Discrete Math

Lecture 33

Modular Arithmetic

Def. x is "congruent mod n" to y means

(note: $x, y \in \mathbb{Z}$, $n \in \mathbb{N}^* = \{1, 2, \ldots\}$)

First def: $x - y$ is a multiple of n

$\exists\, m \in \mathbb{Z},\ x - y = m \cdot n$

Second def: x & y have the same remainder when divided by n

(recall: $r \in \{0, 1, \ldots, n-1\}$)

notation: "x is congruent to y mod n"
(equivalent)

$x \equiv y \bmod n$

ex| Is $5 \equiv 13 \mod 4$?

①: $5-13 = -8 = (-2)4$

so yes, $5 \equiv 13 \mod 4$

remainder $r=1$

②: $5 = 1 \cdot 4 + 1$ ⟵ $5 \equiv 1 \mod 4$

$13 = 3 \cdot 4 + 1$ ⟵ $13 \equiv 1 \mod 4$

Suppose $a \equiv b \mod n$

① $a-b = m \cdot n$

Division alg. to $(a-b) \div n$

$a-b = \underline{m}\, n + \underline{0}$

Div. alg. to $a \div n$ & $b \div n$

$$\left.\begin{aligned} a &= q_1 n + r_1 \\ b &= q_2 n + r_2 \end{aligned}\right\} \text{subtract these}$$

$a-b = (q_1 - q_2) n$

$+ (r_1 - r_2)$

Def. 1 $\Rightarrow$ Def. 2

2 $a \equiv b \mod n$

$a = q_1 n + r$

$b = q_2 n + r$

$a - b = (q_1 - q_2) n + (r - r)$

$= (q_1 - q_2) n$ ✓

2 $\Rightarrow$ 1

ex) which integers are congruent to 6 mod 8?

i.e. solve $x \equiv 6 \mod 8$

find x's that satisfy:

$x - 6 = m \cdot 8$

select $m = 1$: $x - 6 = 8 \longrightarrow \boxed{x = 14}$

$m = 0$: $x - 6 = 0 \longrightarrow \boxed{x = 6}$

$m = -1: \quad x - 6 = -8 \longrightarrow \boxed{x = -2}$

$m = 2: \quad x - 6 = 16 \longrightarrow \boxed{x = 32}$

$\{ \ldots, -2, 6, 14, 32, \ldots \}$

note: all solutions are of the form $8m + 6$

$x \equiv 6 \mod 8$

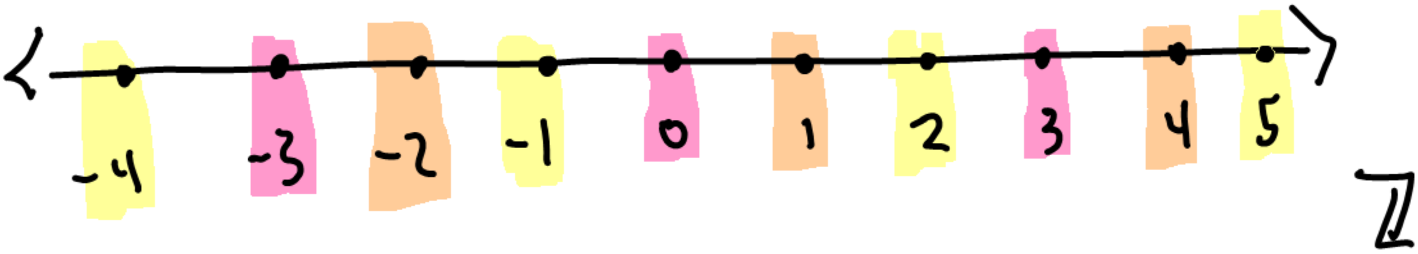
$(x - 6)$ is a mult. of 8

$(x - 6) = m \cdot 8$

$$\boxed{x = m8 + 6}$$

$$\boxed{\{ m \cdot 8 + 6 \ : \ m \in \mathbb{Z} \}}$$

consider mod 3



$$-1 = (-1)\cdot 3 + \underline{2}$$

$$\{x \in \mathbb{Z} : x \equiv 0 \bmod 3\} = \overline{0}$$

$$\{x \in \mathbb{Z} : x \equiv 1 \bmod 3\} = \overline{1}$$

$$\{x \in \mathbb{Z} : x \equiv 2 \bmod 3\} = \overline{2}$$

$$\mathbb{Z}_3 = \text{"integers mod 3"} = \{\, \overline{0}, \overline{1}, \overline{2} \,\}$$

most people ignore / don't write bars!

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

$$1 +_3 2 = 0$$

$$2 +_3 2 = 1$$

$$1 \cdot_3 2 = 2$$

$$2 \cdot_3 2 = 1$$

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

multi. table for $\mathbb{Z}_3$

this works in <u>any</u> $\mathbb{Z}_n$!

ex) $\mathbb{Z}_4$

$3 \cdot_4 2 = 2$

this lets us do arithmetic mod n!

$3 \equiv 3 \mod 4$

$2 \equiv 2 \mod 4$

$a \equiv b \mod n$

$c \equiv d \mod n$

$ac \equiv bd \mod n$

$a \pm c \equiv b \pm d \mod n$

note $2 \cdot_4 2 = 0$

non-zero   zero!

---

in familar sets like $\mathbb{R}$

$ax = b$

if $a \neq 0$, we can solve this by "dividing by a" i.e. by "multiplying by a^{-1}"

ex) $4x = 12$

$\cancel{4^{-1}} \cdot 4x = 4^{-1} \cdot \overset{3}{\cancel{12}}$

$\boxed{x = 3}$

in $\mathbb{Z}_n$

$ax \equiv b \mod n$

if $a \not\equiv 0 \mod n$, then maybe we can find a^{-1} to multiply both sides by!

$\longrightarrow x \equiv a^{-1} \cdot b \mod n$

not all $a \in \mathbb{Z}$ have "mult. inverses" mod n

(warning ex: $2 \in \mathbb{Z}$, 2 has no inv. mod 4 !!)

($2x \equiv 3 \bmod 4$ has no solutions !)

What we actually need:

$$ax \equiv b \bmod n$$

has solutions if & only if

$\gcd(a, n) \mid b$

ex) $2x \equiv 3 \bmod 4$

$\gcd(2,4) = 2 \quad 2 \nmid 3 \longrightarrow$ no solutions

0, 1, 2, 3, 4, 5, 6, 7, 8

ex] $3x \equiv 6 \mod 9$

$\gcd(3,9) = 3$, $3 \mid 6$ ✓

→ are solutions !!!

<u>to find these</u>

1) divide eqn by $\gcd(a,b)$

$$x \equiv 2 \mod 3$$

one solution : $x = 2$

(also have $x=2$, $x=5$, $x=8$, ...)

2) additional solutions

one solution $x_0 + \frac{n}{\gcd(a,n)}$

↓

$$2 + \frac{9}{3} = 5$$

$\boxed{\text{three solutions : } 2, 5, 8}$