4460

3/5/25

Def: Let $n \in \mathbb{Z}$, $n \geq 2$.
Let $x \in \mathbb{Z}$.
The equivalence class of x modulo n is

$$\overline{x} = \{ y \in \mathbb{Z} \mid y \equiv x \pmod{n} \}$$

For computing, by 5 of the theorem from last time:

$$\overline{x} = \{ \ldots, x-3n, x-2n, x-n, x, x+n, x+2n, x+3n, \ldots \}$$

Ex: Let $n=2$

$\overline{0} = \{ y \in \mathbb{Z} \mid y \equiv 0 \pmod 2 \}$

$= \{ \ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots \}$

$\overline{1} = \{ y \in \mathbb{Z} \mid y \equiv 1 \pmod 2 \}$

$= \{ \ldots, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots \}$

$\overline{2} = \{ y \in \mathbb{Z} \mid y \equiv 2 \pmod 2 \}$

$= \{ \ldots, -4, -2, 0, 2, 4, 6, 8, \ldots \} = \overline{0}$

$\overline{3} = \{ y \in \mathbb{Z} \mid y \equiv 3 \pmod 2 \}$

$= \{ \ldots, -3, -1, 1, 3, 5, 7, 9, \ldots \}$

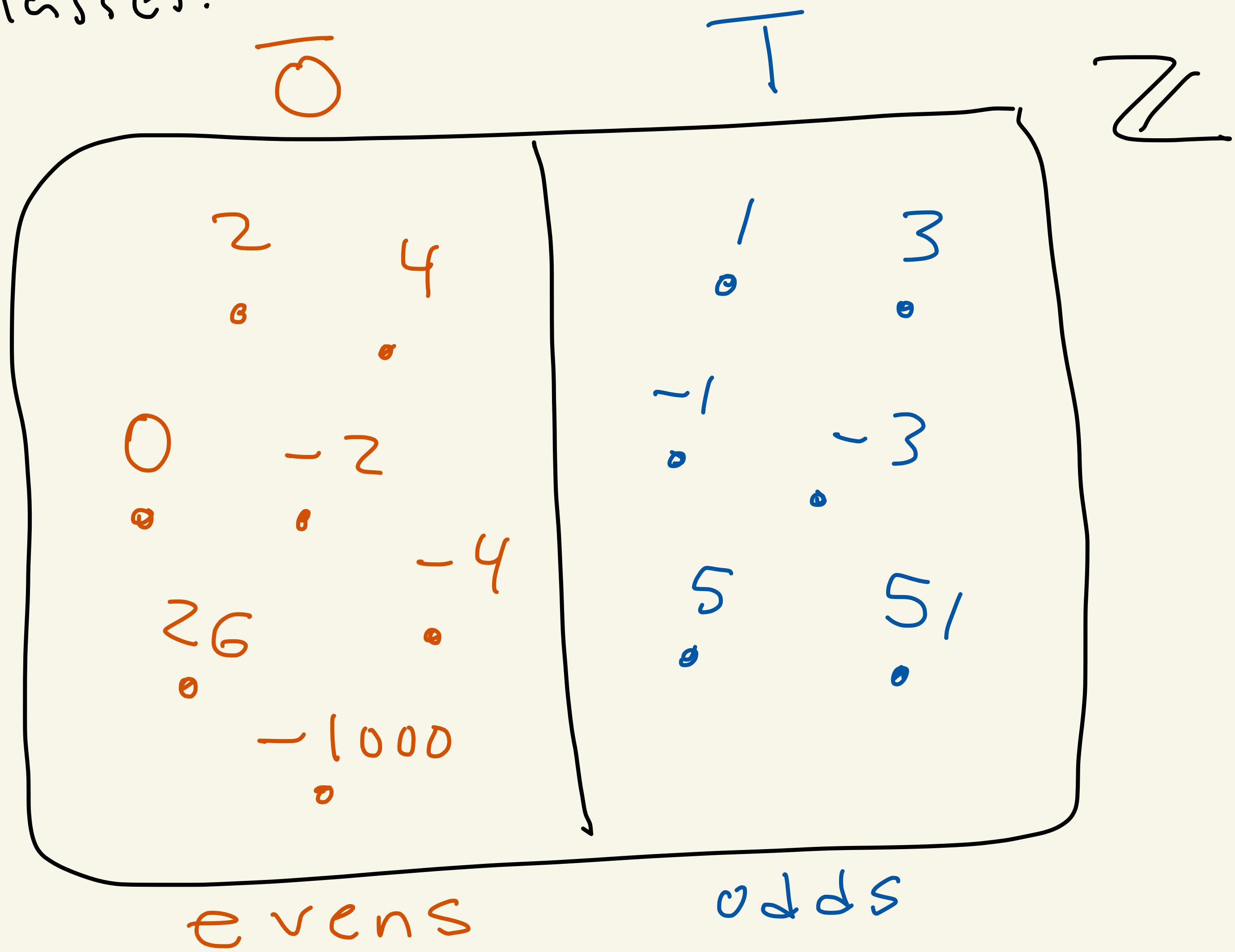
$= \overline{1}$

Note:

$\overline{0} = \overline{2} \leftarrow \boxed{2 \in \overline{0}}$ & $\boxed{2 \equiv 0 \pmod{2}}$

$\overline{1} = \overline{3} \leftarrow \boxed{3 \in \overline{1}}$ & $\boxed{3 \equiv 1 \pmod{2}}$

Modulo $n=2$ breaks the integers $\mathbb{Z}$ into two disjoint equivalence classes.



