Math 3450
2/15/24

Def: Let $a, b \in \mathbb{Z}$ ← integers

We say that a **divides** b if there exists $k \in \mathbb{Z}$ where $b = ak$. If a divides b then we write $a \mid b$.

If a does not divide b then we write $a \nmid b$.

Ex: $3 \mid 12$ because $12 = 3 \cdot \underbrace{4}_{k}$

Ex: $(-4) \mid 12$ because

$$12 = (-4)\underbrace{(-3)}_{k}$$

Ex: $12 \nmid 3$ because the only sol to $3 = 12 \cdot k$ would be $k = \frac{3}{12} = \frac{1}{4}$ and $\frac{1}{4} \notin \mathbb{Z}$

Def: Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. We say that a and b are congruent modulo n if $n \mid (a-b)$. If this is the case then we write $a \equiv b \pmod{n}$ and if not then we write $a \not\equiv b \pmod{n}$.

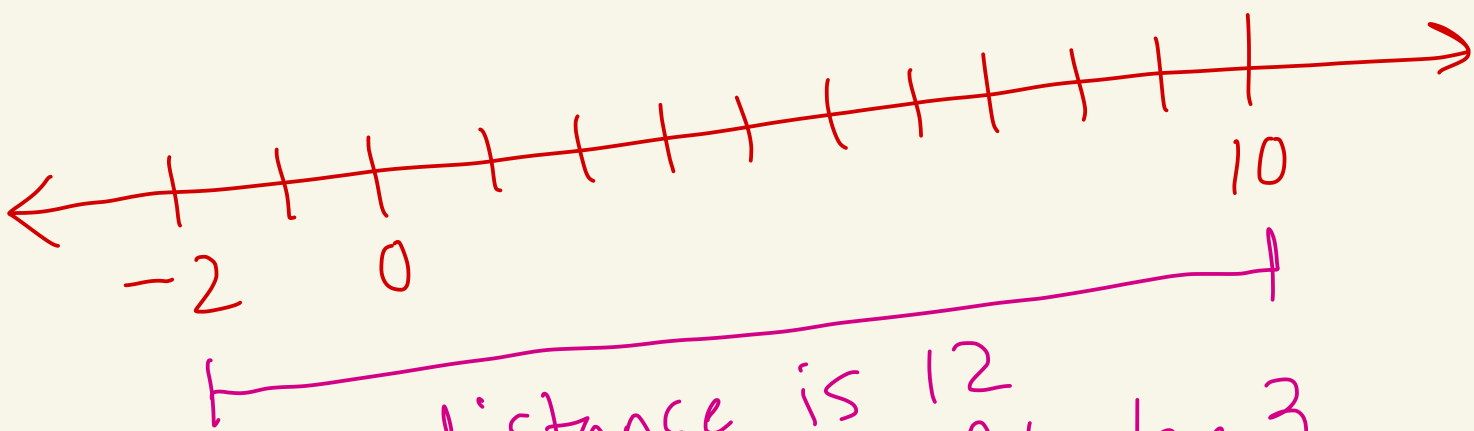
Ex: Let $n = 3$.

Q: Is -2 congruent to 10 modulo 3?

We have
$$(-2)-(10) = -12 = 3\cdot(-4)$$

So, $3 \mid ((-2)-10)$.

Thus, $-2 \equiv 10 \pmod{3}$.



distance is 12
which is divisible by 3

Q: Is 3 congruent to 127 modulo 3?

We have

$$3 - 127 = -124$$

And $3 \nmid -124$.

Thus, $3 \not\equiv 127 \pmod{3}$

$$\begin{array}{r} 41 \\ 3\overline{)124} \\ -12 \\ \hline 04 \\ -3 \\ \hline 1 \end{array}$$

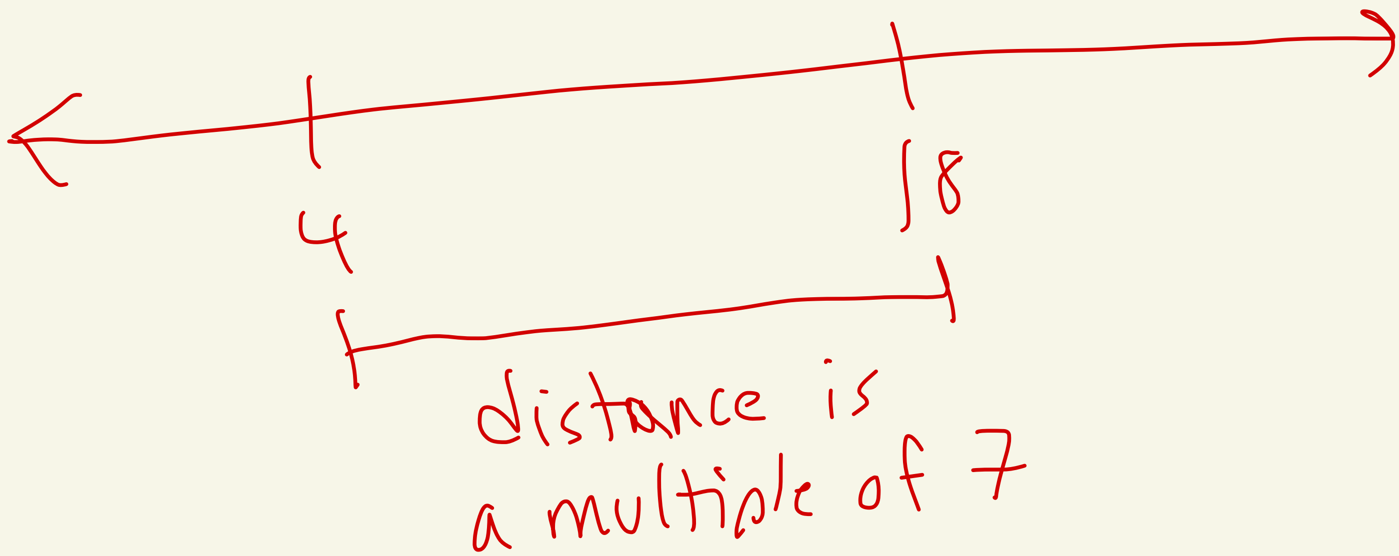
distance is 124
which is not
divisible by 3

