9/2/2026

Thm (Gauss's lemma) Let $p > 2$ be prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Define

$$\varepsilon_a = \begin{cases} 1, & a > 0, \\ -1, & a < 0. \end{cases}$$

For each $1 \leq i \leq \frac{p-1}{2}$, consider

$$i \, \overset{|a|}{\boxed{\varepsilon_a a}} = q_i p + r_i, \quad 1 \leq r_i < p.$$

Let m be the number of $1 \leq i \leq \frac{p-1}{2}$ s.t.

$$\frac{p}{2} < r_i < p.$$

Then

$$\left(\frac{a}{p}\right) = (-1)^m \varepsilon_a^{\frac{p-1}{2}}. \qquad (1)$$

Moreover,

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{k\varepsilon_a a}{p} \right\rfloor + \frac{p^2-1}{8}(a-1) \pmod 2. \quad (2)$$

Pf. Let

$$I = \{1 \leq i \leq \tfrac{p-1}{2} : r_i < \tfrac{p}{2}\},$$

$$J = \{1 \leq j \leq \tfrac{p-1}{2} : r_j > \tfrac{p}{2}\}.$$

$I \cap J = \phi$, $I \cup J = \{1, 2, \cdots, \frac{p-1}{2}\}$, $|J| = m$.

Observation: r_i ($i \in I$) are distinct.

r_j ($j \in J$) are distinct.

For example, if $r_{i_1} = r_{i_2}$ for $i_1, i_2 \in I$, then

$$i_1 \varepsilon_a a \equiv i_2 \varepsilon_a a \pmod p.$$

So $i_1 \equiv i_2 \pmod p$. But $1 \leq i_1, i_2 < \frac{p}{2}$. So $i_1 = i_2$.

Let

$$A = \{ r_i : i \in I \} \subseteq \{1, 2, \dots, \tfrac{p-1}{2}\}$$

$$B = \{ p - r_j : j \in J \} \subseteq \{1, 2, \dots, \tfrac{p-1}{2}\}.$$

Claim: $A \cap B = \emptyset$.

Why: Say $r_i = p - r_j$. Then

$$i \varepsilon_a \cdot a \equiv -j \varepsilon_a \cdot a \pmod{p}.$$

$$\Leftrightarrow \quad i \equiv -j \pmod{p}.$$

$$\Leftrightarrow \quad i + j \equiv 0 \pmod{p}.$$

$$\Leftrightarrow \quad p \mid i + j.$$

$$\Rightarrow \quad i + j \geq p.$$

But $1 \leq i, j \leq \frac{p-1}{2} \Rightarrow i + j < p$, a contradiction.

Hence, $A \cup B = \{1, 2, \cdots, \frac{p-1}{2}\}$. So

$$\prod_{i\in I} \underbrace{r_i}_{\equiv i\varepsilon_a a \pmod{p}} \prod_{j\in J} \underbrace{(p-r_j)}_{\equiv -j\varepsilon_a a \pmod{p}} = 1\cdot 2\cdots\left(\frac{p-1}{2}\right).$$

$$\Rightarrow \prod_{i\in I} i\varepsilon_a a \prod_{j\in J} (-j\varepsilon_a a) \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

$$\Rightarrow (-1)^m (\varepsilon_a a)^{\frac{p-1}{2}} \underbrace{\prod_{i\in I} i \prod_{j\in J} j}_{\cancel{\left(\frac{p-1}{2}\right)!}} \equiv \cancel{\left(\frac{p-1}{2}\right)}! \pmod{p}$$

$$\Rightarrow (-1)^m \varepsilon_a^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^m \varepsilon_a^{\frac{p-1}{2}} \pmod{p}$$

Euler's criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

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

Equivalently,

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

This proves (1).

To proceed, recall

$$i \varepsilon_a a = q_i p + r_i, \quad 1 \le r_i < p.$$

By HWI, $q_i = \left\lfloor \frac{i \varepsilon_a a}{p} \right\rfloor$.

