Introduction to Quadratic Reciprocity

Clyde Kertzer

December 13, 2021

Modular Arithmetic

Modular Arithmetic

$$7/5 = 1, \text{ remainder } 2 \longrightarrow 7 \equiv 2 \bmod 5$$

Modular Arithmetic

$$7/5 = 1, \text{ remainder } 2 \longrightarrow 7 \equiv 2 \bmod 5$$
$$9/4 = 2, \text{ remainder } 1 \longrightarrow 9 \equiv 1 \bmod 4$$

Modular Arithmetic

$$7/5 = 1, \text{ remainder } 2 \longrightarrow 7 \equiv 2 \bmod 5$$
$$9/4 = 2, \text{ remainder } 1 \longrightarrow 9 \equiv 1 \bmod 4$$
$$13/4 = 3, \text{ remainder } 1 \longrightarrow 13 \equiv 1 \bmod 4$$

Modular Arithmetic

$$7/5 = 1, \text{ remainder } 2 \longrightarrow 7 \equiv 2 \bmod 5$$
$$9/4 = 2, \text{ remainder } 1 \longrightarrow 9 \equiv 1 \bmod 4$$
$$13/4 = 3, \text{ remainder } 1 \longrightarrow 13 \equiv 1 \bmod 4$$

Leftover number $\longrightarrow$ **residue**

Basic Functions in Modular Arithmetic

Basic Functions in Modular Arithmetic

Addition:

Basic Functions in Modular Arithmetic

Addition:

$$\begin{aligned}(8+6) \bmod 5 &\equiv 8 \bmod 5 + 6 \bmod 5\\ &\equiv 3 \bmod 5 + 1 \bmod 5\\ &\equiv 4 \bmod 5\\ 14 \bmod 5 &\equiv 4 \bmod 5\end{aligned}$$

Multiplication:

$$\begin{aligned}(8*6) \bmod 5 &\equiv 8 \bmod 5 * 6 \bmod 5\\ &\equiv 3 \bmod 5 * 1 \bmod 5\\ &\equiv 3 \bmod 5\\ 48 \bmod 5 &\equiv 3 \bmod 5\end{aligned}$$

Division:

Basic Functions in Modular Arithmetic

Division:

$$
\begin{aligned}
(8/2) \bmod 6 &\equiv (8 \bmod 6)/(2 \bmod 6) \\
&\equiv (2 \bmod 6)/(2 \bmod 6) \\
&\equiv 1 \bmod 6 \\
4 \bmod 6 &\equiv 4 \bmod 6
\end{aligned}
$$

Basic Functions in Modular Arithmetic

Division:

$$\begin{aligned}(8/2) \bmod 6 &\equiv (8 \bmod 6)/(2 \bmod 6)\\ &\equiv (2 \bmod 6)/(2 \bmod 6)\\ &\equiv 1 \bmod 6\\ 4 \bmod 6 &\equiv 4 \bmod 6\end{aligned}$$

$$\frac{a}{b} \bmod m \neq \frac{a \bmod m}{b \bmod m}$$

Basic Functions in Modular Arithmetic

$$12 \equiv 2 \bmod 5$$

Basic Functions in Modular Arithmetic

$$12 \equiv 2 \bmod 5$$

$$6 \equiv 1 \bmod 5$$

Residue Systems

Residue Systems

$$\text{mod}4 \longrightarrow \{0, 1, 2, 3\} \quad \mathbb{Z}_4$$

Residue Systems

$$\text{mod}4 \longrightarrow \{0, 1, 2, 3\} \quad \mathbb{Z}_4$$
$$\text{mod}12 \longrightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}\mathbb{Z}_{12}$$

Residue Systems

$\text{mod} 4 \longrightarrow \{0, 1, 2, 3\} \quad \mathbb{Z}_4$
$\text{mod} 12 \longrightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \mathbb{Z}_{12}$
Reduce a residue system: remove residues that are coprime.

Residue Systems

$\text{mod} 4 \longrightarrow \{0, 1, 2, 3\} \quad \mathbb{Z}_4$

$\text{mod} 12 \longrightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \mathbb{Z}_{12}$

Reduce a residue system: remove residues that are coprime.

$\text{mod} 4 \longrightarrow \{1, 3\}$

Residue Systems

$\text{mod} 4 \longrightarrow \{0, 1, 2, 3\} \quad \mathbb{Z}_4$

$\text{mod} 12 \longrightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}\mathbb{Z}_{12}$

Reduce a residue system: remove residues that are coprime.

