Distributions of Quadratic Residues

PROMYS Counselor Seminar

Joshua Im

August 5, 2025

1 Review

These notes are written that the readers are familiar with quadratic residues. Recall the following definitions and properties of quadratic residues.

Definition 1.1: Quadratic Residue

A **quadratic residue** modulo a prime p is a number $a \in \{1, \ldots, p-1\}$ such that there exists $x \in \{1, \ldots, p-1\}$ such that

$$x^2 \equiv a \pmod{p}.$$

If a is not a quadratic residue, we call them quadratic nonresidues. We abbreviate quadratic residues to QR, and quadratic nonresidues to QNR.

Theorem 1.1

- QR $\times$ QR $=$ QR.
- QR $\times$ QNR $=$ QNR.
- QNR $\times$ QNR $=$ QR.

Theorem 1.2

-1 is a QR mod p if and only if $p \equiv 1 \pmod 4$.

Theorem 1.3

There are $\frac{p-1}{2}$ QRs mod p.

Definition 1.2: Legendre Symbol

Let p be a fixed prime. The Legendre symbol mod p is a function $\chi : \mathbb{Z} \to \{-1, 0, 1\}$, defined by

$$\chi'(n) = \left(\frac{n}{p}\right) = \begin{cases} 1 & n \text{ is QR mod } p \\ -1 & n \text{ is QNR mod } p \\ 0 & p \mid n \end{cases}.$$

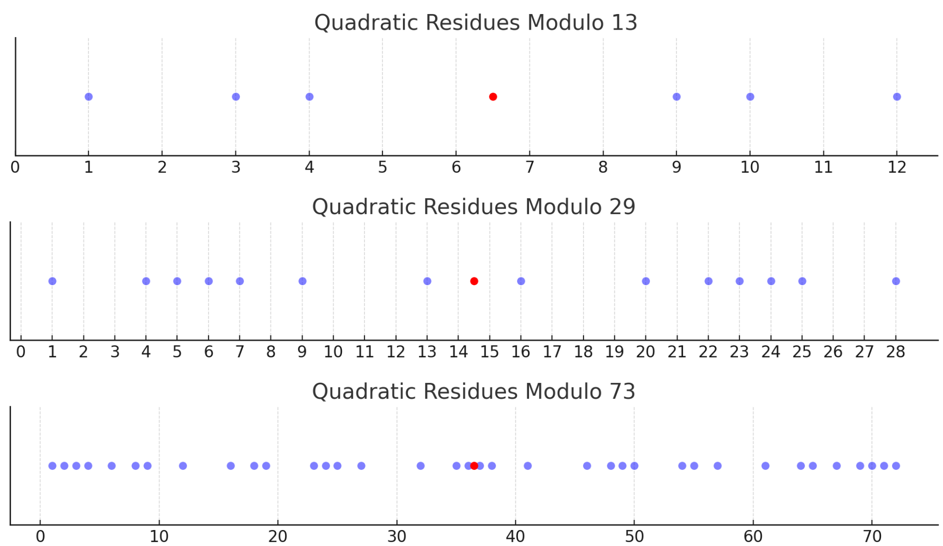
The Legendre symbol is completely multiplicative. That is,

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

for all m, $n \in \mathbb{Z}$.

2 Motivation

Let p be a 1 mod 4 prime. If $a \in \{1, 2, \ldots, p-1\}$ is a QR mod p, then $-a \equiv p - a \pmod{p}$ is also a QR mod p. Thus if $p \equiv 1 \pmod{4}$, then the QRs are distributed symmetrically with respect to $p/2$.

