

Question: what is  $\left(\frac{-1}{p}\right)$ ?

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

Theorem (Euler's Criterion) Let  $p$  be an odd prime, and  $a$  an integer with  $\gcd(a, p) = 1$ .

Then:  $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ .

Proof: First, we assume that  $a$  is a QR.

This means  $\left(\frac{a}{p}\right) = 1$ ,

and we can find  $b$  such that

$$b^2 \equiv a \pmod{p}$$

This gives:

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

$$\equiv b^{p-1}$$

$$\equiv 1 \pmod{p}$$

↓ Fermat's  
Little  
Theorem.

This shows: when  $a$  is a QR.

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \equiv 1 \pmod{p}.$$

We consider the equation:

$$X^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

This is a polynomial of degree  $\frac{p-1}{2}$ .

It has at most  $\frac{p-1}{2}$  incongruent solutions

We know that we have exactly  $\frac{p-1}{2}$  QR

and each QR will be solution for

$$X^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$\Rightarrow$  QR will exhaust all the solutions for the equation.

Therefore, let  $b$  be a NR (mod  $p$ ).

$$b^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$$

On the other hand, Fermat's Little Theorem:

$$b^{p-1} \equiv 1 \pmod{p}$$

$$p \mid (b^{p-1} - 1) = (b^{\frac{p-1}{2}} + 1)(b^{\frac{p-1}{2}} - 1)$$

$$b^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \Rightarrow p \nmid b^{\frac{p-1}{2}} - 1$$

$$\text{Therefore } b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$$\underline{b \text{ is a NR}} \Rightarrow \left(\frac{b}{p}\right) \equiv -1 \pmod{p}$$

$$\Rightarrow b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}$$

Therefore, for any  $a$  with  $\gcd(a, p) = 1$

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}. \quad \square$$

Theorem (21.2. Quadratic Reciprocity, Part I).

Let  $p$  be an odd prime. Then

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

Proof: By Euler's criterion,

$$(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p}$$

Case I:  $p \equiv 1 \pmod{4}$ ,  $\frac{p-1}{2}$  is even

$$(-1)^{\frac{p-1}{2}} = 1.$$

$$\left(\frac{-1}{p}\right) \equiv 1 \pmod{p}$$

$p$  odd and  $\left(\frac{-1}{p}\right)$  only takes value  $\pm 1$

$$\Rightarrow \left(\frac{-1}{p}\right) = 1.$$

Case II:  $p \equiv 3 \pmod{4}$ ,  $\frac{p-1}{2}$  odd

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

$$\left(\frac{-1}{p}\right) \equiv -1 \pmod{p}$$

$p$  odd and  $\left(\frac{-1}{p}\right)$  only takes value  $\pm 1$

$$\Rightarrow \left(\frac{-1}{p}\right) = -1.$$

□

Theorem: There are infinitely many primes that are congruent to  $1 \pmod{4}$ .

Proof: (Proof by contradiction)

Suppose that we can find only finitely many primes which are congruent to  $1 \pmod{4}$ , we can list all such numbers:

$$p_1, p_2, \dots, p_r.$$

Set  $A = (2p_1 p_2 \dots p_r)^2 + 1$ .

Then  $\gcd(A, p_1) = \gcd(A, p_2) = \dots = \gcd(A, p_r) = 1$

Let  $q \mid A$  be a prime.

(Then  $\gcd(q, p_1) = \gcd(q, p_2) = \dots = \gcd(q, p_r) = 1$ )

Claim:  $q \equiv 1 \pmod{4}$

$$q \mid A \quad \text{and} \quad A = (2p_1 p_2 \dots p_r)^2 + 1$$

$$\Rightarrow (2p_1 p_2 \cdots p_r)^2 + 1 \equiv 0 \pmod{q}$$

$$\text{i.e. } (2p_1 p_2 \cdots p_r)^2 \equiv -1 \pmod{q}$$

$$\text{This means: } \left(\frac{-1}{q}\right) = 1$$

$$\text{and hence } q \equiv 1 \pmod{4}$$

$p_1, p_2, \dots, p_r$  is the complete list of primes that are congruent to  $1 \pmod{4}$

$\Rightarrow q$  should be one of them.

However,  $\gcd(p_1, q) = \gcd(p_2, q) = \dots = \gcd(p_r, q) = 1$ .

A contradiction.

Therefore, there are infinitely many primes which are congruent to  $1 \pmod{4}$   $\square$