Quadratic Excess Theorem

Quadratic Excess Theorem

Joshua Im

Mentor: William Taylor

April 24, 2025

Quadratic Residues

Let p denote a prime number throughout the presentation.

Definition: Quadratic Residue

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

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

Quadratic Residues

Let p denote a prime number throughout the presentation.

Definition: 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

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

$3^2 \equiv 2 \pmod{7}$, so 2 is a quadratic residue mod 7.

Quadratic Nonresidues

$$\begin{aligned}
1^2 &= 1 \equiv 1 \pmod 7 \\
2^2 &= 4 \equiv 4 \pmod 7 \\
3^2 &= 9 \equiv 2 \pmod 7 \\
4^2 &= 16 \equiv 2 \pmod 7 \\
5^2 &= 25 \equiv 4 \pmod 7 \\
6^2 &= 36 \equiv 1 \pmod 7
\end{aligned}$$

- 1, 2, 4 are quadratic residues mod 7.
- 3, 5, 6 are not quadratic residues, or **quadratic nonresidues** mod 7.

Use QR for quadratic residues, QNR for quadratic nonresidues.

Basic Properties (1)

Theorem

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

Basic Properties (1)

Theorem

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

This seems like

- $1 \times 1 = 1$
- $1 \times (-1) = -1$
- $(-1) \times (-1) = 1!$

Legendre Symbol

Definition: 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

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

Legendre Symbol

Definition: 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

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

Then 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 $m, n \in \mathbb{Z}$.

Basic Properties

Theorem

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

Basic Properties

Theorem

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

Theorem

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

Basic Properties

Theorem

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

Theorem

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

So if $p \equiv 1 \pmod 4$ and a is a QR, then $-a \equiv p - a$ is also a QR.

Therefore if $p \equiv 1 \pmod 4$ the QRs mod p are symmetric to $p/2$.

Basic Properties

Theorem

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

Theorem

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

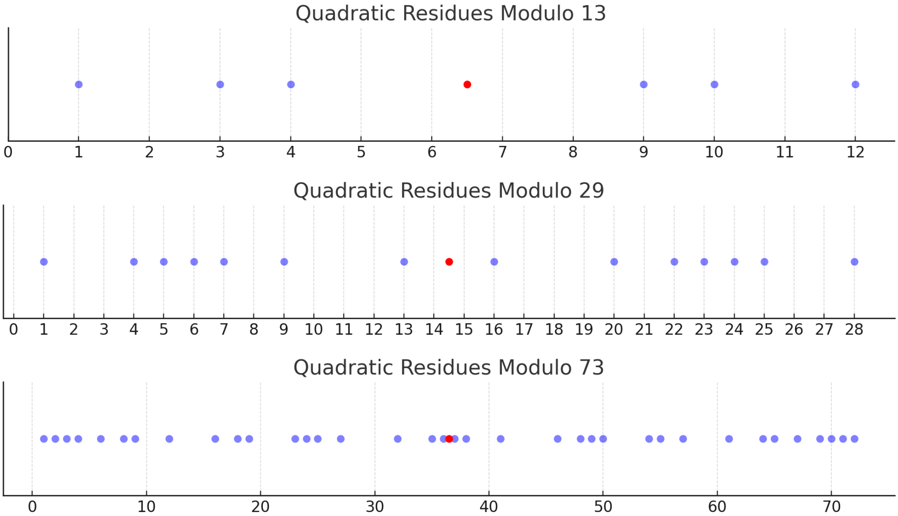
So if $p \equiv 1 \pmod 4$ and a is a QR, then $-a \equiv p - a$ is also a QR.

Therefore if $p \equiv 1 \pmod 4$ the QRs mod p are symmetric to $p/2$.

Theorem

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

Distribution of Quadratic Residues – 1 mod 4 primes



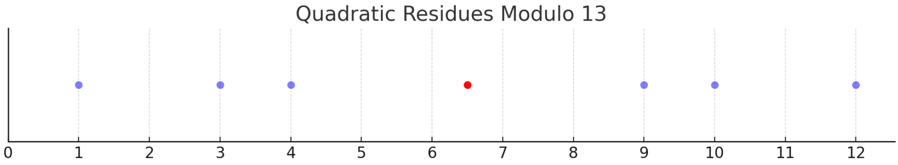
Distribution of Quadratic Residues – 1 mod 4 primes

- QRs symmetric to $p/2$
- Equal numbers of QRs lying on $(0, p/2)$ and $(p/2, p)$.

Let

$$E_p = (\# \text{ of QRs lying on } (0, p/2)) - (\# \text{ of QRs lying on } (p/2, p))$$

Then $E_p = 0$ if $p \equiv 1 \pmod 4$.



Distribution of Quadratic Residues - 3 mod 4 primes

Is $E_p = 0$ if $p \equiv 3 \pmod 4$?

