem, any prime number congruent to 17 modulo 24 will satisfy $p \equiv 1 \pmod{8}$ and $p \equiv 2 \pmod{3}$.

And so for any given prime number with $p \equiv 17 \pmod{24}$, the Kazhdan constant for $\kappa(\mathbb{Z}_p, \Gamma_p)$ is given by the formula

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \|P(2) - 1\| = \|e^{\pi i(1-\frac{3}{p})} - 1\|.$$

And, we can easily check that

$$\lim_{p\to\infty} \|e^{\pi i(1-\frac{3}{p})} - 1\| = 2.$$

We will now consider prime numbers for which $\Phi(P(1)) = \Phi(P(2)) = 1 \neq \Phi(P(3))$. Suppose $p \equiv 1 \pmod 8$ so that $\left(\frac{2}{p}\right) = 1$.

And so we now want $\left(\frac{\frac{p-3}{2}}{p}\right) = \left(\frac{p}{3}\right) = 1$ and $\left(\frac{\frac{p-5}{2}}{p}\right) = \left(\frac{p}{5}\right) = -1$. One solution is given by the following system of congruences:

$$p \equiv 1 \pmod 8$$

$$p \equiv 1 \pmod 3$$

$$p \equiv 3 \pmod 5$$

Using the Chinese Remainder Theorem, we get that the solution to the above congruences is $p \equiv 97 \pmod{120}$. So, if $p \equiv 97 \pmod{120}$, the Kazhdan constant for $(\mathbb{Z}_p, \Gamma_p)$ is given by the formula

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \|P(3) - 1\| = \|e^{\pi i(1-\frac{5}{p})} - 1\|.$$

And like the preceding formula, we get

$$\lim_{p\to\infty} \|e^{\pi i(1-\frac{5}{p})} - 1\| = 2.$$

This generating process can be repeated indefinitely, giving a never ending slew of formulas that are each valid for a particular class of primes. Unfortunately, this does not lead us to a general formula, yet it strongly suggests the existence of the limit. To conclude this chapter, we will prove that the Kazhdan constant tends to 2 when considering primes congruent to 5 modulo 8. For the first time, we will get the limit we want without the use of a formula, and in the second chapter, we will generalize to any prime congruent to 1 modulo 4.

Lemma 1.24. *Let α be a real number with $\frac{1}{2} < \alpha < 1$. There exists a positive number N_α such that for any $p > N_\alpha$, there exists an integer x*

$$\alpha\pi < \frac{2\pi x^2}{p} < \pi.$$

Proof. Consider the interval $\left[\sqrt{\frac{\alpha p}{2}}, \sqrt{\frac{p}{2}}\right]$. Then,

$$\begin{aligned}\lim_{p\to\infty}\left(\sqrt{\frac{p}{2}} - \sqrt{\frac{\alpha p}{2}}\right) &= \lim_{p\to\infty}\sqrt{\frac{p}{2}}\left(1-\sqrt{\alpha}\right)\\ &= \left(1-\sqrt{\alpha}\right)\lim_{p\to\infty}\sqrt{\frac{p}{2}}\\ &= \infty\end{aligned}$$

Hence, there is a number N_α such that

$$\left(\sqrt{\frac{p}{2}} - \sqrt{\frac{\alpha p}{2}}\right) > 1$$

whenever $p > N_\alpha$.

And now we have that for a sufficiently large prime number p, there exists an integer x such that

$$\sqrt{\frac{\alpha p}{2}} < x < \sqrt{\frac{p}{2}},$$

which is equivalent to

$$\alpha\pi < \frac{2\pi x^2}{p} < \pi.$$

□

Theorem 1.25. *Considering only prime numbers congruent to 5 modulo 8,*

$$\lim_{p\to\infty}\kappa(\mathbb{Z}_p, \Gamma_p) = 2.$$

Proof. Let $p \equiv 5 \pmod 8$.

