Quadratic Excess Theorem

Joshua Im

Texas A&M University

April 5, 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

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 $p \equiv 1 \pmod 4$.

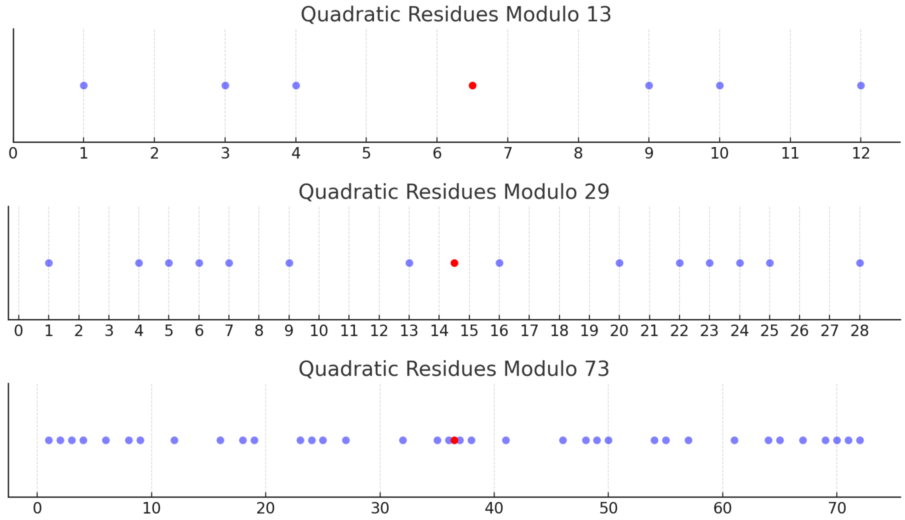
So if $p \equiv 1 \pmod 4$ and a is a QR, then $-a \equiv p - a$ is also a QR.

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



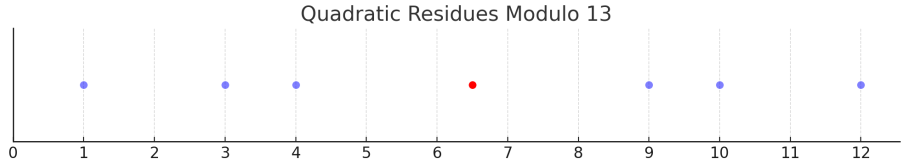
Distribution of Quadratic Residues – 1 mod 4 primes

- 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

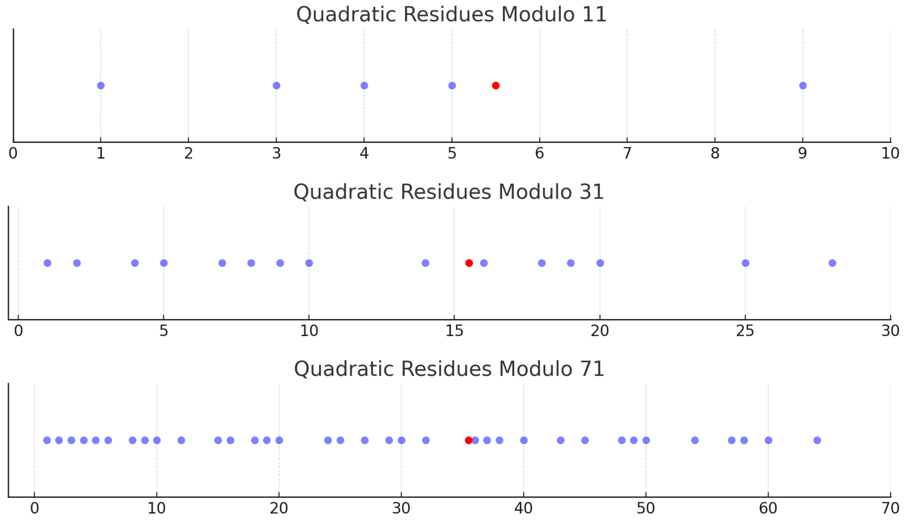
Is $E_p = 0$ if $p \equiv 3 \pmod 4$?

No!

