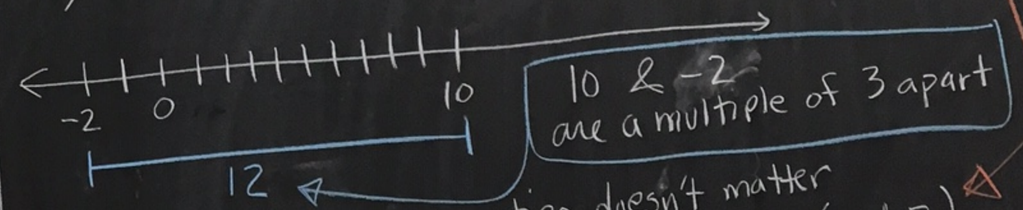
9/16
Monday

Def: Let $a, b \in \mathbb{Z}$. We say that a *divides* b if there exists $k \in \mathbb{Z}$ with $ak = b$. We write $a \mid b$ to mean that a divides b.
If a doesn't divide b we write $a \nmid b$.

Ex: $2 \mid 12$ since $12 = (2)(6)$, with $k = 6$

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 so then we write $a \equiv b \pmod{n}$.
If $n \nmid (a-b)$ we write
$a \not\equiv b \pmod{n}$

Ex: $n = 3$
Are -2 and 10 congruent modulo 3?
$(-2) - 10 = -12 \leftarrow 3 \mid (-12)$ since $-12 = 3(-4)$
So, $-2 \equiv 10 \pmod{3}$



Note: The order of subtraction doesn't matter
$10 - (-2) = 12 \leftarrow 3 \mid 12$ so $10 \equiv -2 \pmod{3}$

Ex: $n=3$

$10 \not\equiv 2 \pmod 3$

$10-2=8$ is not divisible by 3.

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$. Modulo n is an equivalence relation. That is,

1. $a \equiv a \pmod n$ for all $a \in \mathbb{Z}$.
2. If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
3. If $a, b, c \in \mathbb{Z}$ and $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

2.

on.

),

n).

proof:

① Let $a \in \mathbb{Z}$.
Then,
$a - a = 0 = n \cdot 0$.
So $a \equiv a \pmod{n}$.

② Let $a, b \in \mathbb{Z}$.
Assume that $a \equiv b \pmod{n}$.
Then $n \mid (a-b)$.
So, $a - b = nk$ for some $k \in \mathbb{Z}$.

Multiply by (-1) to get
$b - a = n(-k)$.
So, $n \mid (b-a)$.
Thus, $b \equiv a \pmod{n}$.

③ Let $a, b, c \in \mathbb{Z}$.
Assume that $a \equiv b \pmod{n}$
and $b \equiv c \pmod{n}$.
So, $n \mid (a-b)$
and $n \mid (b-c)$.

So there exists $k, \ell \in \mathbb{Z}$
with $a - b = nk$ and $b - c = n\ell$.
Adding the equations gives
$a - c = nk + n\ell$.

So,
$a - c = n[k + \ell]$.

Since $k + \ell \in \mathbb{Z}$ we get $n \mid (a-c)$.
Therefore, $a \equiv c \pmod{n}$.

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

-9

Previously:

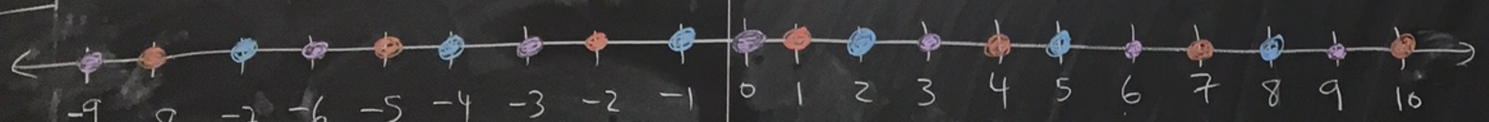
$\sim$ is an equivalence relation on S. The set of equivalence classes was denoted $S/\sim$.

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

2.

Ex: Calculate $\mathbb{Z}_3$ (ie the equivalence classes modulo 3)

So, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.



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

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

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

Use the super-duper equivalence class Theorem

$\bar{2} = \bar{5}$ since $2 \equiv 5 \pmod 3$

OR

$\bar{2} = \bar{5}$ since $5 \in \bar{2}$

$\mathbb{Z}$

... -9 -6 -3 0 3 6 9 ...	$\bar{0}$
... -8 -5 -2 1 4 7 10 ...	$\bar{1}$
... -7 -4 -1 2 5 8 11 ...	$\bar{2}$

Congruence modulo 3 breaks $\mathbb{Z}$ into 3 disjoint equivalence classes: $\bar{0}, \bar{1}, \bar{2}$

