

19.791

20 Mar 2003

p odd prime, $(a, p) = 1$

Formula for $\left(\frac{a}{p}\right)$:

Let $S = \left\{ \frac{-(p-1)}{2}, \frac{-(p-3)}{2}, \dots, -1, 1, 2, \dots, \frac{p-1}{2} \right\}$ reduced residue system

Let r_l be the unique representative of the congruence class of la , $1 \leq l \leq \frac{p-1}{2}$

Let $\mu = \#$ neg. r_l 's.

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

Proof. Write $r_l = (-1)^{\sigma_l} m_l$, where $m_l = |r_l|$ and $\sigma_l \in \{0, 1\}$

claim: For $l \neq k$, $m_l \not\equiv m_k \pmod{p}$

Reason: $la = (-1)^{\sigma_l} m_l \equiv (-1)^{\sigma_k} m_k \equiv ka \pmod{p}$, if $m_k \equiv m_l \pmod{p}$.

$\Rightarrow (l-k)a \equiv 0 \pmod{p} \Rightarrow p \mid l-k$, since $(p, a) = 1$.

But $1 \leq l, k \leq \frac{p-1}{2}$, so $l+k \leq l+k < p$, so $p \mid (l-k) \Rightarrow l=k$.

What are the classes of the m_l 's?

$\Rightarrow \{m_1, \dots, m_{\frac{p-1}{2}}\} = \{1, \dots, \frac{p-1}{2}\}$ (since m_l is distinct and contained in this set).

Now multiply together $la = (-1)^{\sigma_l} m_l \pmod{p}$, $1 \leq l \leq \frac{p-1}{2}$

$\Rightarrow \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv \prod (-1)^{\sigma_l} (m_1 \dots m_{\frac{p-1}{2}}) \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p}$

cancel $\left(\frac{p-1}{2}\right)!$, since prime to p :

$\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}$, and from last time

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

Thm. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, p odd prime

Proof:

Lemma: $8 \mid p^2 - 1$ and $\frac{p^2-1}{8} = \begin{cases} \text{even } p \equiv \pm 1 \pmod{8} \\ \text{odd } p \equiv \pm 3 \pmod{8} \end{cases}$

Proof: Write $p = 8q + r$, $r \in \{1, \pm 3\}$

$$p^2 - 1 = 64q^2 + 16qr + r^2 - 1$$

case 1: $r = \pm 1$.

Then $r^2 - 1 = 0$, so $p^2 - 1 = 64q^2 + 16qr$,

and $\frac{p^2-1}{8} = 8q^2 + 2qr$, an even integer.

case 2: $r = \pm 3$

$$\frac{p^2-1}{8} = \frac{64q^2 \pm 48q + 8}{8} = 8q^2 \pm 6q + 1, \text{ an odd integer.}$$

Write down μ in this case:

$\{2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot \frac{p-1}{2}\}$, look at corresponding classes r_l

is $\left\{ \frac{-(p-1)}{2}, \dots, \frac{p-1}{2} \right\}$

Let m be defined by $2m \equiv \frac{p-1}{2}$, $2(m+1) > \frac{p-1}{2}$

$$\mu = \left(\frac{p-1}{2} - m\right)$$

$$\begin{aligned}
 p &= 8k+1 & \frac{p-1}{2} &= \frac{8k+1-1}{2} = 4k, \quad m=2k, \text{ even}, \mu = \left(\frac{p-1}{2} - 2k\right), \text{ even} \Rightarrow \left(\frac{a}{p}\right) = 1 \\
 p &= 8k+7 & \frac{p-1}{2} &= \frac{8k+7-1}{2} = 4k+3, \quad m=2k+1, \mu = 4k+5-2(2k+1) = 2k+2, \text{ even} \Rightarrow \left(\frac{a}{p}\right) = 1 \\
 p &= 8k+5 & \frac{p-1}{2} &= \frac{8k+5-1}{2} = 4k+2, \quad m=2k, \mu = 4k+1-2k = 2k+1, \text{ odd} \Rightarrow \left(\frac{a}{p}\right) = -1 \\
 p &= 8k+3 & \frac{p-1}{2} &= \frac{8k+3-1}{2} = 4k+1, \quad m=2k+1, \mu = 4k+2-(2k+1) = 2k+1, \text{ odd} \Rightarrow \left(\frac{a}{p}\right) = -1.
 \end{aligned}$$

Quadratic Reciprocity Thm:

If $p \neq q$ are odd primes, then

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

ex: Does $x^2 \equiv 7 \pmod{1009}$ have a solution?

- Assume 1009 prime.

$$\left(\frac{7}{1009}\right)\left(\frac{1009}{7}\right) = (-1)^{\left(\frac{7-1}{2}\right)\left(\frac{1009-1}{2}\right)} = 1, \text{ so } \left(\frac{7}{1009}\right) = \left(\frac{1009}{7}\right) \text{ (since both } \neq 1)$$

$$\text{Now } 1009 \equiv 1 \pmod{7}, \text{ so } \left(\frac{1009}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

so 7 is a square mod 1009.

ex: For which primes p is 5 a square?

$$\text{Ans: } \left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\left(\frac{p-1}{2}\right)} = 1 \text{ so } \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

$$x \mid 1 \ 2 \ 3 \ 4 \quad (\text{mod } 5), \text{ so } \left(\frac{5}{p}\right) = 1 \text{ iff } p \equiv \pm 1 \pmod{5}$$

$$x^2 \mid 1 \ 4 \ 4 \ 1 \quad \text{or } p = 2.$$