Quadratic Residues

Nicholas Wendt

November 18, 2025

1 Intro

Some integer a is a quadratic residue mod n if there exists some integer x such that:

$$x^2 \equiv a \ (mod \ n)$$

If no x exists, then a is called a quadratic nonresidue mod n.

2 Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

2.1 Euler's Criterion

For an odd prime p and integer a not divisible by p,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p}, & \text{if } a \text{ is a quadratic residue,} \\ -1 \pmod{p}, & \text{if } a \text{ is a nonresidue.} \end{cases}$$

2.2 Monday Rule

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$

3 Quadratic Reciprocity

Law of Quadratic Reciprocity: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$

where p and q are distinct odd primes.

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