8/31/2026

Recall:

Legendre symbol: For any prime $p > 2$ and $a \in \mathbb{Z}$, define

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \, R \, p, \\ -1, & a \, N \, p, \\ 0, & p \mid a. \end{cases}$$

(1) (Periodicity) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) (Complete multiplicativity). Given $a, b \in \mathbb{Z}$,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

So $a \, R \, p, \; b \, R \, p \Rightarrow ab \, R \, p$

$a \, R \, p, \; b \, N \, p \Rightarrow ab \, N \, p$

$a \, N \, p, \; b \, N \, p \Rightarrow ab \, R \, p$

Thm (Euler's criterion) For any prime $p > 2$ and $a \in \mathbb{Z}$ with $p \nmid a$,

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

Cor (-1 mod p) Let $p > 2$ be prime. Then

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

In other words, $-1 \, R \, p$ if $p \equiv 1 \pmod 4$;

$-1 \, N \, p$ if $p \equiv 3 \pmod 4$.

Cor. Let $p \geq 2$ be prime.

(1) (Wilson's thm) $(p-1)! \equiv -1 \pmod p$.

(2) Suppose $p > 2$. Let

$$R = \{\text{quadratic residues mod } p\},$$

$$N = \{\text{quadratic nonresidues mod } p\}.$$

$$\prod_{r \in R} r \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

$$\prod_{n \in N} n \equiv (-1)^{\frac{p-1}{2}} \pmod p.$$

Moreover, if $p \geq 5$, then

$$\sum_{r \in R} r \equiv \sum_{n \in N} n \equiv 0 \pmod p.$$

E.g. $p=7$: $(p-1)! = 6! = 720 = 7\cdot 100 + 20$

$$\equiv 20 \pmod 7$$

$$\equiv -1 \pmod 7.$$

Pf. (1) Consider

$$f(x) = \underbrace{(x^{p-1}-1)} - \underbrace{(x-1)(x-2)\cdots(x-(p-1))}.$$

① degree $= p-1$

② leading coefficient $=1$

③ has $1, 2, \cdots, p-1$ as roots

① $\deg f(x) < p-1$

② $f(x)$ has $1, 2, \cdots, p-1$ as roots.

By Lagrange, p divides every coefficient of $f(x)$.

So p divides the constant $= -1 - (-1)^{p-1}(p-1)!$

If $p > 2$, then $p-1$ is even, so

$$-1-(p-1)! \equiv 0 \pmod p$$

$$\Leftrightarrow \quad (p-1)! \equiv -1 \pmod p.$$

If $p=2$, $(2-1)! = 1 \equiv -1 \pmod 2$

(2) For quadratic residues, consider

$$g(x) = (x^{\frac{p-1}{2}} - 1) - \prod_{r \in R} (x-r);$$

for quadratic nonresidues, consider

$$h(x) = (x^{\frac{p-1}{2}} + 1) - \prod_{n \in N} (x-n).$$

Can show p divides all the coefficients of $g(x)$ and $h(x)$.

Constant coefficients $\Rightarrow \prod_{r \in R} r, \prod_{n \in N} n \pmod p$.

Coefficients of $x \Rightarrow \sum_{r \in R} r, \sum_{n \in N} n \pmod p$.

$(p \geq 5 \Rightarrow \frac{p-1}{2} \geq 2)$ $\square$

Floor function

For $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.

You showed in HW: $x - 1 < \lfloor x \rfloor \leq x$.

E.g. (i) $\lfloor 3.2 \rfloor = 3$.

(ii) $\lfloor -2.5 \rfloor = -3$.

Observation: When $x \geq 0$, $\lfloor x \rfloor$ counts the number of positive integers $n \leq x$.

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

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

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

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

Then

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

Moreover,

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

Pf. Let

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

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

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

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 $1 \le i_1, i_2 < \frac{p}{2}$. So $i_1 = i_2$.

Let

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

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

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

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

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

Continue next time.