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

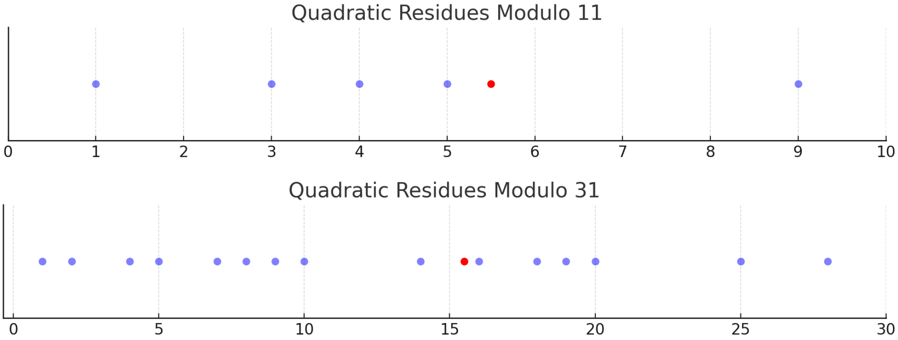
So $E_p \neq 0$ for $p \equiv 3 \pmod 4$ primes.

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 $p \equiv 3 \pmod 4$.

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 $p \equiv 3 \pmod 4$.

Proof is hard!

A Weaker Result - Statement

From *Online Monmouth Math Competition* for high school students.

Theorem: OMMC 2023 Final Round P8

Let p be a prime. If the mean of the nonzero quadratic residues mod p is less than $p/2$, then the median of the nonzero quadratic residues mod p is less than $p/2$.

A Weaker Result - Statement

From *Online Monmouth Math Competition* for high school students.

Theorem: OMMC 2023 Final Round P8

Let p be a prime. If the mean of the nonzero quadratic residues mod p is less than $p/2$, then the median of the nonzero quadratic residues mod p is less than $p/2$.

- The mean of QRs $< \frac{p}{2}$ implies $p \equiv 3 \pmod 4$
- The proof of the converse is true, but hard to prove
- Proof does not use $p \equiv 3 \pmod 4$

Proof idea by *i3435* from *Art of Problem Solving*.

A Weaker Result - Proof

Let

- n: the number of QRs mod p lying on $(0, p/2)$
- S: the sum of all QRs mod p

Then $\frac{p-1}{2} - n$ QRs mod p lie in $(p/2, p)$, and

$$S < \frac{p-1}{2} \cdot \frac{p}{2} = \frac{p(p-1)}{4}.$$

Divide cases to if 2 is a QR modulo p or not.

A Weaker Result - Proof

Case 1: 2 is a QR mod p.

- Multiply all QRs by 2 and take modulo p
- Gives a bijection from the QRs to QRs.
- Take modulo p, i.e. subtract p for some of these.

A Weaker Result – Proof

Case 1: 2 is a QR mod p.

- Multiply all QRs by 2 and take modulo p
- Gives a bijection from the QRs to QRs.
- Take modulo p, i.e. subtract p for some of these.

$\frac{p-1}{2} - n$ QRs on $(p/2, p)$, so

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

or $S = \dfrac{p(p-1)}{2} - pn$. Therefore

$$S < \frac{p(p-1)}{4} \Rightarrow n > \frac{p-1}{4}$$

More than half of the QRs mod p lie on $(0, p/2)$.

A Weaker Result - Proof

Case 2: 2 is a QNR mod p.

- Multiply all QRs by 2 and take modulo p
- Gives a bijection from the QRs to QNRs.
- Take modulo p, i.e. subtract p for some of these.

A Weaker Result - Proof

Case 2: 2 is a QNR mod p.

- Multiply all QRs by 2 and take modulo p
- Gives a bijection from the QRs to QNRs.
- Take modulo p, i.e. subtract p for some of these.

$\frac{p-1}{2} - n$ QRs on $(p/2, p)$, so

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

or $S = \frac{p(p-1-n)}{3}$. Therefore

$$S < \frac{p(p-1)}{4} \Rightarrow n > \frac{p-1}{4}$$

More than half of the QRs mod p lie on $(0, p/2)$.

Thank you for listening!