LECTURE 12

(Wed. FEB. 5, 2020)

N=3: (midterm 1)

$A = \{3q : q \in \mathbb{Z}\}$

$B = \{3q+1 : q \in \mathbb{Z}\}$

$C = \{3q+2 : q \in \mathbb{Z}\}$

partition

$\mathbb{Z} = A \cup B \cup C$.

Show: $x \in C \wedge y \in C \Rightarrow xy \in B$.

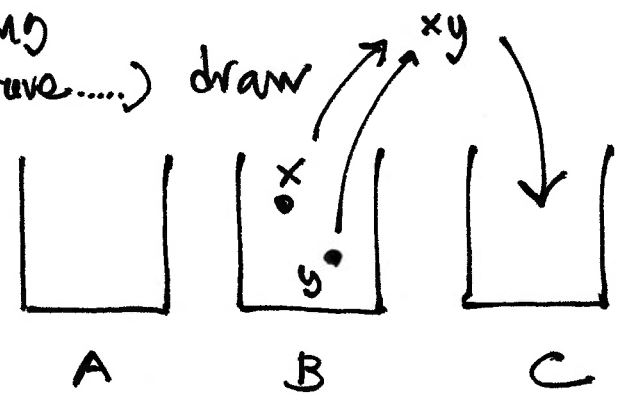
- How? $x = 3p+2$ and $y = 3q+2$, some $p, q \in \mathbb{Z}$.

Then, $xy = (3p+2)(3q+2) = 9pq + 6p + 6q + 4$

$= 3(\underbrace{3pq+2p+2q+1}_{\text{integer}}) + 1$

- visibly in B.

(wrong picture.....) draw



"$C \cdot C = B$"

Same for any choice of two boxes. (similarly for +)

- multiplication table:

·	A	B	C
A	A	A	A
B	A	B	C
C	A	C	B

- addition table:

+	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

D E

N=5 $Z = A \cup B \cup C \cup E \cup F$ (new A, B, C !)

$A = \{5q : q \in \mathbb{Z}\} = [0]$

$B = \{5q+1 : q \in \mathbb{Z}\} = [1]$

$C = \{5q+2 : q \in \mathbb{Z}\} = [2]$

$D = \{5q+3 : q \in \mathbb{Z}\} = [3]$

$E = \{5q+4 : q \in \mathbb{Z}\} = [4]$.

"$C \cdot D = B$"

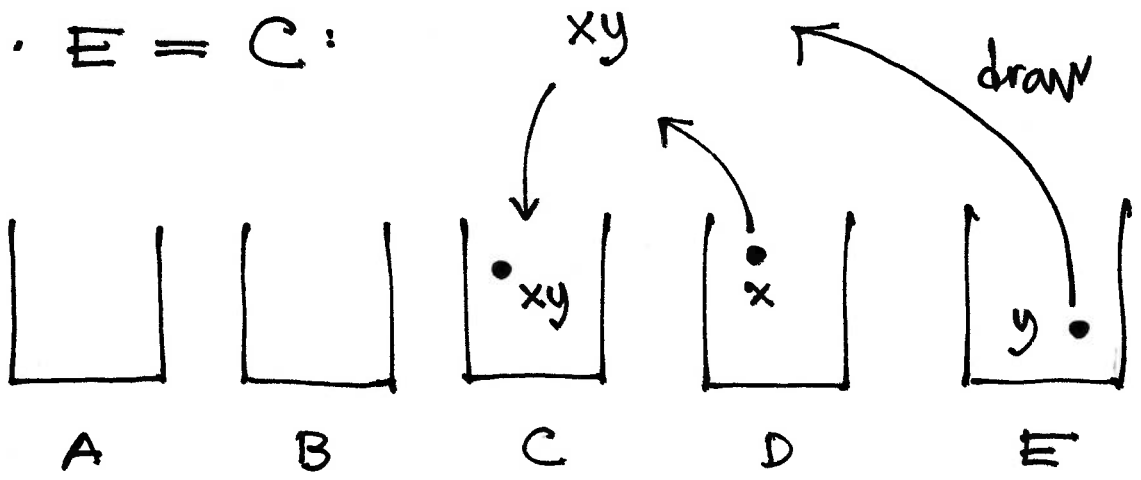
Here, $x \in C \wedge y \in D \Longrightarrow xy \in B$.

$xy = (5p+2)(5q+3) = 25q^2 + 15p + 15q + 6$

$= 5(\underbrace{5q^2 + 3p + 3q + 1}_{\text{in } \mathbb{Z}}) + 1$

(similarly $C + D = A$).

