Recall: In the previous lecture, we've seen for a polynomial $p(x)$ with integer coefficients that

$$a \equiv b \pmod{m} \implies p(a) \equiv p(b) \pmod{m}$$

For example, let $p(x) = x^3 + 2x^2 + 3x + 5$. Then, we have $p(1) = 11$, $p(4) = 113$, and $11 \equiv 113 \pmod{3}$.

This is actually a very useful tool to prove that some equations have no solution in the integers.

Example: $x^3 - x + 1 = 42$ has no integer solution.

$p(0) \equiv 1 \pmod{3}$, $p(1) \equiv 1 \pmod{3}$, $p(2) \equiv 7 \equiv 1 \pmod{3}$

$x \equiv 0, 1, \text{ or } 2 \pmod{3} \implies p(x) \equiv p(0), p(1), \text{ or } p(2) \pmod{3}$

$\implies p(x) \equiv 1 \pmod{3}$, but $42 \not\equiv 1 \pmod{3}$.

An interesting problem: Is there a polynomial $p(x)$ with integer coefficients such that $p(n)$ is prime for every $n \in \mathbb{Z}$, except the constant polynomial?

The answer is no, see Theorem 3.6 for that.

Now, some properties of the congruences

- Suppose $d \geqslant 1$ and $d \mid m$, then

$$a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$$

$a \equiv b \pmod{m} \Rightarrow m \mid a-b \Rightarrow d \mid a-b \Rightarrow a \equiv b \pmod{d}$.

e.g. $3 \equiv 19 \pmod{8} \Rightarrow 3 \equiv 19 \pmod{2}$

- Suppose $c > 0$, then

$$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{mc}$$

$a \equiv b \pmod{m} \Rightarrow m \mid a-b \Rightarrow a-b = m \cdot k$

$\Rightarrow ac - bc = c \cdot (a-b) = (mc) \cdot k$

$\Rightarrow mc \mid ac - bc \Rightarrow ac \equiv bc \pmod{mc}$.

The next property is similar to

$$m \mid ab \Rightarrow m \mid (m,a) \cdot b \quad .$$

- $ax \equiv ay \pmod{m} \Rightarrow x \equiv y \left(\bmod \dfrac{m}{(m,a)} \right)$

$ax \equiv ay \pmod{m} \Rightarrow m \mid ax - ay \Rightarrow m \mid a \cdot (x-y)$

$\Rightarrow m \mid (m,a) \cdot (x-y) \Rightarrow (m,a) \cdot (x-y) = m \cdot k$

$\Rightarrow x - y = \dfrac{m}{(m,a)} \cdot k \Rightarrow x \equiv y \left(\bmod \dfrac{m}{(m,a)} \right)$.

Special case: $(m,a)=1$, we say $x \equiv y \pmod m$)

This property is useful solving linear congruences:

$$\overset{\text{find}}{ax} \equiv b \pmod{m}$$

given

<u>Example:</u> Which integers x satisfy $15x \equiv 30 \pmod{40}$?

$15 \cdot x \equiv 15 \cdot 2 \pmod{40}$ and $\dfrac{40}{(40,15)} = 8$

$\Rightarrow x \equiv 2 \pmod 8$.

Check: $x \equiv 2 \pmod 8 \Rightarrow x = 8k+2$

$15x = 15(8k+2) = 120k + 30 \equiv 30 \pmod{40}$.

We'll solve $ax \equiv b \pmod m$ in general case (similar to linear diophantine equations).

$k \in \mathbb{Z}$

$ax \equiv b \pmod m$ means $m \mid ax - b$, i.e. $ax - b = m \cdot k$.

Rewrite it as $ax - mk = b$.

- No solution unless $(a,m) \mid b$.
- When $(a,m) \mid b$: There is a solution, say

(x_0, k_0). Then the all solutions will have

$$x = x_0 - t \cdot \frac{m}{(a,m)} \quad \text{with} \quad t \in \mathbb{Z}.$$

$$\text{Set of all solutions} = \left\{ x \in \mathbb{Z} : x = x_0 - t \cdot \frac{m}{(a,m)}, t \in \mathbb{Z} \right\}.$$

$$= \left\{ x \in \mathbb{Z} : x \equiv x_0 \left(\text{mod } \frac{m}{(a,m)} \right) \right\}.$$

<u>Examples:</u> Solve (a) $3x \equiv 7 \pmod{11}$

(b) $9x \equiv 6 \pmod{12}$ (c) $66x \equiv 100 \pmod{121}$

(d) $14x \equiv 1 \pmod{45}$

(a) $x_0 = 6$ is a solution $\Rightarrow x \equiv 6 \pmod{11}$

(b) $9x \equiv 6 \pmod{12} \Rightarrow 3 \cdot 3x \equiv 3 \cdot 2 \pmod{12}$ and $(12,3) = 3$

$\Rightarrow 3x \equiv 2 \pmod{4}$. $x_0 = 2$ is a solution

$\Rightarrow x \equiv 2 \pmod{4}$.

(c) $(121, 66) = 11 \nmid 100 \Rightarrow$ no solution.

(d) $14x \equiv 1 \pmod{45} \Rightarrow 14x = 45k + 1$

$\Rightarrow 14x - 45k = 1$

Euclidean algorithm: $1 = 5 \cdot 45 - 16 \cdot 14$.

$\Rightarrow x_0 = -16$ is a solution $\Rightarrow x \equiv -16 \pmod{45}$.