Division Algorithm on $\mathbb{Z}$

Let $a, b \in \mathbb{Z}$ and $a > 0$.
There exist unique integers q and r with

$$b = aq + r$$

and

$$0 \leq r < a.$$

Ex: $a = 5$, $b = 17$

$$17 = 5(3) + 2$$

3: q; 2: r; $0 \leq 2 < 5$, $0 \leq r < a$

$a = 5$
$b = -17$

$-17 = 5(-3) - 2$ doesn't work since r is negative

$-17 = 5(-4) + 3$
$a\,q + r$
$0 \leq r < a$

division algorithm

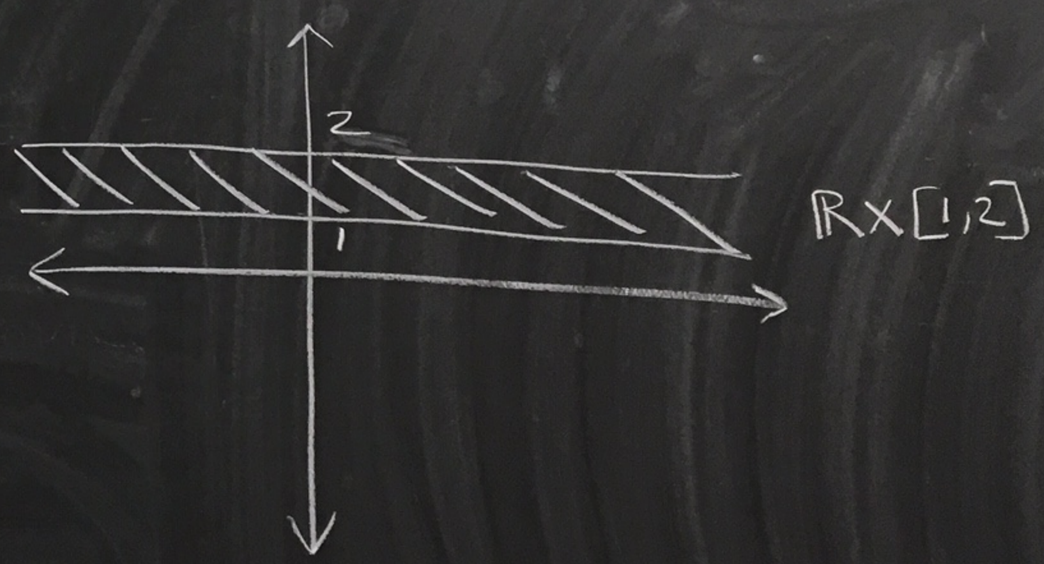
Hammock book 1.8

(7) (a) $\bigcup_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1]$

(b) $\bigcap_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1]$

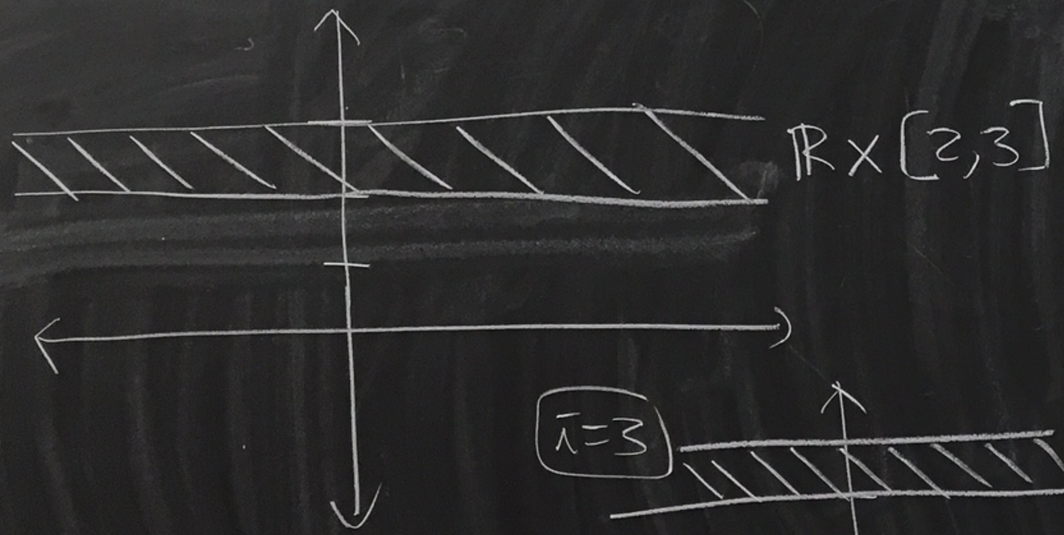
$i = 1$

$\mathbb{R} \times [1,2] = \{(x,y) \mid \begin{matrix} x \in \mathbb{R} \\ y \in [1,2] \end{matrix}\}$

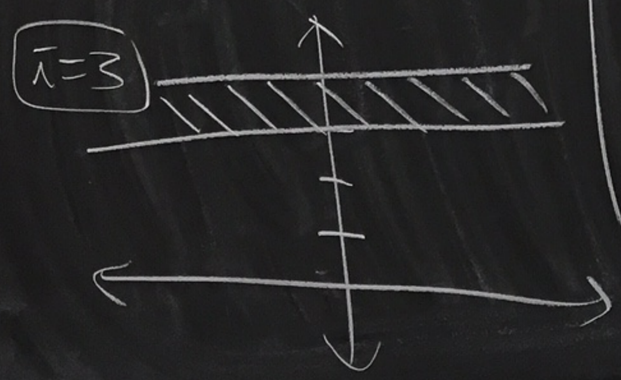


$\tilde{x}=2$

$R\times[2,3]=\{(x,y)\mid x\in R,\ y\in[2,3]\}$

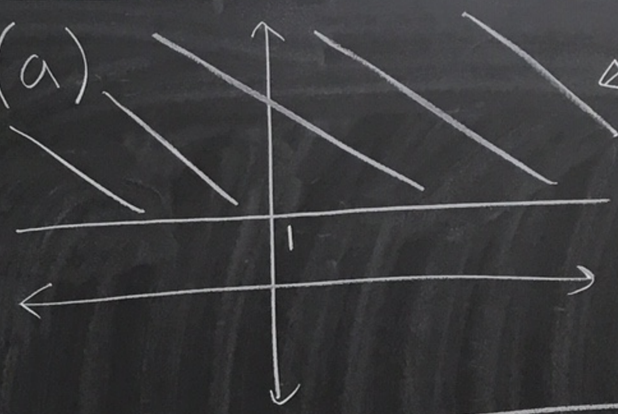


$\tilde{x}=3$



Answers

(a)



$\{(x,y)\mid x\in R,\ y\geq 1\}$

$=R\times[1,\infty)$

(b) $\emptyset$