Distribution of Quadratic Residues - 3 mod 4 primes

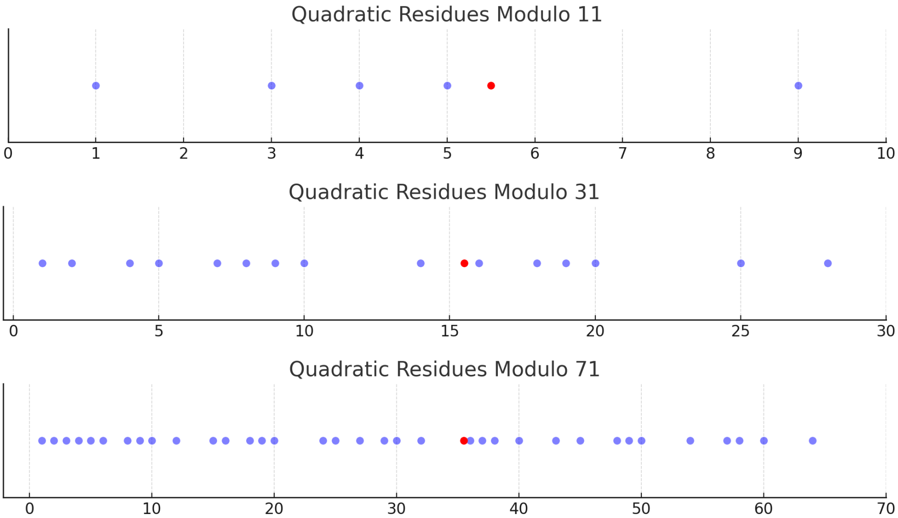
Is $E_p = 0$ if $p \equiv 3 \pmod 4$?

No!

There are $\frac{p-1}{2}$ (odd) QRs mod p, there can't be same amount of QRs on $(0, p/2)$ and $(p/2, p)$.

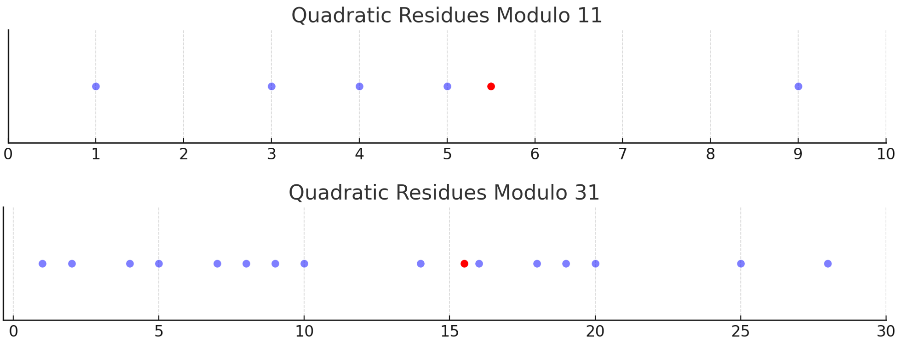
So $E_p \neq 0$ for $p \equiv 3 \pmod 4$ primes.

Distribution of Quadratic Residue - 3 mod 4 primes



Distribution of Quadratic Residues – 3 mod 4 primes

$E_{11} = 3$, $E_{31} = 3$, $E_{71} = 7$.



Seems like $E_p > 0$ for $p \equiv 3 \pmod 4$?

Quadratic Excess Theorem - Statement

Theorem: 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 $E_p > 0$ when $p \equiv 3 \pmod 4$.

Lemma - Gauss Sum

Theorem: Weighed Gauss Sum

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

Lemma - Gauss Sum

Theorem: Weighed Gauss Sum

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

Define $G(n) = \sum_{k=1}^{p-1} \left(\frac{p}{k}\right) \exp\left(\frac{2\pi ikn}{p}\right)$. Then

$$G(n) = \left(\frac{n}{p}\right) i\sqrt{p}$$

$$G(1) = \left(\frac{1}{p}\right) i\sqrt{p} = i\sqrt{p}$$

$$\frac{G(n)}{G(1)} = \left(\frac{n}{p}\right)$$

Quadratic Excess Theorem - Proof Outline

Let $p \equiv 3 \pmod 4$ a prime. Define $L(s)$ by

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

- Sum runs over all positive integers

Quadratic Excess Theorem – Proof Outline

Let $p \equiv 3 \pmod 4$ a prime. Define $L(s)$ by

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

- Sum runs over all positive integers
- Can rearrange to let the sum run over all odds

$$L(1) = \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n} = \alpha \sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n}$$

for some positive constant α.

Quadratic Excess Theorem – Proof Outline

$$L(1) = \alpha \sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n}$$

We now note that $L(1) > 0$ (Dirichlet). So

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

Quadratic Excess Theorem – Proof Outline

Recall that $\left(\frac{n}{p}\right) = \frac{G(n)}{G(1)} = \frac{1}{i\sqrt{p}} \sum_{k=1}^{p-1} \left(\frac{p}{k}\right) \exp\left(\frac{2\pi ikn}{p}\right)$. Then

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

$$= \frac{i\pi/4}{i\sqrt{p}} \left(\sum_{k\in(0,p/2)} \left(\frac{k}{p}\right) - \sum_{k\in(p/2,p)} \left(\frac{k}{p}\right) \right)$$

Quadratic Excess Theorem – Proof Outline

Thus

$$\sum_{n \text{ odd}} \frac{\left(\frac{n}{p}\right)}{n} = \frac{i\pi/4}{i\sqrt{p}} \left(\sum_{k\in(0,p/2)} \left(\frac{k}{p}\right) - \sum_{k\in(p/2,p)} \left(\frac{k}{p}\right) \right) > 0,$$

which gives

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

Quadratic Excess Theorem – Proof Outline

Since there are $\frac{p-1}{2}$ QRs and $\frac{p-1}{2}$ QNRs

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

Therefore

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

gives

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

as desired.

Further Results about Quadratic Residues

- No elementary proof of the Quadratic Excess Theorem is known.

Further Results about Quadratic Residues

- No elementary proof of the Quadratic Excess Theorem is known.

Define

$$S_p = (\text{sum of QRs lying on } (0,p)) - (\text{sum of QNRs lying on } (0,p)).$$

Theorem

S_p is an odd multiple of p.

- $S_{11} = -11 = (-1) \cdot 11$
- $S_{13} = 0$
- $S_{29} = 0$
- $S_{31} = -93 = (-3) \cdot 31$

Thank you for listening!