LECTURE 11

(Mon. FEB. 3, 2020)

– Why N boxes?

Division Algorithm: For any two integers $a, N \in \mathbb{Z}$ with $N > 0$, there are unique $q, r \in \mathbb{Z}$ sat. the two conditions below simultaneously:

$$\begin{cases} (1) & a = qN + r, \quad \text{and} \\ (2) & 0 \leq r < N. \end{cases}$$

PROOF. Ignoring (2) at first, look at the set of all possible remainders:

$$A = \{a - qN : q \in \mathbb{Z}\}.$$

Obviously $a \in A$ so certainly $A \neq \emptyset$. (take $q = 0$)

– Stronger: $A \cap \mathbb{N} \neq \emptyset$

(if $a \leq 0$ consider $a - qN$ for negative q).

Ex ($N = 10$)

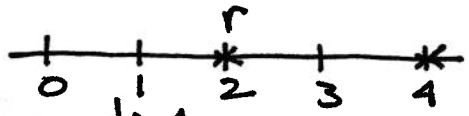
$25 = 2 \cdot 10 + 5$

$= 3 \cdot 10 + (-5)$

$= 1 \cdot 10 + 15$

$\vdots$

$A = \{\cdots -5, 5, 15 \cdots\}$



Let r be the smallest non-negative integer in A (cf. "well-ordering principle" — to be discussed later)

Write $r = a - qN$.

CLAIM: $r < N$

(so the pair q, r works)

any non-empty $S \subseteq \mathbb{N}$ has a smallest element.

For suppose (sake of contradiction) that $r \geq N$. Then

$$r - N = a - qN - N = a - (q+1)N$$

is non-negative and in A. By minimality of r, must have $r \leq r - N$. I.e., $N \leq 0$.

— contradiction (we've assuming $N > 0$)

— This shows the existence of q, r.

- Uniqueness: Suppose $\tilde{q}, \tilde{r}$ is another pair sat. (1) & (2). Then:

$$r - \tilde{r} = (a - qN) - (a - \tilde{q}N) = (\tilde{q} - q)N \qquad (*)$$

is a multiple of N,

and

$$r - \tilde{r} \leq r < N.$$

↑ since $\tilde{r} \geq 0$

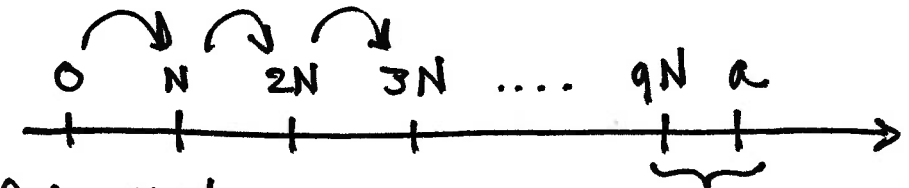
Similarly $\tilde{r} - r \leq \tilde{r} < N$. Conclude:

$r - \tilde{r}$ is a multiple of N in the interval $(-N, N)$.

Must be 0. $r - \tilde{r} = 0$.

I.e., $r = \tilde{r}$ and therefore also

↳ by $(*)$ $q = \tilde{q}$. □



- steps of length N towards a (starting at 0).

q = # steps.

Ex ($N = 100$) $2020 = 1 \cdot 100 + 1920$

$= 2 \cdot 100 + 1820$

$\vdots$

$= 19 \cdot 100 + 120$

$= 20 \cdot 100 + \boxed{20}$ smallest ≥ 0.

$= 21 \cdot 100 + (-80)$

$\vdots$

N boxes: Have shown that $\forall a \in \mathbb{Z}$ there's a unique $r \in \mathbb{Z}$ in the range $0 \leq r < N$:

$$a \equiv r \pmod{N}.$$

— & the boxes are

$$\{[0], [1], [2], \ldots, [N-1].\} = \mathbb{Z}_N.$$

($\mathbb{Z}_N$ is a finite set whose elements are infinite sets of integers)

NOT a subset of $\mathbb{Z}$, $\mathbb{Z}_N$ is a subset of $\mathcal{P}(\mathbb{Z})$.