By Theorem A.2, $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = 1$. Hence,

$$\left(\frac{\frac{p-1}{2}}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = 1.$$

So, we deduce that $\Phi(P(1)) = -1$. And since $p \equiv 1 \pmod 4$, by Proposition 1.19,

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \max_{k \in \Gamma_p} ||e^{\frac{2\pi ik}{p}} - 1||.$$

Let α be a real number with $\frac{1}{2} < \alpha < 1$. By Lemma 1.24, there exists a positive number N_α such that if $p > N_\alpha$, there is an integer x with $\alpha < \frac{2\pi x^2}{p} < \pi$. Hence, if p is a prime with $p > N_\alpha$, we have

$$\max_{k \in \Gamma_p} \|e^{\frac{2\pi ik}{p}} - 1\| > \|e^{i\alpha\pi} - 1\|.$$

Therefore, if p is a sufficiently large prime number congruent to 5 modulo 8,

$$2 > \kappa(\mathbb{Z}_p, \Gamma_p) > \|e^{i\alpha\pi} - 1\|.$$

Therefore, since the left side is independent of α, we let $\alpha \to 1$ and get

$$\lim_{p \to \infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 2.$$

□

Chapter 2

The End Behavior of $\kappa(\mathbb{Z}_p, \Gamma_p)$

2.1 Lower bounds for κ

In this second and final chapter, we will state and prove the main theorem of this thesis. Up to now, we have seen enough examples suggesting that the Kazhdan constant tends to 2 as p tends to infinity, and in Section 1.2 we gave a proof without the need of a formula. However, it was only valid when restricted to $p \equiv 5 \pmod 8$. Thus we have only been able to argue the limit by making a clever restriction. We now use a result obtained by Peralta to count the number of squares that show up in a consecutive run, giving us a way of determining the lower bound of $\kappa(\mathbb{Z}_p, \Gamma_p)$ valid for any odd prime p.

With all the results obtained in Chapter 1, we are now only left to deal with the primes congruent to 1 modulo 8, and so we can simplify our argument because $\Phi(P(1)) = 1$. So, for a given prime number p, the value of $\kappa(\mathbb{Z}_p, \Gamma_p)$ corresponds to the the smallest integer n_0 among the set $\{2, 3, ..., \frac{p-1}{2}\}$ such that $\Phi(P(n_0)) = -1$. We obtain a formula for the lower bound by limiting how large n_0 can be for a given prime number. That is, we count the maximum number of squares that can occur in a consecutive pattern. For instance if we know that there are up to 5 occurrences of triples, we can only have at most 7 squares in a row starting from P(1), so we can conclude that $\kappa(\mathbb{Z}_p, \Gamma_p) \geq \|P(8) - 1\|$. First, we will state a theorem from [1] that

allows us to determine the maximum number of pairs of quadratic residues.

Definition 2.1. *The collection* $\{r_1, r_2, r_3, ..., r_n\}$ *is called a complete residue system for* $\mathbb{Z}_n$ *if*

1. *For every* $x \in \mathbb{Z}$, $x \equiv \pmod{r_i}$ *for some* $i = 1, 2, 3, ..., n$.

2. $r_i \neq r_j$ *in* $\mathbb{Z}_n$ *for* $i \neq j$.

Lemma 2.2. *Suppose* c_j *is defined for all integers* j, *and* $c_j = c_k$ *whenever* $j = k \pmod{n}$. *Let* $r_1, r_2, ..., r_n$ *be any complete residue system modulo* n. *Then*

$$\sum_{j=0}^{n-1} c_j = c_{r_1} + c_{r_2} + \cdots + c_{r_n} = \sum_{r \pmod{n}} c_r.$$

Proof. Since both $\{r_1, r_2, r_3, ..., r_n\}$ and $\{0, 1, ..., n-1\}$ make up a complete residue system, each nonnegative integer $i < n$ is congruent to exactly one r_j, and so $c_i = c_{r_j}$. Hence, the sums $c_0 + c_1 + \cdots + c_{n-1}$ and $c_{r_1} + c_{r_2} + \cdots + c_{r_n}$ are just commutations of one another and thus equal. □

Lemma 2.3. *If* p *is a prime number, then*

$$\sum_{n=0}^{p-1} \left(\frac{(n-a)(n-b)}{p} \right) = \begin{cases} p-1, \text{ if } a \text{ is congruent to } b \text{ modulo } p \\ -1, \text{ otherwise} \end{cases}$$

