Primitive Roots and Quadratic Residues

Temi Owoeye

March 24, 2020

If $x^2 \equiv$ a (mod p) has a solution, it is a **quadratic residue** (mod p)

If $x^2 \equiv$ a (mod p) no solution, it is a **quadratic non-residue** (mod p)

Example

Quadratic redsidues (mod 11) $\longrightarrow 1, 3, 4, 5, 9$

Quadratic nonresidues (mod 11) $\longrightarrow 2, 6, 7, 8, 10$

Is 10 **a quadratic residue (mod 43) ?**

We use ***Legendre Symbol*** *to figure that out!*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if p|a} \\ 1 & \text{if } x^2 = \text{a (mod p) exists} \\ -1 & \text{if } x^2 = \text{a (mod p) has no solution} \end{cases}$$

Example

$\left(\frac{3}{11}\right) = 1$

$\left(\frac{2}{11}\right) = -1$

$\left(\frac{15}{11}\right) = 1$

$\left(\frac{33}{11}\right) = 0$

Rules for the Legendre Symbol

1. For the Legendre Symbol, the bottom number must be prime!
2. If a $\equiv$ b (mod p), then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \longrightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Example

$$\left(\frac{6}{11}\right) = \left(\frac{2*3}{11}\right)$$

$$= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)(1) = -1$$

3. **Quadratic Reciprocity** $\longrightarrow$ If p and q are both odd primes, then

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if} \equiv 3 \pmod 4 \text{ and q} \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right) & \text{otherwise at least 1 of them is} \equiv 1 \pmod 4 \end{cases}$$

4. If

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

Using the rules above **Is** 10 **a quadratic residue (mod 43) ?**

$$\left(\frac{10}{43}\right) = \left(\frac{2*5}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{5}{43}\right)$$

focus on* $\left(\frac{2}{43}\right)$ *first

Use rule 4 $\longrightarrow$ 43(mod 8) $\equiv$ 3(mod 8) = -1

$$\left(\frac{10}{43}\right) = -1 * \left(\frac{5}{43}\right)$$

Use rule 3, quadratic reciprocity, on $\left(\frac{5}{43}\right)$

$$\left(\frac{5}{43}\right) = \left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{10}{43}\right) = -1 * -1 = 1$$

Therefore, 10 is a quadratic residue of 43.

Example Is 1001 a quadratic residue (mod 8039)?

$\left(\frac{1001}{8039}\right)$ *1001 is not a prime... use rule 2!*

$$\left(\frac{1001}{8039}\right) = \left(\frac{7 * 11 * 13}{8039}\right) = \left(\frac{7}{8039}\right)\left(\frac{11}{8039}\right)\left(\frac{13}{8039}\right)$$

use quadratic reciprocity on each because the numerators are all prime numbers

$$\left(\frac{1001}{8039}\right) = -\left(\frac{8039}{7}\right) - \left(\frac{8039}{11}\right)\left(\frac{8039}{13}\right)$$

use the 2nd rule

$$\left(\frac{1001}{8039}\right) = -\left(\frac{3}{7}\right) - \left(\frac{9}{11}\right)\left(\frac{5}{13}\right) = \left(\frac{3}{7}\right)\left(\frac{9}{11}\right)\left(\frac{5}{13}\right)$$

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = -1$$

$$\left(\frac{9}{11}\right) = \left(\frac{3 * 3}{11}\right) = 1$$

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{1001}{8039}\right) = -1 * 1 * -1 = 1$$

Therefore, 1001 is a quadratic residue of 8039.