Topic 2

Equivalence relations

Def: Let S be a set. A relation $\sim$ on S is a subset of $S \times S$.
If (a,b) an element of $\sim$ then we say that a is related to b and write $a \sim b$.
Otherwise we say that a is not related to b and write $a \nsim b$.

Note: Normally we just give a formula to define $\sim$ and don't treat it as a subset of $S \times S$.

<u>Ex:</u> Define a relation $\sim$ on $S = \mathbb{Z}$ where $a \sim b$ means $a \leq b$.

For example, $5 \sim 11$ since $5 \leq 11$.

And $-10 \sim 3$ since $-10 \leq 3$.

But $3 \not\sim -10$ since $3 \not\leq -10$

Formally you can think of

$$\leq \; = \{ (5,11), (-10,3), (2,20), (1,3), \ldots \}$$

means $5 \leq 11$

means $-10 \leq 3$

means $2 \leq 20$

means $1 \leq 3$

but we won't do this.

<u>Ex:</u> Define a relation $\sim$ on $\mathbb{Z}$ where $a \sim b$ means that $|a| = |b|$.

For example,

$5 \sim (-5)$ since $|5| = |-5|$

$2 \sim 2$ since $|2| = |2|$

$-2 \sim 2$ since $|-2| = |2|$

$7 \not\sim 3$ since $|7| \neq |3|$

$4 \not\sim -10$ since $|4| \neq |-10|$

Def: Let S be a set and $\sim$ be a relation on S. We say that $\sim$ is an equivalence relation on S if three properties hold:

1. (reflexive) $a \sim a$ for all $a \in S$
2. (symmetric) If $a, b \in S$ and $a \sim b$, then $b \sim a$.
3. (transitive) If $a, b, c \in S$ and $a \sim b$ and $b \sim c$, then $a \sim c$.

<u>Def</u>: Suppose that $\sim$ is an equivalence relation on S. Given $x \in S$, define the <u>equivalence class</u> of x to be

$$\overline{x} = \{ y \mid y \in S \text{ and } \underbrace{x \sim y} \}$$

could also put $y \sim x$ here since $\sim$ is symmetric

Denote the set of all equivalence classes by $S/\sim$.

Ex: Consider the relation $\leq$ on $\mathbb{Z}$.

$\leq$ is reflexive on $\mathbb{Z}$ since $a \leq a$ for all $a \in \mathbb{Z}$.

$\leq$ is not symmetric on $\mathbb{Z}$ since for example $3 \leq 5$ but $5 \not\leq 3$.

$\leq$ is transitive on $\mathbb{Z}$ since if $a \leq b$ and $b \leq c$, then $a \leq c$.

So, $\leq$ is not an equivalence relation on $\mathbb{Z}$.

Ex: Consider $\sim$ on $\mathbb{Z}$ where $a \sim b$ means $|a| = |b|$.

$$\boxed{\text{Claim: } \sim \text{ is an equivalence relation on } \mathbb{Z}.}$$

proof:

(reflexive) Let $a \in \mathbb{Z}$.
Then $|a| = |a|$.
So $a \sim a$.

(symmetric) Let $a, b \in \mathbb{Z}$ with $a \sim b$.
Then $|a| = |b|$.
So, $|b| = |a|$.
Thus, $b \sim a$

(transitive) Let $a, b, c \in \mathbb{Z}$ with $a \sim b$ and $b \sim c$.

Then $|a| = |b|$ and $|b| = |c|$.

Thus, $|a| = |b| = |c|$.

So, $a \sim c$.

$\boxed{\text{claim}}$

Let's compute some equivalence classes for $\sim$.

$$\begin{aligned}\overline{0} &= \{y \mid y \in \mathbb{Z} \text{ and } 0 \sim y\} \\ &= \{y \mid y \in \mathbb{Z} \text{ and } \underbrace{0 = |y|}_{|0| = |y|}\} \\ &= \{0\}\end{aligned}$$

$$\begin{aligned}\overline{1} &= \{y \mid y \in \mathbb{Z} \text{ and } 1 \sim y\} \\ &= \{y \mid y \in \mathbb{Z} \text{ and } \underbrace{1 = |y|}_{|1| = |y|}\} \\ &= \{1, -1\}\end{aligned}$$

$$\overline{-1} = \{ y \mid y \in \mathbb{Z} \text{ and } -1 \sim y \}$$

$$= \{ y \mid y \in \mathbb{Z} \text{ and } \underbrace{1 = |y|}_{|-1| = |y|} \}$$

