8/24/2026

Recall:

Congruences.

Defn (Congruence) Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$. We say a is congruent to b modulo m if $m \mid (a-b)$.

Notation. $a \equiv b \pmod{m}$

"$\equiv$" is an equivalence relation:

(1) Reflexivity: $a \equiv a \pmod{m}$.

(2) Symmetry: $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

(3) Transitivity: $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$

$\Rightarrow a \equiv c \pmod{m}$.

Properties :

1. $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$

$$\Rightarrow \begin{cases} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m \\ a_1 a_2 \equiv b_1 b_2 \pmod m \end{cases}$$

Special cases : ① $a \equiv b \pmod m \Leftrightarrow a \pm c \equiv b \pm c \pmod m$.

② $a \equiv b \pmod m \Rightarrow ka \equiv kb \pmod m$

③ $a \equiv b \pmod m \Rightarrow a^k \equiv b^k \pmod m$, $k \geq 0$.

2. $a \equiv b \pmod{mn} \Rightarrow a \equiv b \pmod m$, $a \equiv b \pmod n$.

3. $ka \equiv kb \pmod m \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$, $d = (k, m)$

Special cases : ① If $(k, m) = 1$, then

$$ka \equiv kb \pmod m \Leftrightarrow a \equiv b \pmod m .$$

② When $m = kn$,

$$ka \equiv kb \pmod{kn} \iff a \equiv b \pmod{n}.$$

4. $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$

"least common multiple of m, n"

$$\iff a \equiv b \pmod{\frac{mn}{d}}, \quad d = (m, n)$$

Warning! $4 \equiv 2 \pmod{2}$, $4 \equiv 2 \pmod{2}$

But $4 \equiv 2 \pmod{2 \cdot 2}$ ✗

Defn (Residue/Congruence class) A residue class mod m is just an equivalence class under $\equiv$. Explicitly, it is a set $K_a = \{n \in \mathbb{Z} : n \equiv a \pmod{m}\}$. There are m different residue classes mod m.

Observation: If $a_1, a_2, \dots, a_m$ are from difference residue classes mod m, and if $b \in \mathbb{Z}$ with $(b, m) = 1$, then $a_1 b, a_2 b, \dots, a_m b$ also come from difference residue classes.

Why? Say $a_i b \equiv a_j b \pmod{m}$. Since $(b, m) = 1$, $a_i \equiv a_j \pmod{m}$. So $i = j$.

Similarly, if $a_1, \dots, a_k$ are the numbers from 1 to m with gcd 1 with m, and if $b \in \mathbb{Z}$ with $(b, m) = 1$, then $a_1 b, \dots, a_k b$ represent all residue classes with gcd 1 with m.

Exercise.

Euler's Thm and Fermat's Little Thm.

Defn (Euler's totient function) Let m be a positive integer. The Euler totient function, denoted by $\phi(m)$, counts the number of integers $1 \le n \le m$ s.t. $(n, m) = 1$.

E.g. 1. $m = 12$: $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$

So $\phi(12) = 4$.

2. m is prime : $n = 1, 2, 3, \dots, m-1, m$

So $\phi(m) = m - 1$.

Thm (Euler) Let m be a positive integer and let $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

E.g. $m = 12$, $a = 5$; $\phi(12) = 4$

$$a^{\phi(m)} = 5^4 = (5^2)^2$$

$$\Rightarrow (25)^2 \equiv 1^2 \equiv 1 \pmod{12}$$

$$\equiv 1 \pmod{12}$$

pf. Let $1 \le a_1 < a_2 < \cdots < a_{\phi(m)} \le m$ be all the numbers from 1 to m that have gcd 1 with m. Multiply each of them by a:

$$a_1 \cdot a, \; a_2 \cdot a, \; \ldots, \; a_{\phi(m)} \cdot a.$$

These numbers come from distinct residue classes that have gcd 1 with m, and hence they form a rearrangement of $a_1, \dots, a_{\phi(m)} \pmod{\phi(m)}$. So

$$a_1 a_2 \cdots a_{\phi(m)} \equiv (a_1 \cdot a)(a_2 \cdot a) \cdots (a_{\phi(m)} \cdot a) \pmod{m}.$$

$$1 \equiv a^{\phi(m)} \pmod{m} \qquad \square$$

Thm (Fermat) Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Equivalently, $a^p \equiv a \pmod{p}$.

pf. Take $m = p$ in Euler's thm and observe $\phi(p) = p-1$. $\square$

Linear congruence equations.

A linear congruence equation in unknown x is a congruence of the form

$$ax + b \equiv 0 \pmod{m}$$

or equivalently, of the form

$$ax \equiv b \pmod{m}.$$

Q: 1. When is it solvable?

2. How many solutions?

3. What do the solutions look like?

Eg. $3x \equiv 6 \pmod 9$.

$x = 0, 1, 2, 3, 4, 5, 6, 7, 8$.

Solvable ✓

How many? $3 = \gcd(3, 9)$.

Solutions: $2, 5, 8$. (+3, +3)

Thm. The linear equation $ax \equiv b \pmod m$ has a solution if and only if $d \mid b$, where $d = \gcd(a, m)$, in which case there are exactly d solutions. Moreover, if x_0 is a solution, then every solution is of the form $x = x_0 + k \cdot \frac{m}{d}$, where k is any integer.