$\text{mod} 4 \longrightarrow \{1, 3\}$

$\text{mod} 12 \longrightarrow \{1, 5, 7, 11\}$

Residue Systems

$\text{mod}4 \longrightarrow \{0, 1, 2, 3\} \quad \mathbb{Z}_4$

$\text{mod}12 \longrightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}\mathbb{Z}_{12}$

Reduce a residue system: remove residues that are coprime.

$\text{mod}4 \longrightarrow \{1, 3\}$

$\text{mod}12 \longrightarrow \{1, 5, 7, 11\}$

$\text{mod}11 \longrightarrow \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Quadratic Residues

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.

Quadratic residues mod 5:

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow a$ is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.
Quadratic residues mod 5:
Residue system: $\{0, 1, 2, 3, 4\}$ (0 is trivial)

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.
Quadratic residues mod 5:
Residue system: $\{0, 1, 2, 3, 4\}$ (0 is trivial)
$x^2 \equiv 1 \bmod 5 \longrightarrow 1$

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.
Quadratic residues mod 5:
Residue system: $\{0, 1, 2, 3, 4\}$ (0 is trivial)
$x^2 \equiv 1 \bmod 5 \longrightarrow 1$
$x^2 \equiv 2 \bmod 5 \longrightarrow$ nothing, nonresidue

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.

Quadratic residues mod 5:

Residue system: $\{0, 1, 2, 3, 4\}$ (0 is trivial)

$x^2 \equiv 1 \bmod 5 \longrightarrow 1$

$x^2 \equiv 2 \bmod 5 \longrightarrow$ nothing, nonresidue

$x^2 \equiv 3 \bmod 5 \longrightarrow$ nothing, nonresidue

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.
Quadratic residues mod 5:
Residue system: $\{0, 1, 2, 3, 4\}$ (0 is trivial)
$x^2 \equiv 1 \bmod 5 \longrightarrow 1$
$x^2 \equiv 2 \bmod 5 \longrightarrow$ nothing, nonresidue
$x^2 \equiv 3 \bmod 5 \longrightarrow$ nothing, nonresidue
$x^2 \equiv 4 \bmod 5 \longrightarrow 2$

Quadratic Residues

Quadratic Residue

For a and m coprime, if $x^2 \equiv a \bmod m$ has a solution $\longrightarrow$ a is a **quadratic residue**

If it has no solution $\longrightarrow$ nonresidue.
Quadratic residues mod 5:
Residue system: $\{0, 1, 2, 3, 4\}$ (0 is trivial)
$x^2 \equiv 1 \bmod 5 \longrightarrow 1$
$x^2 \equiv 2 \bmod 5 \longrightarrow$ nothing, nonresidue
$x^2 \equiv 3 \bmod 5 \longrightarrow$ nothing, nonresidue
$x^2 \equiv 4 \bmod 5 \longrightarrow 2$
Conclusion: quadratic residues are 1 and 4, quadratic nonresidues are 2 and 3.

Wilson's Theorem

Wilson's Theorem

Wilson's Theorem

If p is a prime then

$$(p-1)! \equiv -1 \bmod p.$$

Proof of Wilson's Theorem

Proof of Wilson's Theorem

Suppose that $a^2 \equiv 1 \bmod p$, then $p \mid a^2 - 1$ and $p \mid (a-1)(a+1)$.

Proof of Wilson's Theorem

Suppose that $a^2 \equiv 1 \bmod p$, then $p \mid a^2 - 1$ and $p \mid (a-1)(a+1)$.
Then $p \mid a - 1$ or $p \mid a + 1$.

Proof of Wilson's Theorem

Suppose that $a^2 \equiv 1 \mod p$, then $p \mid a^2 - 1$ and $p \mid (a-1)(a+1)$.
Then $p \mid a - 1$ or $p \mid a + 1$.
Follows $a \equiv 1 \mod p$ or $a \equiv -1 \mod p$
Consider $(p-1)! \equiv 1 \cdot (2 \cdot 3 \cdots (p-2))(p-1) \mod p$.