$$= \{ 1, -1 \}$$

$$\overline{2} = \{ y \mid y \in \mathbb{Z} \text{ and } \underbrace{|y| = 2}_{y \sim 2} \}$$

$$= \{ -2, 2 \}.$$

$$\overline{-2} = \{ y \mid y \in \mathbb{Z} \text{ and } \underbrace{|y| = 2}_{\substack{y \sim 2 \\ |y| = |-2|}} \}$$

$$= \{ -2, 2 \}$$

So we have the following:

$$\downarrow$$

$\overline{0} = \{0\}$

$\overline{1} = \{1, -1\} = \overline{-1}$

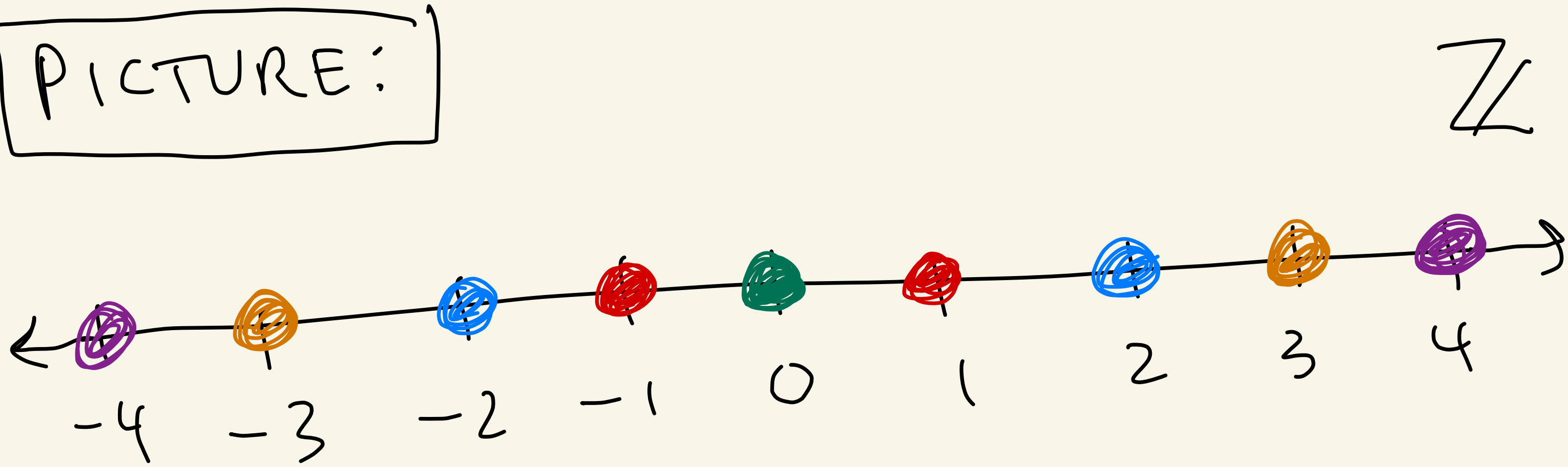
$\overline{2} = \{2, -2\} = \overline{-2}$

$\overline{3} = \{3, -3\} = \overline{-3}$

$\overline{4} = \{4, -4\} = \overline{-4}$

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

$\boxed{\text{PICTURE:}}$



The set of equivalence classes is

$$\mathbb{Z}/\sim \; = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \ldots\}$$

Super-duper Equivalence relation theorem

Let $\sim$ be an equivalence relation on a set S.

Let $x, y \in S$.

Then:

① $x \in \overline{x}$

② $\overline{x} = \overline{y}$ iff $x \in \overline{y}$

③ $\overline{x} = \overline{y}$ iff $x \sim y$

④ $\overline{x} \cap \overline{y} = \phi$ iff $x \nsim y$

Ex from above

① $2 \in \overline{2}$

$\overline{2} = \{2, -2\}$

② / ③

$\overline{1} = \{1, -1\} = \overline{-1}$

$-1 \in \overline{1}$

$-1 \sim 1$

④

$\overline{1} = \{1, -1\}$

$\overline{2} = \{2, -2\}$

$\overline{1} \cap \overline{2} = \phi$

$1 \nsim 2$

<u>proof:</u>

① We Know $\overline{x} = \{y \in S \mid x \sim y\}$

Since $\sim$ is reflexive, $x \sim x$.