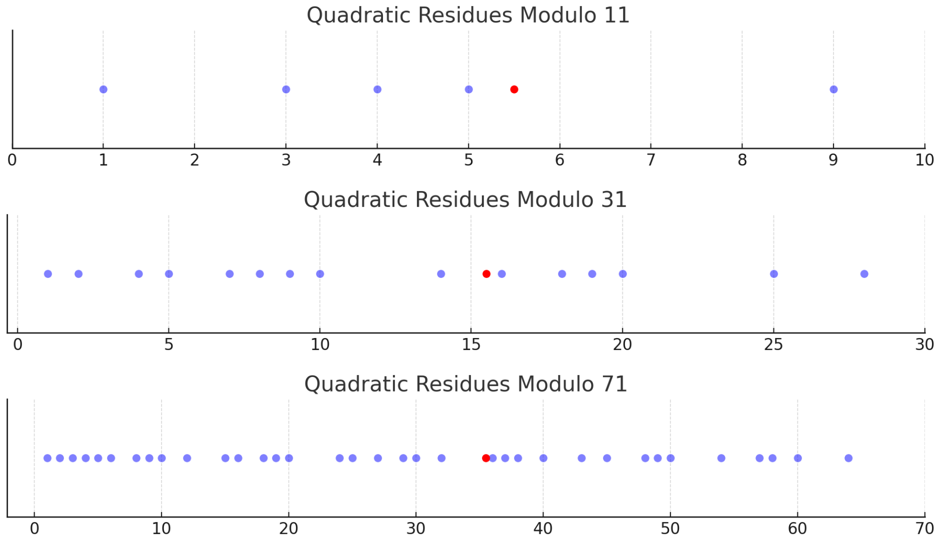


The QRs mod p for $p = 13$, 29, and 71 are displayed on the image above. QRs are plotted in blue dots, while the red dot is $p/2$. 13, 29, and 71 are all 1 mod 4 primes, and it is easy to see that the blue dots are distributed symmetrically with respect to the red dot.

For a fixed prime p, define E_p to be the number of QRs on $(0, p/2)$ minus the number of QRs on $(p/2, p)$. Then $E_p = 0$ if $p \equiv 1 \pmod 4$.

What if $p \equiv 3 \pmod 4$? Since there are $\frac{p-1}{2}$ QRs mod p, if we let $p = 4k + 3$, there are $2k+1$ QRs mod p, which is odd. Thus there cannot be the same amount of QRs in intervals $(0, p/2)$ and $(p/2, p)$ the number of QRs in each interval should have different parity.

We do some numericals.



We see the distribution of QRs when $p = 11$, 31, and 71, which are all 3 mod 4 primes. The blue dots are QRs, and the red dot is $p/2$. By intuition, it seems like there are more QRs on the interval $(0, p/2)$ than on the interval $(p/2, p)$. Is this a coincidence?

3 The Theorem

Theorem 3.1: Quadratic Excess Theorem

Let p be a 3 mod 4 prime. Then more quadratic residues mod p lie on the interval $(0, p/2)$ than in the interval $(p/2, p)$.

So $E_p > 0$ if $p \equiv 3 \pmod 4$.

To prove the theorem, we need some lemmas.

Lemma : Weighed Gauss Sum

If $p \equiv 3 \pmod 4$ is a prime, then $\displaystyle\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \exp\left(\frac{2\pi ikn}{p}\right) = \left(\frac{n}{p}\right) i\sqrt{p}$.

Proof. The proof is omitted. □

There is one more lemma that we need, which we will introduce in the next section.

4 Dirichlet L-functions

Definition 4.1: Dirichlet Character

Let $m \in \mathbb{Z}^+$. A **Dirichlet character** modulo m is a function $\chi : \mathbb{Z} \to \mathbb{C}$ such that

- $\chi(a+m) = \chi(a)$ for all $a \in \mathbb{Z}$
- $\chi(ab) = \chi(a)\chi(b)$ for all a, $b \in \mathbb{Z}$ (so χ is completely multiplicative)
- $\chi(1) = 1$
- $\chi(a) = 0$ if $\gcd(a, m) \neq 1$.

There are several Dirichlet characters modulo a given positive integer m.

Definition 4.2: Dirichlet L-function

Let χ be a Dirichlet character mod m. The **Dirichlet L-functions** are defined as

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

The sum runs over all positive integers. We state one lemma that is used for the proof of the theorem.

Lemma : Dirichlet

Suppose χ is a Dirichlet character mod m that only takes real values. Then $L(1, \chi) \in \mathbb{R}$ and $L(1, \chi) > 0$.

Proof. The proof is omitted. □

5 The Proof

This section proves the quadratic excess theorem.

Let $G_p(n)$ be the weighted Gauss sum above, so

$$G_p(n) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \exp\left(\frac{2\pi i k n}{p}\right).$$

Then

$$G_p(n) = \left(\frac{n}{p}\right) i\sqrt{p} \qquad \text{and} \qquad G_p(1) = \left(\frac{1}{p}\right) i\sqrt{p} = i\sqrt{p}$$

since $1 = 1^2$ is always a QR. Thus we have $\left(\frac{n}{p}\right) = \frac{G_p(n)}{G_p(1)} = \frac{G_p(n)}{i\sqrt{p}}$.