Proof. By Lemma 2.2, we have that

$$\sum_{n=0}^{p-1} \left(\frac{(n-a)(n-b)}{p} \right) = \sum_{n \pmod{p}} \left(\frac{(n-a)(n-b)}{p} \right)$$

Because n assumes all values in a complete residue system modulo p, we deduce that $n + a$ does as well. Hence

$$\sum_{n \pmod{p}} \left(\frac{(n-a)(n-b)}{p} \right) = \sum_{n \pmod{p}} \left(\frac{n(n+a-b)}{p} \right).$$

Now, if $a \equiv b \pmod{p}$, we get that

$$\left(\frac{n(n+a-b)}{p}\right) = \left(\frac{n^2}{p}\right) = 1 \text{ for } n \not\equiv 0 \pmod{p},$$

thus,

$$\sum_{n=0}^{p-1}\left(\frac{(n-a)(n-b)}{p}\right) = p-1.$$

Now, suppose that $a \not\equiv b \pmod{p}$ and let $t = a - b$ so that $t \not\equiv 0 \pmod{p}$. By definition, $\left(\frac{n}{p}\right) = 0$ if and only if $n \equiv 0 \pmod{p}$. So,

$$\sum_{n \pmod{p}} \left(\frac{n(n+t)}{p}\right) = \sum_{\substack{n \pmod{p} \\ n \not\equiv 0 \pmod{p}}} \left(\frac{n(n+t)}{p}\right).$$

If we have that $n \not\equiv 0 \pmod{p}$, then there exists a number $\overline{n}$ such that $n\overline{n} \equiv 1 \pmod{p}$.

Now, since $\left(\frac{\overline{n}^2}{p}\right) = 1$, we get that

$$\begin{aligned}
\sum_{\substack{n \pmod{p} \\ n \not\equiv 0 \pmod{p}}} \left(\frac{n(n+t)}{p}\right) &= \sum_{\substack{n \pmod{p} \\ n \not\equiv 0 \pmod{p}}} \left(\frac{\overline{n}^2}{p}\right)\left(\frac{n(n+t)}{p}\right) \\
&= \sum_{\substack{n \pmod{p} \\ n \not\equiv 0 \pmod{p}}} \left(\frac{n\overline{n}(n\overline{n}+t\overline{n})}{p}\right) \\
&= \sum_{\substack{n \pmod{p} \\ n \not\equiv 0 \pmod{p}}} \left(\frac{1+t\overline{n}}{p}\right).
\end{aligned}$$

Since n assumes all values in a complete residue system modulo p, so does $\overline{n}$. And since $t \not\equiv 0 \pmod{p}$, we have that $t\overline{n}$ does too. So, by setting $m = t\overline{n}$, we get

$$\begin{aligned}
\sum_{\substack{n \pmod{p} \\ n \not\equiv 0 \pmod{p}}} \left(\frac{n(n+t)}{p}\right) &= \sum_{\substack{m \pmod{p} \\ m \not\equiv 0 \pmod{p}}} \left(\frac{\overline{n}^2}{p}\right)\left(\frac{1+m}{p}\right) \\
&= \sum_{m \pmod{p}} \left(\frac{1+m}{p}\right) - \left(\frac{1}{p}\right)
\end{aligned}$$

Note that $1+m$ will be -1 just as many times as it will be +1. Therefore,

$$\sum_{\substack{n \pmod p \\ n \not\equiv 0 \pmod p}} \left(\frac{n(n+t)}{p}\right) = -1.$$

This completes the proof. □

Theorem 2.4.

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

where $N(p)$ denotes the number of pairs of consecutive quadratic residues modulo a prime number p in [1,p-1].

Proof. Let $c_p(n)$ be defined as equaling 1 if both n and $n+1$ are quadratic residues modulo p, and 0 otherwise.

Then,

$$N(p) = \sum_{n=1}^{p-2} c_p(n).$$

It is easy to verify that

$$c_p(n) = \frac{1}{4}\left(1 + \left(\frac{n}{p}\right)\right)\left(1 + \left(\frac{n+1}{p}\right)\right).$$

Therefore,

$$\begin{aligned} N(p) &= \frac{1}{4}\sum_{n=1}^{p-2}\left(1 + \left(\frac{n}{p}\right)\right)\left(1 + \left(\frac{n+1}{p}\right)\right) \\ &= \frac{1}{4}\sum_{n=1}^{p-2}\left(1 + \left(\frac{n}{p}\right) + \left(\frac{n+1}{p}\right) + \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\right) \\ &= \frac{1}{4}\sum_{n=1}^{p-2} 1 + \frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n}{p}\right) + \frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n+1}{p}\right) + \frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right). \end{aligned}$$

Because there are as many quadratic residues as nonresidues modulo p, we get that

$$\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = 0,$$

and therefore,

$$\sum_{n=1}^{p-2}\left(\frac{n}{p}\right) = -\left(\frac{p-1}{p}\right) = -\left(\frac{-1}{p}\right) = -(-1)^{\frac{p-1}{2}},$$

and

$$\sum_{n=1}^{p-2}\left(\frac{n+1}{p}\right) = -\left(\frac{1}{p}\right) = -1.$$

So, by using Lemma 2.3 with $a = 0$ and $b - 1$, we get

$$\begin{aligned} N(p) &= \frac{1}{4}\left(p - 2 - (-1)^{\frac{p-1}{2}} - 1 - 1\right) \\ &= \frac{1}{4}\left(p - 4 - (-1)^{\frac{p-1}{2}}\right). \end{aligned}$$

□

Example 2.1.1. Using Theorem 2.4, we can obtain a formula for the lower bound of $\kappa(\mathbb{Z}_p, \Gamma_p)$ valid for whenever $p \equiv 1 \pmod 8$. First, from Theorem A.2, we immediately note that $\left(\frac{2}{p}\right) = 1$ whenever $p \equiv 1 \pmod 8$. This means that $\Phi(P(1)) = 1$, and so $\kappa(\mathbb{Z}_p, \Gamma_p) = \|P(n_0) - 1\|$ where n_0 is the smallest integer among the set $\{2, 3, ..., \frac{p-1}{2}\}$ such that $\Phi(P(n_0)) = -1$. From Theorem 2.4, since $p \equiv 1 \pmod 4$, the number of occurrences of a consecutive pair of squares in $\mathcal{U}_p$ is at most

$$j = \left\lfloor \frac{1}{8}(p - 4 - (-1)^{\frac{p-1}{2}}) \right\rfloor = \left\lfloor \frac{1}{8}(p-5) \right\rfloor.$$

This means that starting at the point $P(1)$ there can be at most $j + 1$ squares lined up in a consecutive pattern. And so it must be true that $j + 2$ is the greatest integer among the set $\{2, 3, ..., \frac{p-1}{2}\}$ such that

$$1 = \Phi(P(1)) = \Phi(P(2)) = \cdots = \Phi(P(j+1)) \neq \Phi(P(j+2)) = -1.$$

Thus for any given prime number congruent to 1 modulo 8, we have

$$\kappa(\mathbb{Z}_p, \Gamma_p) \geq \|P(j+2) - 1\| = \|e^{\pi i[1 - \frac{3}{p} - \frac{2j}{p}]} - 1\|.$$

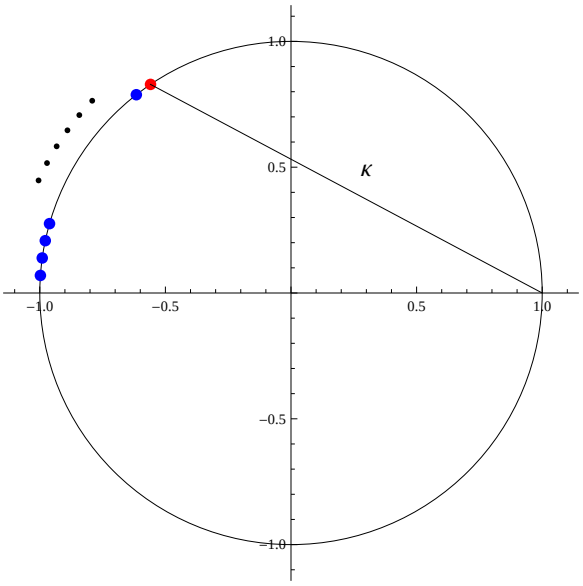

Figure 2.1: j+1 squares in a row.