So, $x \in \overline{x}$.

$\boxed{①}$

② ($\Rightarrow$) Suppose $\overline{x} = \overline{y}$.

By 1, $x \in \overline{x}$.

Thus, since $x \in \bar{x}$ and $\bar{x} = \bar{y}$ we get $x \in \bar{y}$.

($\Leftarrow$) Now suppose $x \in \bar{y}$.

Why is $\bar{x} = \bar{y}$?

$\bar{x} = \{ b \in S \mid x \sim b \}$

Claim 1: $\bar{x} \subseteq \bar{y}$

pf of claim 1: Let $z \in \bar{x}$

$\bar{y} = \{ b \in S \mid y \sim b \}$

Thus, $x \sim z$.

Also, since $x \in \bar{y}$ we know $y \sim x$.

Since $y \sim x$ and $x \sim z$, then by transitivity we get $y \sim z$.

Thus, $z \in \bar{y}$.

$\boxed{\text{claim 1}}$

Claim 2: $\bar{y} \subseteq \bar{x}$

pf of claim 2: Let $z \in \bar{y}$.

Then, $y \sim z$.

Since $x \in \bar{y}$ we know $y \sim x$.

Since $y \sim x$, by reflexivity

we get $x \sim y$.

Since $x \sim y$ and $y \sim z$, by transitivity we get $x \sim z$.

Since $x \sim z$ we know $z \in \overline{x}$

$\boxed{\text{Claim 2}}$

By claim 1 and claim 2 we get $\overline{x} = \overline{y}$. $\boxed{2}$

3

($\Rightarrow$) Suppose $\overline{x} = \overline{y}$.

Then by 2 we get $x \in \overline{y}$.

Thus, $y \sim x$.

By symmetry we get $x \sim y$.

($\Leftarrow$) Suppose $x \sim y$.

By def, get $y \in \overline{x}$

By 2 we get $\overline{y} = \overline{x}$.

$\boxed{3}$

---

4 Instead of proving

"$\overline{x} \cap \overline{y} = \phi$ iff $x \nsim y$"

let's prove the contrapositive

"$\overline{x} \cap \overline{y} \neq \phi$ iff $x \sim y$"

P iff Q
is equivalent to
$\neg P$ iff $\neg Q$

P	Q	$\neg P$	$\neg Q$	P iff Q	$\neg P$ iff $\neg Q$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

<u>pf:</u>

($\Rightarrow$) Suppose $\overline{x} \cap \overline{y} \neq \phi$.

Then there exists $z \in \overline{x} \cap \overline{y}$.

So, $z \in \overline{x}$ and $z \in \overline{y}$.

Then, $x \sim z$ and $y \sim z$.

By symmetry we get $z \sim y$.

Thus, since $x \sim z$ and $z \sim y$,

by transitivity we get $x \sim y$.

($\Leftarrow$) Suppose $x \sim y$.

Then by 3, we get $\overline{x} = \overline{y}$.

By 1, $x \in \overline{x}$.

So, since $\overline{x} = \overline{y}$ and $x \in \overline{x}$

we have $x \in \underbrace{\overline{x} \cap \overline{y}}_{\text{this is just } \overline{x}}$.

So, $\overline{x} \cap \overline{y} \neq \phi$.

$\boxed{4}$

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

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

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

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

[So, here congruence modulo n is a relation on $\mathbb{Z}$]