Let p be a 3 mod 4 prime. Note that the Legendre symbol $\chi'(n) = \left(\frac{n}{p}\right)$ is also a Dirichlet character. Then the L-function for the Legendre symbol is

$$L(s, \chi') = \sum_{n=1}^{\infty} \frac{\chi'(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n^s}.$$

Lemma

Let χ be a Dirichlet character. Then we have

$$\sum_{n \text{ odd}} \frac{\chi(n)}{n^s} = \left(1 - \frac{\chi(2)}{2^s}\right) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Proof. We have

$$\begin{aligned}
\left(1 - \frac{\chi(2)}{2^s}\right) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} - \sum_{n=1}^{\infty} \frac{\chi(2)\chi(n)}{2^s \cdot n^s} \\
&= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} - \sum_{n=1}^{\infty} \frac{\chi(2n)}{(2n)^s} \\
&= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} - \sum_{n \text{ even}} \frac{\chi(n)}{n^s} \\
&= \sum_{n \text{ odd}} \frac{\chi(n)}{n^s}.
\end{aligned}$$

□

So $\sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n^s} = \left(1 - \frac{\left(\frac{2}{p}\right)}{2^s}\right) \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n^s}$. If we let $s = 1$, then

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

Since $\left(\frac{2}{p}\right)$ is either -1 or 1, $1 - \frac{\left(\frac{2}{p}\right)}{2} > 0$. By Dirichlet, the Legendre symbol is a real Dirichlet character, so $L(s, \chi') > 0$. This gives

$$\sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n} > 0.$$

Now recall that $\left(\frac{n}{p}\right) = \frac{G_p(n)}{i\sqrt{p}} = \frac{1}{i\sqrt{p}} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \exp\left(\frac{2\pi i k n}{p}\right)$. We then have

$$\begin{aligned}\sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n} &= \frac{1}{i\sqrt{p}} \sum_{n \text{ odd}} \frac{1}{n} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \exp\left(\frac{2\pi i k n}{p}\right) \\ &= \frac{1}{i\sqrt{p}} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \sum_{n \text{ odd}} \frac{1}{n} \exp\left(\frac{2\pi i k n}{p}\right).\end{aligned}$$

For convenience, let $\omega = \exp\left(\frac{2\pi i}{p}\right)$ be the pth root of unity. Then the expression above is equal to $\frac{1}{i\sqrt{p}} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \sum_{n \text{ odd}} \frac{1}{n} \omega^{kn}$.

We use the Taylor series formula of $\tanh^{-1} z$. Since

$$\tanh^{-1} z = z + \frac{z^3}{3} + \frac{z^5}{5} + \cdots = \sum_{n \text{ odd}} \frac{z^n}{n},$$

we get

$$\sum_{n \text{ odd}} \frac{1}{n} \exp\left(\frac{2\pi i k n}{p}\right) = \tanh^{-1}(\omega^k).$$

We now evaluate this manually.

Lemma

If $\omega = \exp\left(\frac{2\pi i}{p}\right)$ is the pth root of unity, then

$$\tanh^{-1}(\omega^k) = \begin{cases} \frac{\pi i}{4} + c_k & k \in (0, p/2) \\ -\frac{\pi i}{4} + c_k & k \in (p/2, p) \end{cases}$$

where $c_k \in \mathbb{R}$. Furthermore, $c_k = c_{p-k}$ for all $k \in \{1, 2, \ldots, p-1\}$.

Proof. We use the identity

$$\tanh^{-1} z = \frac{1}{2} \operatorname{Log}\left(\frac{1+z}{1-z}\right)$$

where $\operatorname{Log} z = \ln|z| + i \arg z$ is the principal complex logarithm. The identity gives

$$\begin{aligned} \tanh^{-1}(\omega^k) &= \frac{1}{2} \operatorname{Log}\left(\frac{1+\omega^k}{1-\omega^k}\right) \\ &= \frac{1}{2} \operatorname{Log}\left(\frac{\omega^{-k/2}+\omega^{k/2}}{\omega^{-k/2}-\omega^{k/2}}\right) \\ &= \frac{1}{2} \operatorname{Log}\left(\frac{\exp(-\pi ik/p)+\exp(\pi ik/p)}{\exp(-\pi ik/p)-\exp(\pi ik/p)}\right) \\ &= \frac{1}{2} \operatorname{Log}\left(-i\cot\left(-\frac{\pi k}{p}\right)\right) \\ &= \frac{1}{2}\left(\ln\left|\cot\left(-\frac{\pi k}{p}\right)\right| + i\arg\left(-i\cot\left(-\frac{\pi k}{p}\right)\right)\right). \end{aligned}$$