In Figure 2.1, we see the maximum number of squares that can be lined up in consecutive order. Note that $\frac{j}{p} = \frac{1}{p}\lfloor\frac{p-5}{8}\rfloor \to \frac{1}{8}$ as p tends to infinity. And so in the limit, the lower bound is $\|e^{\frac{3\pi i}{4}} - 1\|$.

Theorem 2.4 is limited to counting occurrences of only consecutive pairs of quadratic residues. In order to prove our result, we must utilize a generalized theorem counting occurrences of arbitrary length.

Lemma 2.5. *Let $t \geq 2$. Then,*

$$\liminf_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) \geq \|e^{\pi i\left(1-\frac{1}{2^t}\right)} - 1\|$$

where the limit is over all prime numbers congruent to 1 modulo 8.

Proof. Let t be a fixed integer with $t \geq 2$, and let p be a prime number with $p \equiv 1 \pmod 8$ that is sufficiently larger than t, we say how large later in the proof. From Example 2.1.1, we know that $\kappa(\mathbb{Z}_p, \Gamma_p) = \|P(n_0)-1\|$, where n_0 is the smallest integer among the set $\{2, 3, ..., \frac{p-1}{2}\}$. Peralta proves in [3] that the number of occurrences of

an arbitrary pattern of length t of quadratic residues is in the range

$$\frac{p}{2^t} \pm t(3+\sqrt{p}).$$

Hence, because the squares are distributed symmetrically about the real axis as $p \equiv 1 \pmod 4$, the number of occurrences of a consecutive pattern of length t of squares in $\mathcal{U}_p$ is at most

$$j = \left\lfloor \frac{p}{2^{t+1}} + \frac{t(3+\sqrt{p})}{2} \right\rfloor.$$

Thus starting at $P(1)$, there can be at most $j+(t-1)$ squares lined up in a consecutive pattern. Hence, it must be true that $j+(t-1)+1$ is the greatest integer among the set $\{2, 3, ..., \frac{p-1}{2}\}$ such that

$$1 = \Phi(P(1)) = \Phi(P(2)) = \cdots = \Phi(P(j+1)) \neq \Phi(P(j+2)) = -1.$$

choose p large enough, so that the point $P(j+(t-1)+1)$ will land in the second quadrant. Thus for any given prime number p congruent to 1 modulo 8, we have

$$\kappa(\mathbb{Z}_p, \Gamma_p) \geq \|P(j+t) - 1\| = \|e^{\pi i[1+\frac{1}{p}-j\frac{2}{p}-\frac{2t}{p}]} - 1\|.$$

As a quick check, by setting $t = 2$, we get the lower bound in Example 2.1.1.

Therefore, we have that

$$\kappa(\mathbb{Z}_p, \Gamma_p) \geq \|e^{\pi i[1+\frac{1}{p}-j\frac{2}{p}-\frac{4}{p}]} - 1\| = \|e^{\pi i[1-\frac{3}{p}-\frac{2j}{p}]} - 1\|.$$

Note that $\frac{1}{p}\left\lfloor \frac{p}{2^{t+1}} + \frac{t(3+\sqrt{p})}{2} \right\rfloor \to \frac{1}{2^{t+1}}$ as p tends to infinity. And so in the limit, we get

$$\liminf_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) \geq \|e^{\pi i\left(1-\frac{1}{2^t}\right)} - 1\|.$$

□

Theorem 2.6.

$$\lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 2,$$

where the limit is over all odd prime numbers.

Proof. Recall that we have already dealt in this thesis with the odd primes $p \equiv 5 \pmod 8$ and odd primes $p \equiv 3 \pmod 4$. Now assume that $p \equiv 1 \pmod 8$.