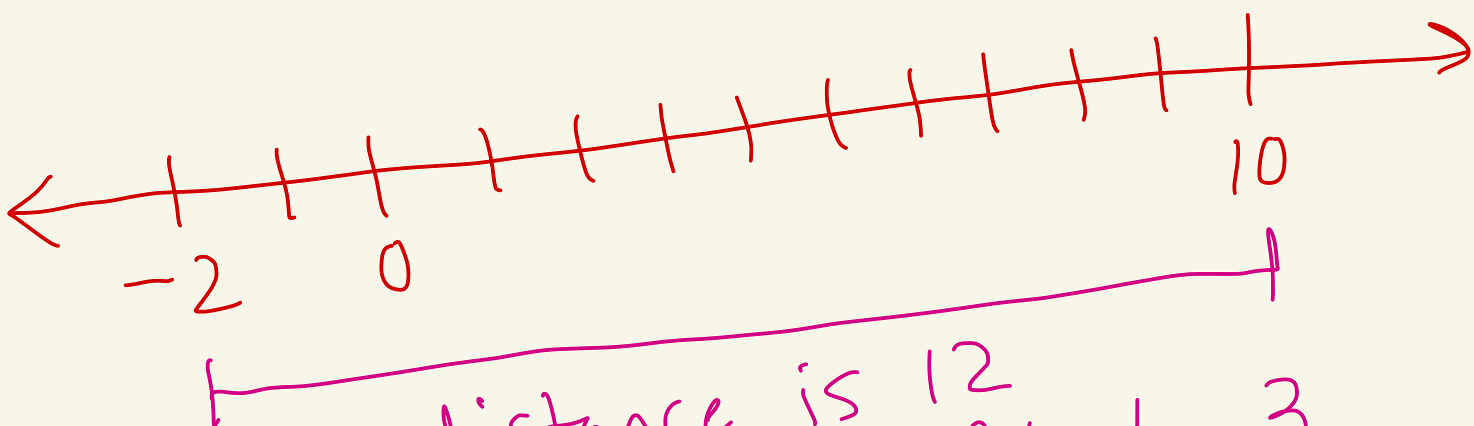
<u>Ex:</u> Let $n = 3$.

<u>Q:</u> Is -2 congruent to 10 modulo 3?

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

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

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



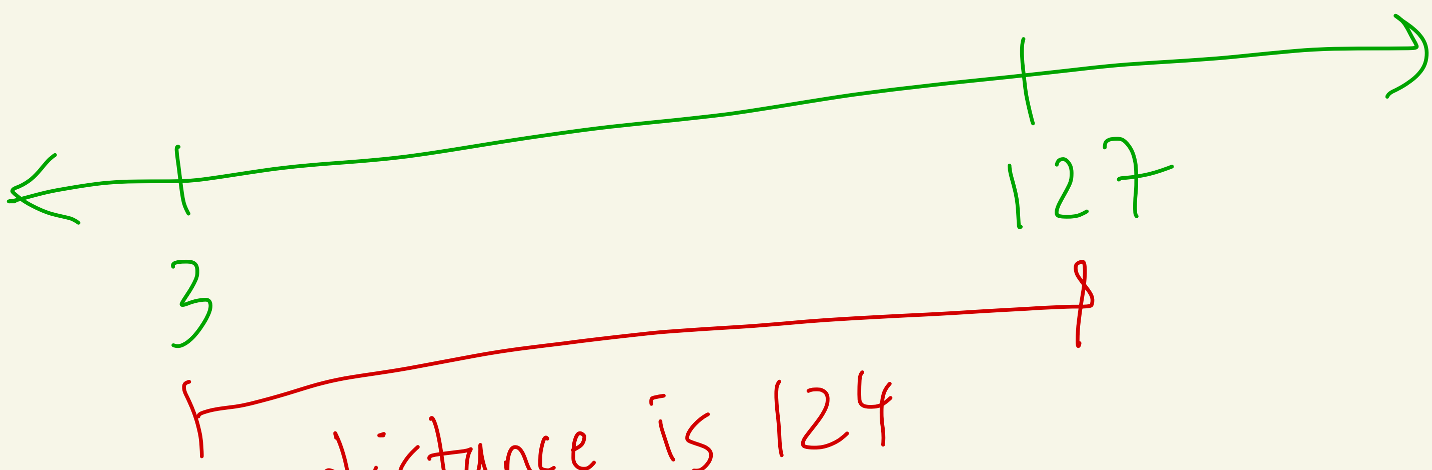
distance is 12
which is divisible by 3

Q: Is 3 congruent to 127 modulo 3?

We have
$$3 - 127 = -124$$
And $3 \nmid -124$.