Ex: Is $4 \equiv 18 \pmod{7}$?

Yes, because

$$4-18=-14=7\cdot(-2).$$

Ie, $7 \mid (4-18)$.



<u>Theorem:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.

Then, mod n is an equivalence relation on $\mathbb{Z}$. That is,

① (reflexive)

$a \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$.

② (symmetric)

If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

③ (transitive)

If $a, b, c \in \mathbb{Z}$ and $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

proof:

$x \equiv y \pmod{n}$ means $x - y = nk$ for some $k \in \mathbb{Z}$

① Let $a \in \mathbb{Z}$.

We have

$$a - a = 0 = n \cdot 0.$$

Thus, $n \mid (a-a)$.

Hence, $a \equiv a \pmod{n}$.

② Let $a, b \in \mathbb{Z}$.

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

Then, $n \mid (a-b)$.

That is, $a - b = nk$ where $k \in \mathbb{Z}$.

Multiply by -1 gives

$$b - a = n\underbrace{(-k)}_{-k \in \mathbb{Z} \text{ since } k \in \mathbb{Z}}.$$

Hence $n \mid (b-a)$.
Therefore $b \equiv a \pmod{n}$.

③ Let $a, b, c \in \mathbb{Z}$.
Suppose $a \equiv b \pmod{n}$
and $b \equiv c \pmod{n}$.
Then, $n \mid (a-b)$ and $n \mid (b-c)$.
Thus, $a-b = nk_1$ and $b-c = nk_2$
where $k_1, k_2 \in \mathbb{Z}$.
It follows that

$$\begin{aligned} a-c &= (b+nk_1)-(b-nk_2) \\ &= nk_1+nk_2 \\ &= n\underbrace{(k_1+k_2)}_{k_1+k_2 \in \mathbb{Z} \text{ since } k_1, k_2 \in \mathbb{Z}} \end{aligned}$$

Thus, $n \mid (a-c)$

So, $a \equiv c \pmod{n}$. $\blacksquare$

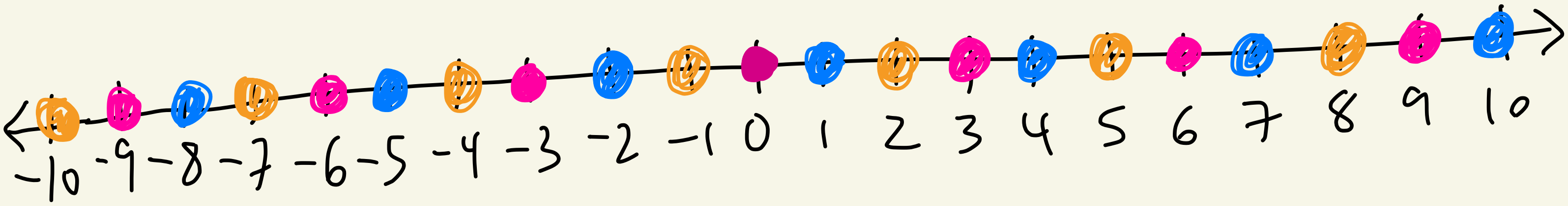
Def: Let $n \in \mathbb{Z}$ with $n \geq 2$. We denote the set of equivalence classes modulo n as $\mathbb{Z}_n$.

Previously, if $\sim$ was an equivalence relation on S, then the set of equivalence classes was denoted $S/\sim$

Some people write $\mathbb{Z}/n\mathbb{Z}$ instead of $\mathbb{Z}_n$

4550

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



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

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

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

By the super-duper equiv. relation thm

$$\overline{3} = \overline{0} = \overline{6} = \overline{9} = \overline{-9} = \dots$$

$$\overline{1} = \overline{-8} = \overline{1} = \overline{7} = \cdots$$

$$\overline{2} = \overline{-4} = \overline{-1} = \overline{5} = \overline{8} = \cdots$$

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

set of equivalence classes mod 3

We partitioned $\mathbb{Z}$ into 3 pieces: