LECTURE 4

(Friday OCT. 4, 2019)

GOAL: Define addition & multiplication on the set

$$\mathbb{Z}_N = \{[0], [1], \dots, [N-1]\}$$ "integers mod N".

(collection of all residue classes modulo N).

— idea: How to add two boxes of numbers?

1) Pick a number from each box
2) Add the two numbers
3) Put the sum back in a box. ← the "sum" of the two boxes.

PROBLEM: The resulting box in 3) may depend on the numbers drawn in 1). .... i.e., not well-defined.

EX: Divide $\mathbb{Z}$ into two boxes:

$$A = \{x \in \mathbb{Z} : x > 0\}$$

$$B = \{x \in \mathbb{Z} : x \leq 0\}$$

— What's $A + B$?

- First say we pick $1 \in A$ and $-2 \in B$. Then $1 + (-2) = -1 \in B$.
- On the other hand, picking $2 \in A$ and $-1 \in B$ yields $2 + (-1) = 1 \in A$. — different boxes!

- This issue does not arise for <u>residue classes</u>:

<u>Theorem</u>. Suppose $a \equiv a'$ and $b \equiv b'$ $\pmod N$.
Then: (i) $ab \equiv a'b'$ and
(ii) $a+b \equiv a'+b'$.

- suppress; N is <u>fixed</u>.

<u>PROOF</u> (ii): $(a+b)-(a'+b') =$

$(a-a')+(b-b')$: divisible by N ✓

both multiples of N.

trick

(i) $ab - a'b' = ab - \underbrace{a'b + a'b}_{\text{cancel.}} - a'b'$

$= (a-a')b + a'(b-b')$: divisible by N ✓

N-multiples

$\square$

- This result justifies:

<u>Definition</u>. Two residue classes in $\mathbb{Z}_N$ are added/multiplied by the rules

$[a]+[b] := [a+b]$

$[a]\cdot[b] := [ab]$

(on RHS usual $+$ and $\cdot$ for $\mathbb{Z}$)

- Well-defined:

$$[a]=[a'] \text{ and } [b]=[b'] \overset{\text{using Thm.}}{\Longrightarrow}$$

$$[a+b]=[a'+b'] \text{ and } [ab]=[a'b'].$$ ✓

Observe: $\mathbb{Z}_N$ with $+$ is a group (abelian).

Indeed, the associative law is "inherited" from $\mathbb{Z}$:

- $([a]+[b])+[c] = [a+b]+[c]$

$$= [a+b+c] = [a]+[b+c] = [a]+([b]+[c])$$

- $[a]+\underset{e}{[0]}=[a+0]=[a]$

- $[a]+[-a]=[a+(-a)]=[0].$

$[-a]$ ← the (additive) inverse of $[a]$.

- However, $\mathbb{Z}_N$ with $\bullet$ is not a group:

Associative law holds, $[1]$ is neutral, but $[0]$ has no (multiplicative) inverse — unless $N=1$.

– Taking out $[0]$ may still not yield a group:

<u>Theorem</u>. $[a]$ has a multiplicative inverse in $\mathbb{Z}_N$ exactly when $GCD(a,N) = 1$.

"coprime".

<u>Why?</u> $\Uparrow$: 1st suppose a, N are <u>coprime</u>. Find $x, y \in \mathbb{Z}$ such that $1 = ax + Ny$. Shows $1 \equiv ax \pmod N$. I.e., $[x]$ is an inverse of $[a]$.

$\Downarrow$: Conversely, if $[a] \cdot [x] = [1]$ we conclude $ax \equiv 1 \pmod N$. In other words $1 - ax = Ny$ for some $y \in \mathbb{Z}$. If $d > 0$ divides a, N this shows $d \mid 1$ — and therefore $d = 1$. $\square$

[<u>EXC</u>: If $a, b \in \mathbb{Z}$ are both <u>coprime</u> to N, then so is their product ab.

(Hint: $p \mid ab \Rightarrow p \mid a$ or $p \mid b$)

— Deduce from exercise that $\bullet$ is a composition law on the set

$$\mathbb{Z}_N^\times = \{[a] : \ GCD(a,N) = 1\}.$$

family of all invertible residue classes.

(multiplicative) group of units in $\mathbb{Z}_N$.

Note: $|\mathbb{Z}_N^\times| = \#\{a : 0 \leq a < N, \ GCD(a,N) = 1\}$

$= \phi(N)$ "Euler's totient function".

Special case: $N = p$ prime.

Here every positive $a < p$ is coprime to p, so

$$|\mathbb{Z}_p^\times| = \phi(p) = p - 1.$$

— in other words, in the prime case, $\mathbb{Z}_p^\times$ consists of all nonzero residue classes.

Ex ($N = 6$) $\mathbb{Z}_6^\times = \{[1], [5]\}$.

$[2] \bullet [3] = [0]$. "zero-divisors"