8/28/2026

Last time:

Thm (Lagrange) Let p be a prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

with $p \nmid a_n$. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n roots.

Qudratic congruence equations.

We reduced

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

to $y^2 \equiv \Delta \pmod{4am}$, where $\Delta = b^2 - 4ac$ and $y = 2ax + b$.

Quadratic residues & nonresidues modulo $p > 2$.

Defn (Quadratic residues & nonresidues). An integer a, with $p \nmid a$, is a quadratic residue mod p if there is $x \in \mathbb{Z}$ s.t. $x^2 \equiv a \pmod{p}$. Otherwise, a is called a quadratic nonresidue mod p.

Notation: Write $a R p$ if a is a residue mod p,

$a N p$ if a is a nonresidue mod p.

Lem. Let $p > 2$ be prime and $a \in \mathbb{Z}$ s.t. $p \nmid a$. Then

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

has no solution or 2 solutions.

The proof shows that if $x \equiv x_0 \pmod p$ is a solution, so

is $x \equiv -x_0 \equiv p - x_0 \pmod p$.

Lem. Let $p > 2$. There are $\frac{p-1}{2}$ quadratic residues and

$\frac{p-1}{2}$ quadratic nonresidues mod p.

Pf. The residues are

A: $1^2, \; 2^2, \; 3^2, \; \ldots, \; \left(\frac{p-1}{2}\right)^2$,

B: $(p-1)^2, \; (p-2)^2, \; (p-3)^2, \; \ldots, \; \left(p - \frac{p-1}{2}\right)^2$.

Take $i^2 \equiv j^2 \pmod p$, $1 \leq i, j \leq \frac{p-1}{2}$.

$\Rightarrow i \equiv j \pmod p$ or $i \equiv -j \pmod p$

As $1 \leq i, j \leq \frac{p-1}{2}$, $|i \pm j| \leq p-1$.

So $i \pm j = 0$, hence $i = j$.

So there are $\frac{p-1}{2}$ residues and $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ nonresidues. $\square$

Thm (Euler's criterion, version 1). Let $p > 2$ and $a \in \mathbb{Z}$ s.t. $p \nmid a$.

(1) If $a R p$, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(2) If $a N p$, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Pf. (1) If $a R p$, there is some $x \in \mathbb{Z}$ s.t.

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

Fermat $\Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$.

(2) Consider

$$\underbrace{x^{p-1}-1}_{f(x)} = \underbrace{(x^{\frac{p-1}{2}}-1)}_{g(x)}\underbrace{(x^{\frac{p-1}{2}}+1)}_{h(x)}.$$

$\left\{\begin{array}{l}\text{Fermat}\\ \text{Lagrange}\end{array}\right. \Rightarrow f(x) \equiv 0 \pmod p$ has exactly $p-1$ roots!

$$x \equiv 1, 2, \cdots, p-1 \pmod p.$$

Part (1) $\overset{\text{Lem}}{\Longrightarrow}$ $g(x) \equiv 0 \pmod p$ has at least $\frac{p-1}{2}$ roots

given by all the quadratic residues mod p.

$\deg g(x) = \frac{p-1}{2} \overset{\text{Lagrange}}{\Longrightarrow} g(x) \equiv 0 \pmod p$ has at most $\frac{p-1}{2}$ roots.

So $g(x) \equiv 0 \pmod p$ has exactly $\frac{p-1}{2}$ roots.

Now, if $a\ N\ p$, then $f(a) \equiv 0 \pmod p$ but $g(a) \not\equiv 0 \pmod p$.

So $h(a) \equiv 0 \pmod p$, i.e. $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$ $\square$

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

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

Thm (Euler's criterion, version 2). 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 (Properties of Legendre symbol) Let $p > 2$ be prime.

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

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

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

In particular, if $ab \equiv 1 \pmod p$, then

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

Pf. Exercise.

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 $p \equiv 3 \pmod 4$.

Pf. (*) follows from Euler's criterion, version 2.

Note also that $\frac{p-1}{2}$ is even when $p \equiv 1 \pmod 4$ and odd when $p \equiv 3 \pmod 4$. For instance, $\frac{p-1}{2}$ is even if

$$\frac{p-1}{2} \equiv 0 \pmod 2$$

$$\Leftrightarrow p-1 \equiv 0 \pmod 4$$

$$\Leftrightarrow p \equiv 1 \pmod 4. \qquad \square$$

E.g. $-1 \; R \; 13$, since $13 = 3 \cdot 4 + 1 \equiv 1 \pmod 4$,

$-1 \; N \; 11$, since $11 = 2 \cdot 4 + 3 \equiv 3 \pmod 4$.

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

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