If $k \in (0, p/2)$, then $-\frac{\pi k}{p} \in (-\pi/2, 0)$, so $\cot\left(-\frac{\pi k}{p}\right) < 0$. Thus $-i\cot\left(-\frac{\pi k}{p}\right)$ is pure imaginary and its imaginary part is positive, so $\arg\left(-i\cot\left(-\frac{\pi k}{p}\right)\right) = \frac{\pi}{2}$. If $k \in (p/2, p)$, then $-\frac{\pi k}{p} \in (-\pi/2, -\pi)$, so $\cot\left(-\frac{\pi k}{p}\right) > 0$. Thus $-i\cot\left(-\frac{\pi k}{p}\right)$ is pure imaginary and its imaginary part is negative, so $\arg\left(-i\cot\left(-\frac{\pi k}{p}\right)\right) = -\frac{\pi}{2}$. Letting $\frac{1}{2}\ln\left|\cot\left(-\frac{\pi k}{p}\right)\right| = c_k$ gives

$$\tanh^{-1}(\omega^k) = \begin{cases} \frac{\pi i}{4} + c_k & k \in (0, p/2) \\ -\frac{\pi i}{4} + c_k & k \in (p/2, p). \end{cases}$$

Now, we have

$$\begin{aligned} c_{p-k} &= \frac{1}{2}\ln\left|\cot\left(-\frac{\pi(p-k)}{p}\right)\right| \\ &= \frac{1}{2}\ln\left|\cot\left(-\pi+\frac{\pi k}{p}\right)\right| \\ &= \frac{1}{2}\ln\left|-\cot\left(-\frac{\pi k}{p}\right)\right| \\ &= \frac{1}{2}\ln\left|\cot\left(-\frac{\pi k}{p}\right)\right| \\ &= c_k, \end{aligned}$$

using the identity $\cot(\pi - z) = -\cot z$. □

With the lemma, we have

$$\begin{aligned} \sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n} &= \frac{1}{i\sqrt{p}}\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\tanh^{-1}(\omega^k) \\ &= \frac{1}{i\sqrt{p}}\left(\sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)\left(\frac{\pi i}{4}+c_k\right)+\sum_{k\in(p/2,p)}\left(\frac{k}{p}\right)\left(-\frac{\pi i}{4}+c_k\right)\right) \\ &= \frac{\pi i}{i\sqrt{p}}\left(\sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)-\sum_{k\in(p/2,p)}\left(\frac{k}{p}\right)\right) \\ &\quad+\frac{1}{i\sqrt{p}}\left(\sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)c_k+\sum_{k\in(p/2,p)}\left(\frac{k}{p}\right)c_k\right). \end{aligned}$$

But

$$\begin{aligned} \sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)c_k+\sum_{k\in(p/2,p)}\left(\frac{k}{p}\right)c_k &= \sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)c_k+\sum_{k\in(0,p/2)}\left(\frac{p-k}{p}\right)c_k \\ &= \sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)c_k-\sum_{k\in(0,p/2)}\left(\frac{k}{p}\right)c_k \\ &= 0, \end{aligned}$$

so the second expression is zero. Therefore

$$\sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n} = \frac{\pi i}{i\sqrt{p}} \left(\sum_{k \in (0,p/2)} \left(\frac{k}{p}\right) - \sum_{k \in (p/2,p)} \left(\frac{k}{p}\right) \right)$$

$$= \frac{\pi}{\sqrt{p}} \left(\sum_{k \in (0,p/2)} \left(\frac{k}{p}\right) - \sum_{k \in (p/2,p)} \left(\frac{k}{p}\right) \right),$$

which is real. Since we know that $\sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n} > 0$, we should have

$$\sum_{k \in (0,p/2)} \left(\frac{k}{p}\right) - \sum_{k \in (p/2,p)} \left(\frac{k}{p}\right) > 0.$$

Since there are $\frac{p-1}{2}$ QRs mod p, there also should be $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ QNRs mod p, i.e. for any prime p, the number QRs and QNRs are equal. Thus

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \sum_{k \in (0,p/2)} \left(\frac{k}{p}\right) + \sum_{k \in (p/2,p)} \left(\frac{k}{p}\right) = 0.$$

This gives $\sum_{k \in (0,p/2)} \left(\frac{k}{p}\right) > 0$, which suggests that there are more QRs than QNRs on the interval $(0, p/2)$. There are $\frac{p-1}{2}$ numbers on the interval $(0, p/2)$, so there are more than $\frac{p-1}{4}$ QRs lying on $(0, p/2)$, and there should be less than $\frac{p-1}{4}$ QRs lying on $(p/2, p)$. Therefore, there are more QRs lying on $(0, p/2)$ than $(p/2, p)$, as desired. □