<u>Ex:</u> Let $n=3$

$$\bar{0} = \{y \in \mathbb{Z} \mid y \equiv 0 \pmod 3\}$$
$$= \{\dots -9, -6, -3, 0, 3, 6, 9, \dots\}$$

$$\bar{1} = \{y \in \mathbb{Z} \mid y \equiv 1 \pmod 3\}$$
$$= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$$

$$\bar{2} = \{y \in \mathbb{Z} \mid y \equiv 2 \pmod 3\}$$
$$= \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

$$\bar{3} = \{y \in \mathbb{Z} \mid y \equiv 3 \pmod 3\}$$
$$= \{\dots, -6, -3, 0, 3, 6, 9, 12, \dots\} = \bar{0}$$

$\bar{3} = \bar{0}$ & $3 \equiv 0 \pmod 3$ & $3 \in \bar{0}$

What will $\overline{7}$ equal?

$\overline{7} = \{\dots, -5, -2, 1, 4, 7, 10, 13, \dots\} = \overline{1}$

Note: $7 \in \overline{1}$ and $7 \equiv 1 \pmod{3}$

Modulo $n = 3$ breaks $\mathbb{Z}$ into 3 equivalence classes: $\overline{0}, \overline{1}, \overline{2}$

$\overline{0}$	$\overline{1}$	$\overline{2}$
6	7	8
3	4	5
0	1	2
-3	-2	-1
-6	-5	-4
333	334	335
$0 + 3k$	$1 + 3k$	$2 + 3k$

$\mathbb{Z}$

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $x, y \in \mathbb{Z}$.

(1) Either $\underbrace{\overline{x} \cap \overline{y} = \phi}_{\text{no overlap}}$ or $\overline{x} = \overline{y}$

disjoint

(2) $\overline{x} = \overline{y}$

iff $x \equiv y \pmod{n}$

iff $x \in \overline{y}$ ← (or $y \in \overline{x}$)

(3) A complete set of distinct equivalence classes modulo n is given by $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$

That is, if $z \in \mathbb{Z}$, then $\overline{z} = \overline{r}$ for a unique integer r with $0 \leq r \leq n-1$. Moreover, r is the remainder when you divide z by n.

Ex: $n = 3$

equivalence classes: $\bar{0}, \bar{1}, \bar{2}$

$z = 1051$

$\bar{z} = \overline{1051}$

$= \bar{1}$

$$\begin{array}{r} 350 \\ 3 \,\big)\,\overline{1051} \\ -9 \\ \hline 15 \\ -15 \\ \hline 01 \\ -0 \\ \hline 1 \end{array}$$

n

remainder

Proof: 1 and 2 are in HW.

Let's prove 3

Let $n \in \mathbb{Z}$, $n \geq 2$.

Let $z \in \mathbb{Z}$.

By the division algorithm

$$z = qn + r$$

divide n into z

where $\underbrace{0 \le r \le n-1}_{0 \le r < n}$.

Then, $z - r = qn$.

So, $n \mid (z-r)$

Thus, $z \equiv r \pmod{n}$

and $0 \le r \le n-1$.

By part 2 we get $\overline{z} = \overline{r}$

with $0 \le r \le n-1$.

So, $\overline{z}$ is one of $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$

So, all the equivalence classes modulo n are amongst

$\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$

Let's show that none of

$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$

are equal to each other.

Suppose $0 \leq a \leq b \leq n-1$ and $\overline{a} = \overline{b}$

We will show $a = b$.

Since $a \leq b \leq n-1$ we get

$$0 \leq b-a \leq n-1-a$$

So, $0 \leq b-a \leq n-1-a \leq n-1$

Thus, $\boxed{0 \leq b-a \leq n-1}$.

Since $\overline{a} = \overline{b}$, by 2, we know

$$a \equiv b \pmod{n}.$$

So, $\boxed{n \mid (b-a)}$.

Since $n \mid (b-a)$ and $0 \leq b-a < n$
we must have, by topic 1,
that $b-a=0$.

So, $b=a$.

Thus, $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$
are the unique equivalence
classes modulo n.

$\blacksquare$

Def: Let $n \in \mathbb{Z}$, $n \geq 2$.

Define

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

$\mathbb{Z}_n$ is called the set of integers modulo n.

Ex:

$$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$$

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

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

$$\vdots \qquad \qquad \vdots$$