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

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



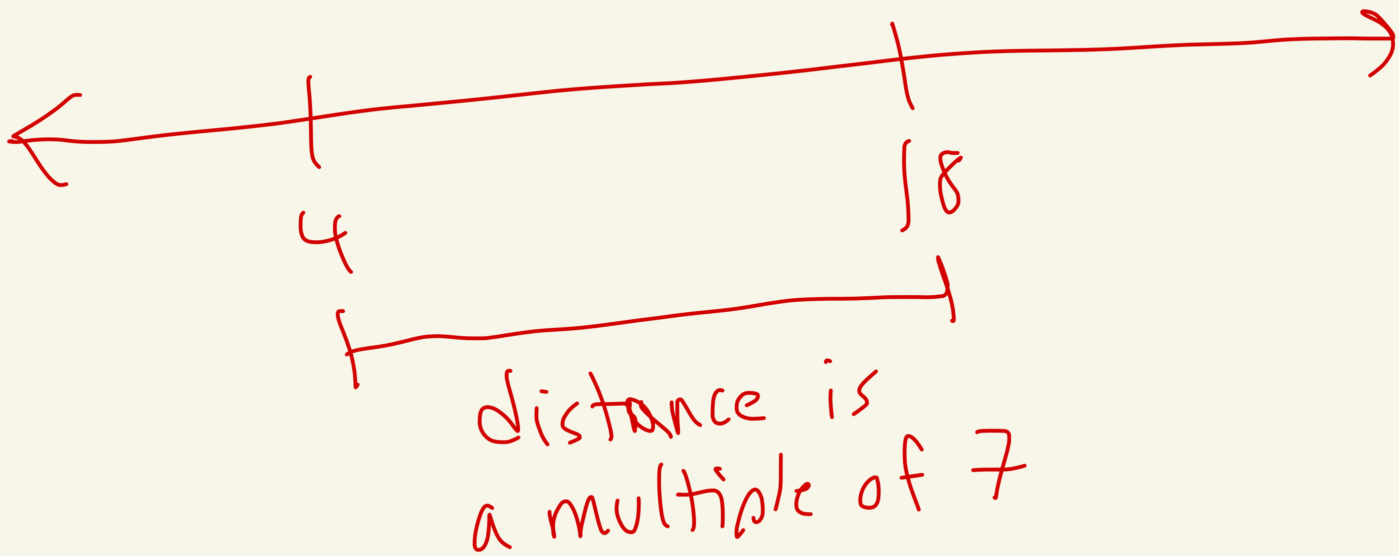
distance is 124
which is not
divisible by 3

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

Yes, because

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

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



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

Then, congruence modulo 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

$$\begin{aligned} a-c &= (b+nk_1)-(b-nk_2) \\ &= nk_1 + nk_2 \\ &= n\underbrace{(k_1+k_2)}_{} \end{aligned}$$

$k_1+k_2 \in \mathbb{Z}$ since $k_1, k_2 \in \mathbb{Z}$

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

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

<u>Def:</u> 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 $\mathbb{Z}_n$

Ex: Let $n = 2$

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

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

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

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

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

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

$= \overline{0}$

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

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

$= \overline{1}$

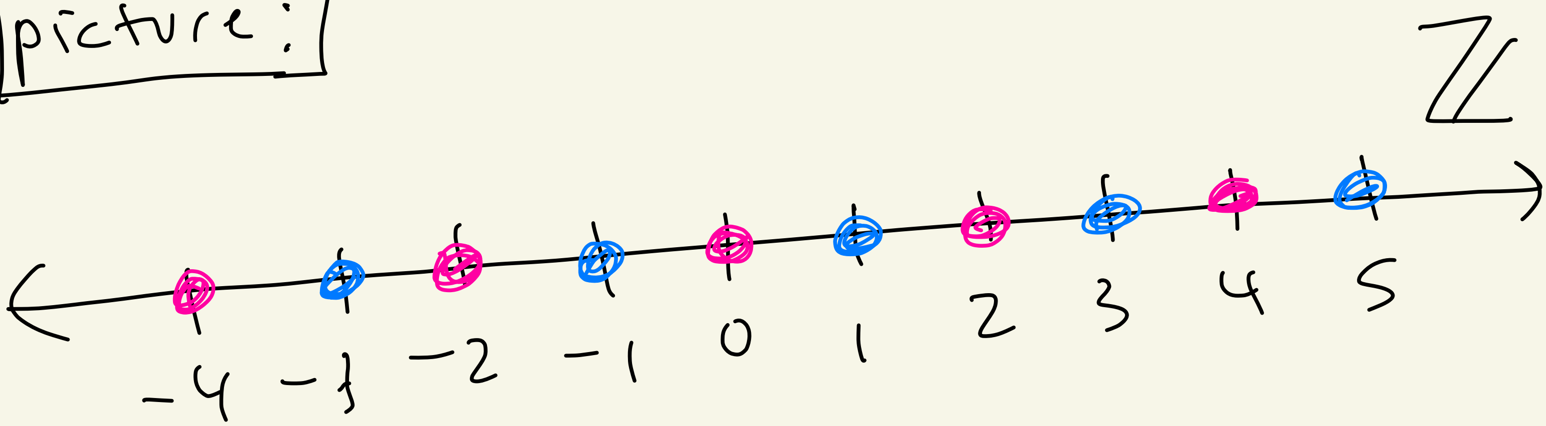
We will get that

$$\left.\begin{array}{l} \bar{0} = \bar{2} = \overline{-2} = \bar{4} = \overline{-4} = \bar{6} = \overline{-6} = \cdots \\ \bar{1} = \overline{-1} = \bar{3} = \overline{-3} = \bar{5} = \overline{-5} = \cdots \end{array}\right\} \text{two equiv. classes}$$