Let $\epsilon > 0$, and let $t \geq 2$ satisfy

$$\|e^{\pi i\left(1-\frac{1}{2^t}\right)} - 1\| \geq 2 - \epsilon.$$

Then by Lemma 2.5,

$$2 \geq \lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) \geq \|e^{\pi i\left(1-\frac{1}{2^t}\right)} - 1\| \geq 2 - \epsilon.$$

Because epsilon was chosen arbitrarily, we get

$$\lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 2 \text{ as required.}$$

□

Now, we quickly explain how this result improves the best possible lower bound obtained in [2]. The following proposition is both stated and proven in [2].

Proposition 2.7. *Let G be a finite nontrivial group, and let $\Gamma \subset G$. Let $d = |\Gamma|$, let $\kappa = \kappa(G, \Gamma)$, and let λ_1 be the second-largest eigenvalue of the Cay(G, Γ). Then*

$$\kappa \geq \sqrt{\frac{2(d - \lambda_1)}{d}}.$$

Now, given a prime number p congruent to 1 modulo 4, the graph $\text{Cay}(\mathbb{Z}_p, \Gamma_p)$ is called the Paley graph of degree $d = \frac{p-1}{2}$. From [2], we note that the second largest eigenvalue of this graph is given by the formula

$$\lambda_1 = \frac{1}{2}\sqrt{p} - \frac{1}{2}.$$

If we substitute the values for d and λ_1 into the inequality above, we get

$$\kappa \geq \sqrt{\frac{2(\frac{p-1}{2} - (\frac{1}{2}\sqrt{p} - \frac{1}{2}))}{\frac{p-1}{2}}} = \sqrt{2\left(1 - \frac{\sqrt{p}-1}{p-1}\right)}.$$

This is a formula for the lower bound of κ of the Paley graph $\mathrm{Cay}(\mathbb{Z}_p, \Gamma_p)$, which is valid for any prime number congruent to 1 modulo 4. And if we take $p \to \infty$, we get $\sqrt{2}$. Thus, we have improved this bound.

Bibliography

[1] G. E. Andrews, *Number Theory,* Dover Publications, Inc., New York, 1994.

[2] M. Krebs and A. Shaheen, *Expander Families and Cayley Graphs,* Oxford University Press, Inc., New York, 2011.

[3] R. Peralta, *On the distribution of quadratic residues and nonresidues modulo a prime number,* Mathematics of Computation, **58**, **197**, (1992), 433–440.

[4] I. Niven, H.S. Zuckerman, H.L Montgomery, *An Introduction to Theory Of Numbers,* John Wiley & Sons, Inc., Canada, 1991.

Appendix A

Number Theory Stuff

Theorem A.1. *Chinese Remainder Theorem. Let $m_1, m_2, ..., m_r$ denote r positive integers that are pairwise relatively prime, and let $a_1, a_2, ..., a_r$ denote any r integers. Then the congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

have common solutions. If x_0 is one such solution, then an integer x satisfies the congruences if and only if x is of the form $x = x_0 + km$ for some integer k. Here $m = m_1 m_2 \cdots m_r$.

Theorem A.2. *The Law of Quadratic Reciprocity. Let p be an odd prime number. Then*

1. *$x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*
2. *$x^2 \equiv 2 \pmod{p}$ has a solution if and only if $p \equiv \pm 1 \pmod{8}$.*
3. *Quadratic Reciprocity. Let $q > 2$ be another prime distinct from p, and let $q^* = \pm q$ where its positive if $p \equiv 1 \pmod{4}$ and negative if $p \equiv -1 \pmod{4}$. Then $x^2 \equiv p \pmod{q}$ has a solution if and only if $x^2 \equiv q^* \pmod{p}$ is solvable.*

Appendix B

Algebra

Theorem B.1. *First Isomorphism Theorem.*

Let G and H be groups, and let $\phi : G \to H$ be a homomorphism. Then:

1. *The kernel of ϕ is a normal subgroup of G.*
2. *The image of ϕ is a subgroup of H.*
3. *The image of ϕ is isomorphic to the quotient group $G/ker\phi$*