

## QUADRATIC RESIDUES

Let  $p$  be an odd prime. Let  $a$  be an integer relatively prime to  $p$ .

We define the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if the congruence } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if the congruence } x^2 \equiv a \pmod{p} \text{ has no solution} \end{cases}$$

### Theorems:

1.  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$  if  $a \equiv b \pmod{p}$
2.  $\left(\frac{a^2}{p}\right) = 1$
3.  $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$  (This is Euler's Criterion)
4.  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
5.  $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$
6.  $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$

### The Law of Quadratic Reciprocity by Gauss:

Let  $p$  &  $q$  be distinct odd primes. Then

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

### Example:

Determine whether  $x^2 \equiv -12 \pmod{29}$  has a solution.

$$\begin{aligned} \left(\frac{-12}{29}\right) &= \left(\frac{-1}{29}\right) \left(\frac{12}{29}\right) && \text{by Theorem (4)} \\ &= \left(\frac{12}{29}\right) && \text{by Theorem (5) since } 29 \equiv 1 \pmod{4} \\ &= \left(\frac{2^2}{29}\right) \left(\frac{3}{29}\right) && \text{by Theorem (4)} \\ &= \left(\frac{3}{29}\right) && \text{by Theorem (2)} \\ &= \left(\frac{29}{3}\right) && \text{by the Law of Quadratic Reciprocity since } 29 \equiv 1 \pmod{4} \\ &= \left(\frac{2}{3}\right) && \text{by Theorem (1)} \\ &= -1 && \text{by Theorem (6) since } 3 \equiv 3 \pmod{8} \end{aligned}$$

Therefore  $x^2 \equiv -12 \pmod{29}$  has no solution.