The set of equivalence classes is

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

$\boxed{\text{picture:}}$



$\bar{0}$ is pink

$\bar{1}$ is blue

Ex: Let $n=3$. Let's compute the equivalence classes modulo 3

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

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

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

By the super-duper equivalence relation theorem we get that

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

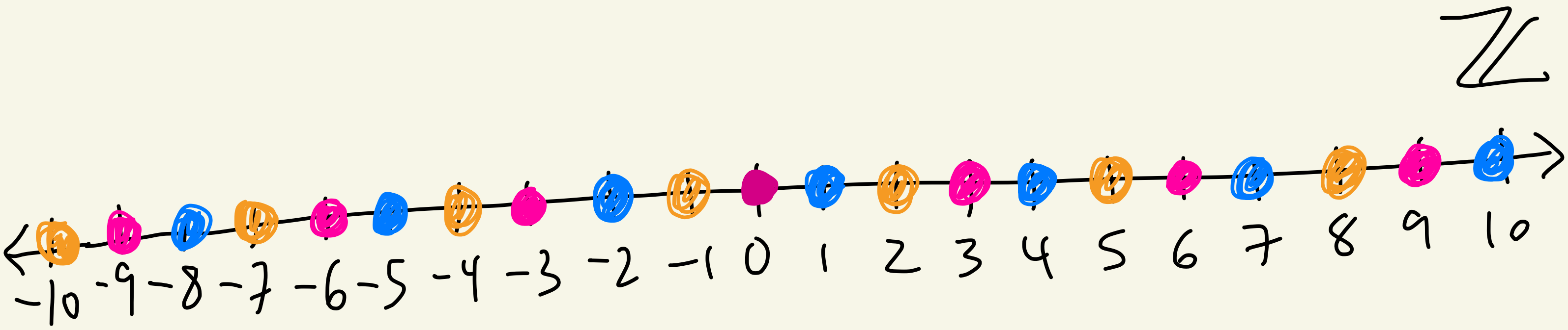
$\overline{1} = \overline{-8} = \overline{1} = \overline{7} = \ldots$