Proof of Wilson's Theorem

Suppose that $a^2 \equiv 1 \bmod p$, then $p \mid a^2 - 1$ and $p \mid (a-1)(a+1)$.
Then $p \mid a - 1$ or $p \mid a + 1$.
Follows $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$
Consider $(p-1)! \equiv 1 \cdot (2 \cdot 3 \cdots (p-2))(p-1) \bmod p$.
Recall that every number has a unique inverse (mod p). Then

Proof of Wilson's Theorem

Suppose that $a^2 \equiv 1 \bmod p$, then $p \mid a^2 - 1$ and $p \mid (a-1)(a+1)$.
Then $p \mid a - 1$ or $p \mid a + 1$.
Follows $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$
Consider $(p-1)! \equiv 1 \cdot (2 \cdot 3 \cdots (p-2))(p-1) \bmod p$.
Recall that every number has a unique inverse (mod p). Then

$$\begin{aligned}(p-1)! &\equiv 1 \cdot 2^{-1} 3^{-1} \cdots (p-2) \cdot (p-2)^{-1} (p-1) \bmod p \\ &\equiv (p-1) \bmod p \\ &\equiv -1 \bmod p\end{aligned}$$

Legendre Symbol

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

$= 1$, if a is a quadratic residue

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

$= 1$, if a is a quadratic residue

$= -1$, if a is a quadratic nonresidue

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

$= 1$, if a is a quadratic residue
$= -1$, if a is a quadratic nonresidue
$= 0$, if $p \mid a$

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

$= 1$, if a is a quadratic residue
$= -1$, if a is a quadratic nonresidue
$= 0$, if $p \mid a$
Find $\left(\frac{2}{5}\right)$:

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

$= 1$, if a is a quadratic residue
$= -1$, if a is a quadratic nonresidue
$= 0$, if $p \mid a$
Find $\left(\frac{2}{5}\right)$:
Is there a solution to $x^2 \equiv 2 \bmod 5$?

Legendre Symbol

Legendre Symbol

$$\left(\frac{a}{p}\right)$$

$= 1$, if a is a quadratic residue

$= -1$, if a is a quadratic nonresidue

$= 0$, if $p \mid a$

Find $\left(\frac{2}{5}\right)$:

Is there a solution to $x^2 \equiv 2 \bmod 5$?

No $\longrightarrow \left(\frac{2}{5}\right) = -1$

Fermat's Little Theorem

Fermat's Little Theorem

Fermat's Little Theorem

If a and p are coprime, then

$$a^{p-1} \equiv a \bmod p.$$

Proof of Fermat's Little Theorem

Proof of Fermat's Little Theorem

Consider the smallest residues of $\{a, 2a, 3a, \ldots, pa\}$

Proof of Fermat's Little Theorem

Consider the smallest residues of $\{a, 2a, 3a, \ldots, pa\}$
We want to show all elements in this list are incongruent mod p.

Proof of Fermat's Little Theorem

Consider the smallest residues of $\{a, 2a, 3a, \ldots, pa\}$
We want to show all elements in this list are incongruent mod p.
Show that their residues are $\{1, 2, 3, \ldots, p-1\}$

Proof of Fermat's Little Theorem

Consider the smallest residues of $\{a, 2a, 3a, \ldots, pa\}$
We want to show all elements in this list are incongruent mod p.
Show that their residues are $\{1, 2, 3, \ldots, p-1\}$
Take ka and la, where k is some integer such that $1 \leq k \neq l \leq p$.

Proof of Fermat's Little Theorem

Consider the smallest residues of $\{a, 2a, 3a, \ldots, pa\}$
We want to show all elements in this list are incongruent mod p.
Show that their residues are $\{1, 2, 3, \ldots, p-1\}$
Take ka and la, where k is some integer such that $1 \leq k \neq l \leq p$.
Suppose $ka \equiv la \bmod p$, then $p \mid (k-l)a$, then $p \mid (k-1)$ or $p \mid a$. We know p cannot divide by a, they are coprime.

Proof of Fermat's Little Theorem

Consider the smallest residues of $\{a, 2a, 3a, \ldots, pa\}$
We want to show all elements in this list are incongruent mod p.
Show that their residues are $\{1, 2, 3, \ldots, p-1\}$
Take ka and la, where k is some integer such that $1 \leq k \neq l \leq p$.
Suppose $ka \equiv la \bmod p$, then $p \mid (k-l)a$, then $p \mid (k-1)$ or $p \mid a$. We know p cannot divide by a, they are coprime.
We also know $p \mid (k-l)a$ is not possible because of $1 \leq k \neq l \leq p$.

Proof of Fermat's Little Theorem

Proof of Fermat's Little Theorem

Now we take the product of each list.