Adding them up:

$$\sum_{i=1}^{\frac{p-1}{2}} i \varepsilon_a a = \sum_{i=1}^{\frac{p-1}{2}} q_i p + \sum_{i=1}^{\frac{p-1}{2}} r_i$$

$$\Rightarrow \varepsilon_a \cdot a \sum_{i=1}^{\frac{p-1}{2}} i = \sum_{i=1}^{\frac{p-1}{2}} q_i p + \sum_{i \in I} r_i + \sum_{j \in J} r_j \quad ①$$

Just showed $\{r_i, p - r_j : i \in I, j \in J\} = \{1, 2, \cdots, \frac{p-1}{2}\}$.

So

$$\sum_{i\in I} r_i + \sum_{j\in J} (p - r_j) = \sum_{i=1}^{\frac{p-1}{2}} i$$

$$\Rightarrow \sum_{i\in I} r_i + mp - \sum_{j\in J} r_j = \sum_{i=1}^{\frac{p-1}{2}} i$$

$$\Rightarrow \sum_{j\in J} r_j = \sum_{i\in I} r_i + mp - \sum_{i=1}^{\frac{p-1}{2}} i$$

Plugging ② in ① :

$$\varepsilon_a \cdot a \sum_{i=1}^{\frac{p-1}{2}} i = \sum_{i=1}^{\frac{p-1}{2}} \varepsilon_i p + 2\sum_{i\in I} r_i + mp - \sum_{i=1}^{\frac{p-1}{2}} i$$

$$\Rightarrow -mp = \sum_{i=1}^{\frac{p-1}{2}} \varepsilon_i p + 2\sum_{i\in I} r_i + mp - (\varepsilon_a a + 1) \underset{\frac{p^2-1}{8}}{\underset{\|}{\boxed{\sum_{i=1}^{\frac{p-1}{2}} i}}}$$

$$\Rightarrow m \equiv \sum_{i=1}^{\frac{p-1}{2}} \underset{\left\lfloor \frac{i\varepsilon_a a}{p} \right\rfloor}{\boxed{\varepsilon_i}} + (a-1)\frac{p^2-1}{8} \pmod 2.$$

$\square$

Cor (2 mod p) For every prime $p > 2$,

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

In other words,

$$2 \, R \, p \iff p \equiv 1, 7 \pmod 8;$$

$$2 \, R \, p \iff p \equiv 3, 5 \pmod 8.$$

Pf. Gauss's lemma with $a = 2$:

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

where

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2k}{p} \right\rfloor + \frac{p^2-1}{8} \pmod 2.$$

$$0 < k < \frac{p}{2} \Rightarrow 0 < \frac{2k}{p} < 1 \Rightarrow \left\lfloor \frac{2k}{p} \right\rfloor = 0.$$

So

$$m \equiv \frac{p^2-1}{8} \pmod 2$$

and

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

Moreover, p odd $\overset{DA}{\Longrightarrow} p = 8q + r$, $r = 1, 3, 5, 7$.

$$p^2 = (8q+r)^2 = 64q^2 + 16qr + r^2$$

$$\Rightarrow \frac{p^2-1}{8} = 8q^2 + 2qr + \frac{r^2-1}{8}$$

$$\equiv \frac{r^2-1}{8} \pmod 2$$

$$\equiv \begin{cases} 0, & r = 1, 7 \\ 1, & r = 3, 5 \end{cases} \pmod 2$$

$\square$

Ex. Use Gauss's lem to show that

$$-3 \, R \, p \iff p \equiv 1 \pmod 6;$$

$$-3 \, N \, p \iff p \equiv 5 \pmod 6.$$

In general, if $p \nmid a$, then

$$a = \varepsilon_a 2^n p_1^{n_1} \cdots p_r^{n_r}, \quad p_1, \dots, p_r \neq p \text{ are odd.}$$

$$\Rightarrow \left(\frac{a}{p}\right) = \underset{\checkmark}{\left(\frac{\varepsilon_a}{p}\right)} \underset{\checkmark}{\left(\frac{2}{p}\right)^n} \underset{?}{\left(\frac{p_1}{p}\right)^{n_1}} \cdots \underset{?}{\left(\frac{p_r}{p}\right)^{n_r}}.$$

Next goal: determine $\left(\frac{q}{p}\right)$ when $p, q > 2$ are distinct primes.