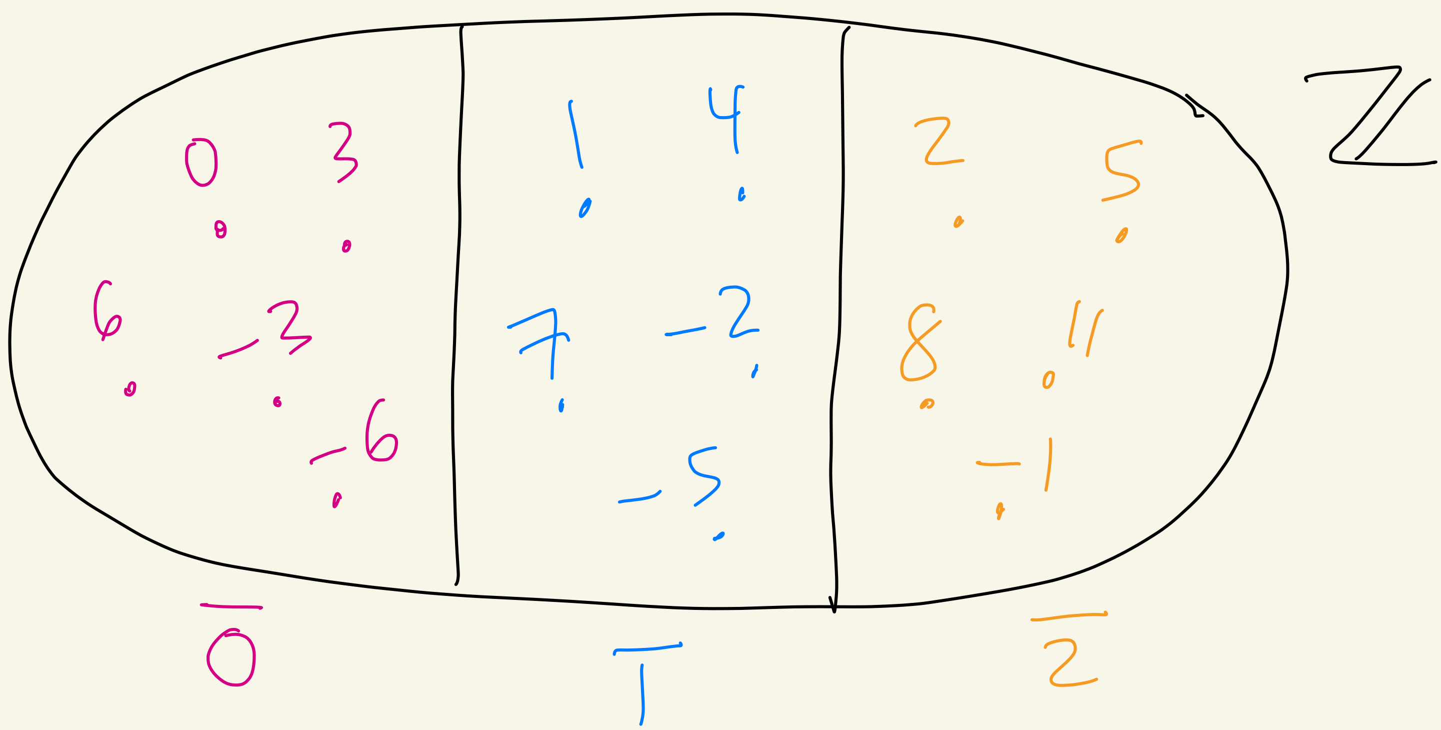
$\overline{2} = \overline{-4} = \overline{-1} = \overline{5} = \overline{8} = \dots$

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

set of equivalence classes mod 3

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





<u>Ex:</u> $a = 5$
$b = 17$

$$\begin{array}{r} 3 \leftarrow \boxed{q} \\ 5\overline{)17} \\ -15 \\ \hline 2 \leftarrow \boxed{r} \end{array}$$

$$\underbrace{17 = 5(3) + 2}_{\begin{array}{c} b = aq + r \\ 0 \le r < a \end{array}}$$

<u>Theorem</u> (Division Algorithm)
Let $a, b \in \mathbb{Z}$ with $a > 0$. Then there exists unique integers q and r where

$$b = aq + r \text{ and } 0 \le r < a$$

proof:

(existence)

Let $S = \{ b - ax \mid x \in \mathbb{Z} \text{ and } b - ax \geq 0 \}$

Ex: $a = 5, b = 17$

$S = \{ 17 - 5x \mid x \in \mathbb{Z},\ 17 - 5x \geq 0 \}$

$= \{ 2, 7, 12, 17, 22, \ldots \}$

Smallest element of S

x	$17-5x$
$\vdots$	$\vdots$
5	-8
4	-3
3	2
2	7
1	12
0	17
-1	22
$\vdots$	$\vdots$

$$S = \left\{ b - ax \;\middle|\; \begin{array}{l} x \in \mathbb{Z} \\ b - ax \geq 0 \end{array} \right\}$$

Let's show $S \neq \emptyset$.

<u>case 1</u>: Suppose $b \geq 0$.

Setting $x = -1$ we get

$$b - ax = b - a(-1) = b + a \geq 0$$

$$\boxed{\begin{array}{c} b \geq 0 \\ a > 0 \end{array}}$$

So, $b - a(-1) \in S$.

<u>case 2</u>: Suppose $b < 0$.

Set $x = 2b$ and we get

$$b - ax = b - a(2b) = \underbrace{b}_{b<0}\underbrace{(1-2a)}_{\begin{array}{l} a \geq 1 \\ -2a \leq -2 \\ 1-2a \leq -1 \\ 1-2a < 0 \end{array}} > 0$$

Thus, $b - a(2b) \in S$.

$\boxed{S = \{b - ax \mid x \in \mathbb{Z},\ b - ax \geq 0\}}$

So, by case 1 and case 2, $S \neq \emptyset$.

Since S is non-empty and it consists of non-negative integers, S must have a smallest element.

Let r be the smallest element of S.

Thus there exists $q \in \mathbb{Z}$ with $r = b - aq$ and $r = b - aq \geq 0$.