Proof of Fermat's Little Theorem

Now we take the product of each list.

$$
\begin{aligned}
a \cdot 2a \cdots (p-1)a &\equiv (p-1)! \bmod p \\
a^{p-1}(p-1)! &\equiv (p-1)! \bmod p \\
a^{p-1} &\equiv 1 \bmod p
\end{aligned}
$$

□

Euler's Criterion

Euler's Criterion

Euler's Criterion

$$\left(\frac{a}{p}\right) = a^{\left(\frac{p-1}{2}\right)} \bmod p$$

Proof of Euler's Criterion

Proof of Euler's Criterion

Case 1: $\left(\frac{a}{p}\right) = 1$

Proof of Euler's Criterion

Case 1: $\left(\frac{a}{p}\right) = 1$

We have some x_0 such that $x_0^2 \equiv a \bmod p$

Proof of Euler's Criterion

Case 1: $\left(\frac{a}{p}\right) = 1$

We have some x_0 such that $x_0^2 \equiv a \bmod p$

$a^{\left(\frac{p-1}{2}\right)} = (x_0^2)^{\left(\frac{p-1}{2}\right)} = x_0^{p-1} \equiv 1 \bmod p$ (By Fermat's Little Theorem).

Proof of Euler's Criterion

Case 1: $\left(\frac{a}{p}\right) = 1$

We have some x_0 such that $x_0^2 \equiv a \bmod p$

$a^{\left(\frac{p-1}{2}\right)} = (x_0^2)^{\left(\frac{p-1}{2}\right)} = x_0^{p-1} \equiv 1 \bmod p$ (By Fermat's Little Theorem).

Case 2: $\left(\frac{a}{p}\right) = -1$

Proof of Euler's Criterion

Case 1: $\left(\frac{a}{p}\right) = 1$

We have some x_0 such that $x_0^2 \equiv a \bmod p$

$a^{\left(\frac{p-1}{2}\right)} = (x_0^2)^{\left(\frac{p-1}{2}\right)} = x_0^{p-1} \equiv 1 \bmod p$ (By Fermat's Little Theorem).

Case 2: $\left(\frac{a}{p}\right) = -1$

For each $1 \leq k \leq p-1$ we have a solution to the solution to $kx \equiv a \bmod p$, $x \equiv k^{-1}a \bmod p$. We also know that $x \not\equiv k \bmod p$ because if it were, k would be a quadratic residue.

Proof of Euler's Criterion

Note: $1, 2, \ldots, p-1$ can be split in to factor pairs of a.

Proof of Euler's Criterion

Note: $1, 2, \ldots, p-1$ can be split in to factor pairs of a.
Now we see $a^{\frac{p-1}{2}} = (1)(2)\cdots(p-1) = (p-1)! \equiv -1 \bmod p$
(This is by Wilson's Theorem). $\square$

Gauss' Lemma

Gauss' Lemma

Gauss' Lemma

For any odd prime p, with coprime a. Consider the integers

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

and their smallest residues mod p. If n denotes the number of residues that are greater than $\frac{p}{2}$, then

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

Example

Example

Let $p = 13$ and $a = 5$

Example

Let $p = 13$ and $a = 5$
$\frac{p-1}{2} = \frac{13-1}{2} = \frac{12}{2} = 6$, $\frac{p}{2} = \frac{13}{2}$

Example

Let $p = 13$ and $a = 5$
$\frac{p-1}{2} = \frac{13-1}{2} = \frac{12}{2} = 6$, $\frac{p}{2} = \frac{13}{2}$

$$5 * 1 = 5 \equiv 5 \text{ mod } 13$$
$$5 * 2 = 10 \equiv 10 \text{ mod } 13$$
$$5 * 3 = 15 \equiv 2 \text{ mod } 13$$
$$5 * 4 = 20 \equiv 7 \text{ mod } 13$$
$$5 * 5 = 25 \equiv 12 \text{ mod } 13$$
$$5 * 6 = 30 \equiv 4 \text{ mod } 13$$

Example

Example

Our list is: 2,4,5,7,10,12 $\longrightarrow$ 3 are greater than $\frac{13}{2}$

Example

Our list is: 2,4,5,7,10,12 $\longrightarrow$ 3 are greater than $\frac{13}{2}$

$$\left(\frac{5}{13}\right) = (-1)^3 = -1$$

Example

Our list is: 2,4,5,7,10,12 $\longrightarrow$ 3 are greater than $\frac{13}{2}$

$$\left(\frac{5}{13}\right) = (-1)^3 = -1$$

Conclusion: 5 is a quadratic nonresidue mod 13.

