

Thm. p odd prime.

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

Proof.

2) - 4) follow from 1)

1) \Rightarrow 2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$, and the equivalence follows since they're ± 1 ,
i.e. $\left(\frac{a}{p}\right) = 1$ iff $\left(\frac{b}{p}\right) = 1 \pmod{p}$

1) \Rightarrow 3) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}$

4) follows from substituting -1 in for a in 1).

Proof of 1):

Let g have order $p-1$

$\{0, g, \dots, g^{p-1}\}$ complete residue system

If $p \nmid a$, the formula holds.

Assume $p \mid a$.

$a \equiv g^i \pmod{p}$.

Claim: $x^2 \equiv a \pmod{p}$ has soln iff $2 \mid i$

If $b^2 \equiv a \pmod{p}$, write $b \equiv g^u \pmod{p}$, so $b^2 \equiv g^{2u} \equiv g^i \equiv a \pmod{p}$,

$$\Rightarrow p-1 \mid 2u-i$$

say $2u \equiv i$. Then $g^{2u-i} \equiv 1 \pmod{p}$, so order $p-1$ of g divides $2u-i$.

p odd $\Rightarrow p-1$ even, so if $p-1 \mid 2u-i$, $2u-i$ even, so i even.

so $i = 2k$, some k . $\left(\frac{a}{p}\right) = 1$, then $a^{\frac{p-1}{2}} \equiv (g^{2k})^{\frac{p-1}{2}} \equiv g^{p-1} \equiv 1 \pmod{p}$

If $a \equiv g^{2k} \pmod{p}$, then $a \equiv (g^k)^2 \pmod{p}$.

If $\left(\frac{a}{p}\right) = -1$, then $2 \nmid i$ because g^{2k} is a square mod p for any k .

Show $a^{\frac{p-1}{2}} \equiv g^{i\left(\frac{p-1}{2}\right)} \pmod{p}$. i.e. could $g^{i\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}$?

since $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ by Fermat if $p \nmid a$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

If $g^{i\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}$, then $p-1 \mid i\left(\frac{p-1}{2}\right)$

$$p-1 = 2^m m', \quad m' \text{ odd}; \quad i\left(\frac{p-1}{2}\right) = 2^{m-1} m' i, \quad (m' i, 2) = 1$$

so this is impossible.

Cor. There are as many quadratic residues as there are quadratic nonresidues, \pmod{p} .

Proof. We showed that $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ has $\frac{p-1}{2}$ solutions.

The number of quadratic residues = $\frac{p-1}{2}$ The number of quadratic nonresidues = $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$

Or just count even exponents in g, g^2, \dots, g^{p-1}

Cor: There are infinitely many primes of the form $4k+1$.

Proof: By contradiction, say p_1, \dots, p_r are all primes of this form.

Look at

$$N = (2p_1 \cdots p_r)^2 + 1$$

add say $p \mid N$, some prime factor p .

• p is odd, since N is odd

$$\bullet p \equiv 1 \pmod{4}$$

Since $(2p_1 \cdots p_r)^2 \equiv -1 \pmod{p}$, which means $\left(\frac{-1}{p}\right) = 1 = (-1)^{\frac{p-1}{2}}$

$$\Rightarrow \frac{p-1}{2} \text{ even} \Rightarrow p = 4k+1, \text{ some } k.$$

$$\Rightarrow p = p_i, \text{ some } i, \Rightarrow p_i \mid (2p_1 \cdots p_r)^2 + 1 \text{ contradiction}$$

Another computation of $\left(\frac{a}{p}\right)$

$S = \left\{ -\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -1, 1, 2, \dots, \frac{p-1}{2} \right\}$ complete residue system $\not\equiv 0 \pmod{p}$

$(a, p) = 1$. For each l , let $r_l \in S$ be unique number in $S \equiv la \pmod{p}$.

Let $\mu = \#$ of negative r_l 's for $1 \leq l \leq \frac{p-1}{2}$.

Invm $\left(\frac{a}{p}\right) = (-1)^\mu$

Ex: $\left(\frac{6}{13}\right)$

$$S = \{-6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6\}$$

compute classes of $1 \cdot 6, 2 \cdot 6, 3 \cdot 6, 4 \cdot 6, 5 \cdot 6, 6 \cdot 6$

$$\begin{array}{cccccc} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & -1 & 5 & -2 & 4 & -5 \end{array}$$

$$\mu = 3 \Rightarrow \left(\frac{6}{13}\right) = (-1)^3 = -1, \text{ so } 6 \text{ not a square mod } 13.$$