LECTURE 3

(Wednesday OCT. 2, 2019)

Congruences.

Fix a positive integer N (the "modulus")

Def. $a, b \in \mathbb{Z}$ are congruent modulo N if

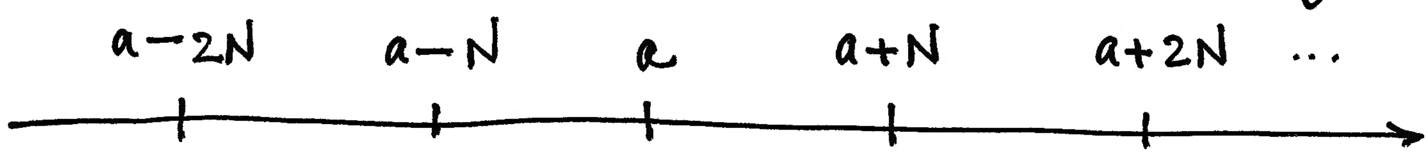
$$N \mid (a-b)$$

- Equivalently a and b have the same remainder "r" upon division by N.

Notation: $a \equiv b \pmod{N}$.

[so this means we can write $b = qN + a$, $q \in \mathbb{Z}$]

— as $q \in \mathbb{Z}$ varies such numbers "b" form an arithmetic progression: (N = step length)



also known as the residue class of a mod N.

Def. $[a] = [a]_N = \{qN + a \mid q \in \mathbb{Z}\}$.

(an infinite subset of $\mathbb{Z}$) $= \{b \in \mathbb{Z} \mid b = qN + a, \text{ some } q \in \mathbb{Z}\}$.

Note: Different a's may give the same residue class, ex. $[0] = \{N\text{-multiples}\} = [N]$.

EX ($N=2$) Only two classes:

$[0] = \{$even numbers$\}$ $\quad (2N)$

$[1] = \{$odd numbers$\}$ $\quad (2N+1)$

Form a partition of $\mathbb{Z}$: Every $x \in \mathbb{Z}$ is even or odd, and not both.

$\mathbb{Z} = [0] \cup [1]$ and $[0] \cap [1] = \emptyset$.

— say they're "disjoint".

Theorem ($N \geq 1$ arbitrary integer)

$\equiv \pmod N$ is an equivalence relation on $\mathbb{Z}$. I.e.,

(i) $a \equiv a \pmod N$ "reflexive"

(ii) $a \equiv b \pmod N \iff b \equiv a \pmod N$ "symmetric"

(iii) $a \equiv b \pmod N$ and $b \equiv c \pmod N$

$\implies a \equiv c \pmod N$

(for all $a, b, c \in \mathbb{Z}$). "transitive"

PROOF. (i) N divides $a-a=0$.

(ii) If $a-b=qN$, then $b-a=(-q)N$.

(iii) If $a-b=q_1N$ and $b-c=q_2N$, then by adding the equations:

$$a-c=(a-b)+(b-c)=\underbrace{(q_1+q_2)}_{\in\mathbb{Z}}N$$

shows $N \mid (a-c)$. $\square$

— recall the residue class:

$$[a]=\{b\in\mathbb{Z} \mid b\equiv a \pmod N\}.$$

reflexive

$[a]$: always contains the element a.

*) Consequence: $[a]=[b] \iff a\equiv b \pmod N$
$(a,b\in\mathbb{Z})$

How? $\Rightarrow$: $b\in[b]$. By assumption $[b]=[a]$
so $b\in[a]$, which means $b\equiv a \pmod N$.

$\Leftarrow$: Our hypothesis is $a\equiv b$. Show an identity between subsets of $\mathbb{Z}$ (two inclusions)

$[a]\subseteq[b]$: Take any $x\in[a]$, i.e. $x\equiv a$.
By transitivity $x\equiv b$, meaning $x\in[b]$.

$[a]\supseteq[b]$: Similar. By symmetry. ✓

- Follows that the residue classes form a partition of $\mathbb{Z}$:

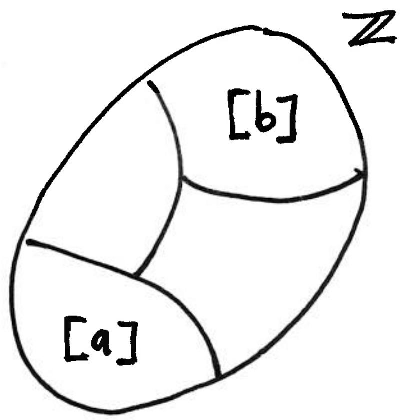
obvious: $x \in [x]$.

- Every $x \in \mathbb{Z}$ belongs to a residue class.

- Two distinct residue classes are disjoint
  - I.e., $[a] \cap [b] \neq \emptyset \implies [a] = [b]$.

(why? Suppose $c \in [a]$ and $c \in [b]$. Then $c \equiv a$ and $c \equiv b$. By (*) we conclude that

$$[a] = [c] = [b].)$$



$\sim$ archiving $\mathbb{Z}$ into N boxes:

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [N-1].$$

EX ($N = 3$)

Remark: $x = qN + r$ with $0 \leq r < N$. Thus $x \in [r]$.

[0]	[1]	[2]
2019	2017	2018
-2019	-2018	-2017

EX (N = 5)

[0]	[1]	[2]	[3]	[4]
2020		2017	2018	2019
−2020	−2019	−2018	−2017	

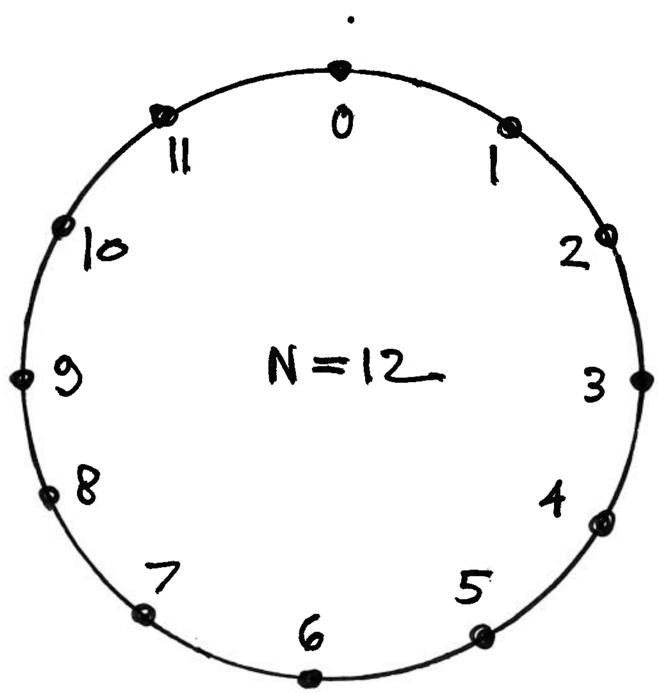
Def. $\mathbb{Z}_N = \{[0], [1], [2], \ldots, [N-1]\}$ .. collection of all N boxes.

a finite set;

– its elements are infinite sets of integers.

$|\mathbb{Z}_N| = N$

Next: Endow $\mathbb{Z}_N$ with addition & multiplication. "clock arithmetic"



EX (N = 12)

$7 + 9 \equiv 4$

$5 \cdot 7 \equiv 11$

$4 \cdot 6 \equiv 0$ — although $4 \not\equiv 0$ and $6 \not\equiv 0$!

"zero – divisors".