$D \cdot E = C$:

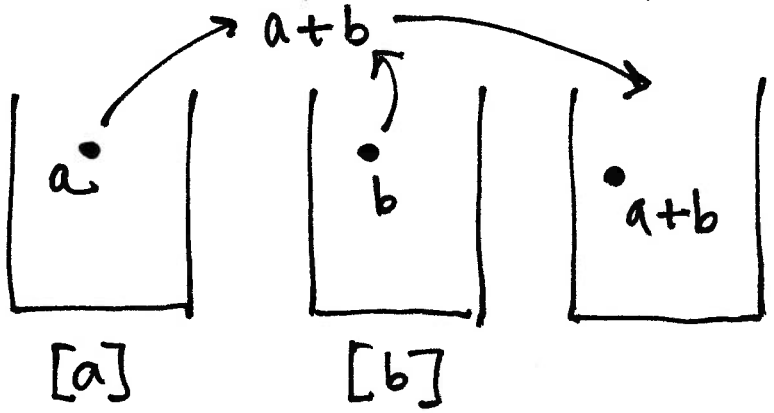


~ How to add & multiply boxes? Define + and · on $\mathbb{Z}_N$.

Def. $[a] + [b] = [a+b]$

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

Well-defined? RHS indep. of the choice of representatives $a, b \in \mathbb{Z}$?



Need to check: if $[a] = [a']$ and $[b] = [b']$,

then $[a+b] = [a'+b']$ and $[ab] = [a'b']$.

(Ex, cont.: $N=12$ $[5] = [17]$ and $[8] = [-4]$. Should have

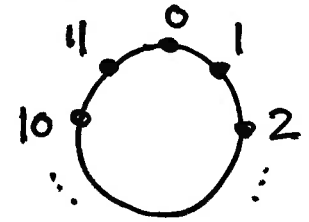
$[17] + [-4] \overset{\checkmark}{=} [1]$ and $[17] \cdot [-4] \overset{\checkmark}{=} [4]$)

— in other words, must verify:

$-68 = (-6) \cdot 12 + 4$

$$a \equiv a' \pmod N \wedge b \equiv b' \pmod N \Rightarrow \begin{cases} a+b \equiv a'+b' \pmod N \text{ and} \\ ab \equiv a'b' \pmod N \end{cases}$$

Ex ($N=12$ "clock")



$[5] + [8] = [13]$

$= [1]$

$[5] \cdot [8] = [40]$

$= [4]$.

$(40 = 3 \cdot 12 + 4)$

Know: $a' = a + sN$ and $b' = b + tN$, some $s, t \in \mathbb{Z}$.

Thus,

$$(a+b) - (a'+b') = (a-a') + (b-b') = (s+t)N$$

and

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= (a-a')b + a'(b-b') \\ &= (sb + a't)N. \end{aligned}$$

cf. Problem on MT1 w. $N=3$, $\mathbb{Z} = A \cup B \cup C$.

Both are multiples of N.

Exc. Usual arithmetic laws hold for $\mathbb{Z}_N$ with $+$ and $\cdot$. (associative etc.)

Application: $a \equiv b \pmod N \Rightarrow a^n \equiv b^n \pmod N$ for all $n \in \mathbb{N}$.

Ex. ($N = 3$, 10) $10 \equiv 1 \pmod 3$ so

$$10^n \equiv 1 \pmod 3.$$

$$\underbrace{a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n}_{x} \equiv \underbrace{a_0 + a_1 + a_2 + \cdots + a_n}_{\text{sum of the digits of } x.} \pmod 3$$

Shows $3 \mid x$ if and only if 3 divides $\sum_{i=0}^{n} a_i$.

$3 \nmid 2020$ since $\Sigma = 4$

$3 \mid 2019$ since $\Sigma = 12$.

Ex ($N=11$) $10 \equiv -1 \pmod{11}$

$10^n \equiv (-1)^n \pmod{11}$

$$\underbrace{a_0 + a_1 10 + \cdots + a_n 10^n}_{x} \equiv \underbrace{a_0 - a_1 + a_2 - \cdots + (-1)^n a_n}_{\text{alternating sum of digits.}} \pmod{11}$$

Shows $11 \mid x$ exactly when 11 divides $\sum_{i=0}^{n} (-1)^i a_i$.

($11 \mid 737$ since 11 divides $7-3+7=11$)

Ex What can go wrong? Suppose we instead partition $\mathbb{Z}$ into two boxes:

$$A = \{x \in \mathbb{Z} : x > 1\}$$
$$B = \{x \in \mathbb{Z} : x \leq 1\}.$$

~ What's $A+B$?

1) Select $2 \in A$ and $1 \in B$. Then

$$2 + 1 = 3 \in \underline{\underline{A}}.$$

2) Select $5 \in A$ and $-7 \in B$. Then

$$5 + (-7) = -2 \in \underline{\underline{B}}.$$

(resulting box depends on the choice of representatives)