Proof of Gauss' Lemma

Proof of Gauss' Lemma

Proof

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

$$\textbf{(1)} \quad a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

$$\textbf{(1)} \quad a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

Let $r_1, r_2, \ldots, r_n$ be the residues $\pmod{p}$ from **(1)** that are $> \frac{p}{2}$

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

$$\textbf{(1)} \quad a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

Let $r_1, r_2, \ldots, r_n$ be the residues $\pmod{p}$ from **(1)** that are $> \frac{p}{2}$
Let $s_1, s_2, \ldots, s_m$ be the residues $\pmod{p}$ from **(1)** that are $< \frac{p}{2}$

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

$$\textbf{(1)} \quad a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

Let $r_1, r_2, \ldots, r_n$ be the residues $\pmod p$ from **(1)** that are $> \frac{p}{2}$
Let $s_1, s_2, \ldots, s_m$ be the residues $\pmod p$ from **(1)** that are $< \frac{p}{2}$
Now consider $p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m$

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

$$\textbf{(1)} \quad a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

Let $r_1, r_2, \ldots, r_n$ be the residues $\pmod p$ from **(1)** that are $> \frac{p}{2}$
Let $s_1, s_2, \ldots, s_m$ be the residues $\pmod p$ from **(1)** that are $< \frac{p}{2}$
Now consider $p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m$
We want to show this list is incongruent $\pmod p$

Proof of Gauss' Lemma

Proof

Consider the smallest residues of

$$\textbf{(1)} \quad a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

Let $r_1, r_2, \ldots, r_n$ be the residues $\pmod p$ from **(1)** that are $> \frac{p}{2}$
Let $s_1, s_2, \ldots, s_m$ be the residues $\pmod p$ from **(1)** that are $< \frac{p}{2}$
Now consider $p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m$
We want to show this list is incongruent $\pmod p$
First half of list is different, second half is different.

Proof of Gauss' Lemma

Proof of Gauss' Lemma

Suppose for the sake of contradiction

Proof of Gauss' Lemma

Suppose for the sake of contradiction

$$p - r_i \equiv s_j \bmod p$$
$$-r_i \equiv s_j \bmod p$$

Notice both r_i and s_j are multiples of a

Proof of Gauss' Lemma

Suppose for the sake of contradiction

$$p - r_i \equiv s_j \bmod p$$
$$-r_i \equiv s_j \bmod p$$

Notice both r_i and s_j are multiples of a

$$-k_i a \equiv k_j a \bmod p$$
$$-k_i \equiv k_j \bmod p$$

These k values are taken from $a, 2a, 3a, \ldots, \frac{p-1}{2}a$, which is not possible, because all are positive.

Proof of Gauss' Lemma

Proof of Gauss' Lemma

We have shown:

$$\{p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m\} = \{1, 2, \ldots, \frac{p-1}{2}\}$$

Proof of Gauss' Lemma

We have shown:

$$\{p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m\} = \{1, 2, \ldots, \frac{p-1}{2}\}$$

We want to find the product of both sides.

Proof of Gauss' Lemma

Proof of Gauss' Lemma

$$(p - r_1)\cdots(p - r_n)s_1\cdots s_m \equiv 1\cdot 2\cdots \frac{p-1}{2} \mod p$$

$$(-r_1)\cdots(-r_n)s_1\cdots s_m \equiv \left(\frac{p-1}{2}\right)! \mod p$$

$$(-1)^n r_1\cdots r_n s_1\cdots s_m \equiv \left(\frac{p-1}{2}\right)! \mod p$$

$$(-1)^n a\cdot 2a\cdot 3a\cdots \frac{p-1}{2}a \equiv \left(\frac{p-1}{2}\right)! \mod p$$

$$(-1)^n a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \mod p$$

$$(-1)^n a^{\frac{p-1}{2}} \equiv 1 \mod p$$

$$a^{\frac{p-1}{2}} \equiv (-1)^n \mod p$$

Quadratic Reciprocity

Quadratic Reciprocity

Quadratic Reciprocity

Let p and q be distinct odd primes. Then

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

Equals 1 if p or $q \equiv 1 \bmod 4$

Quadratic Reciprocity

Quadratic Reciprocity

Let p and q be distinct odd primes. Then

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

Equals 1 if p or $q \equiv 1 \bmod 4$
Equals -1 if $p \equiv q \equiv 3 \bmod 4$