[I switched x to q here.]

So, $\boxed{b = aq + r}$.

We have $0 \leq r$.

We must show that $r < a$.

Suppose instead that $a \leq r$.

Then $0 \leq r - a$.

Also, $r - a = (b - aq) - a$

$$= \underbrace{b - a(q+1)}_{\text{has the form } b-ax} \in S$$

But $r - a < r$ and r is the smallest element of S.

Thus, it can't be that $r - a \in S$.

It's a contradiction.

Hence, $r < a$.

So, $b = aq + r$ with $0 \leq r < a$.

Uniqueness Suppose

$b = aq + r$ with $0 \leq r < a$, and

$b = aq' + r'$ with $0 \leq r' < a$,

where $q, q', r, r' \in \mathbb{Z}$.

We will show $q = q'$ and $r = r'$

Let's show that $r = r'$.

Without loss of generality, assume $r' \geq r$

Means same proof will work if $r \geq r'$

Then, $\boxed{r' - r \geq 0}$.

Since $b = aq + r = aq' + r'$ we get

$$\boxed{a(q - q') = r' - r}.$$

Let $k = q - q'$.

So, $\boxed{ak = r' - r.}$

Then from the eqn above since $a > 0$ and $r' - r \geq 0$ we know $k \geq 0$.

Let's show $k = 0$.

Suppose $k > 0$.

If so, then

$$r' - r = ak \underset{\boxed{k \geq 1}}{\geq} a(1) = a.$$

Then, $a \leq r' - r$.

However we also have that

$$0 \leq r' - r \underset{\boxed{r' < a}}{<} a - r \underset{\boxed{0 \leq r}}{\leq} a$$

So, $r' - r < a$

CONTRADICTION

This is nonsense!

So, $k \not> 0$.

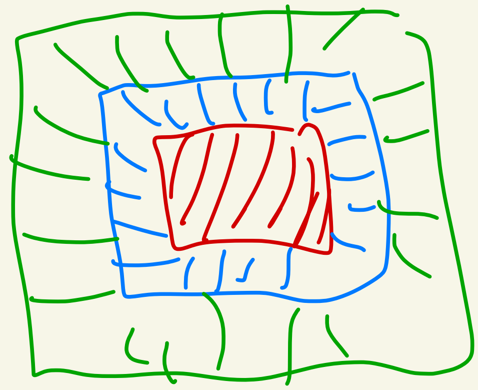
We must have $k = 0$.

Thus, $0 = k = q - q'$.

So, $q = q'$.

Also, $0 = a\underbrace{k}_{0} = r' - r$

So, $r = r'$.



Calculating modulo n using the division algorithm

Let $n \geq 2$.

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

Divide n into x to get

$$x = nq + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r < n$.

Then, $nq = x - r$

So, $n \mid (x - r)$.

So, $x \equiv r \pmod{n}$

Hence, $\overline{x} = \overline{r}$ in $\mathbb{Z}_n$

Ex: Let $n = 4$.

Let $x = 10{,}562$.

$$\begin{array}{r}
2640 \\
4\,\overline{)\,10{,}562} \\
-8\phantom{{,}562} \\
\hline
25 \\
-24 \\
\hline
16 \\
-16 \\
\hline
02 \\
-0 \\
\hline
2
\end{array}$$

$$\underbrace{10{,}562}_{x} = \underbrace{4}_{n}(2640) + \underbrace{2}_{r}$$

So,

$$10{,}562 \equiv 2 \pmod{4}$$

Ex: $n = 6$

$$x = 220$$

$$\begin{array}{r} 36 \\ 6\overline{)220} \\ -18 \\ \hline 40 \\ -36 \\ \hline 4 \end{array}$$

$$\underbrace{220}_{x} = \underbrace{6}_{n}(36) + \underbrace{4}_{r}$$

So, $220 \equiv 4 \pmod{6}$

Theorem: (Equivalence classes modulo n)

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

Then

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

These elements are all distinct.

That is, if $0 \leq x \leq y \leq n-1$ and $\overline{x} = \overline{y}$, then $x = y$.

proof: Let

$$S = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

We want to show that

$$\mathbb{Z}_n = S.$$

Note that $S \subseteq \mathbb{Z}_n$ because it consists of equivalence classes modulo n.

We just need to show that $\mathbb{Z}_n \subseteq S$.

Let $\bar{z} \in \mathbb{Z}_n$ where $z \in \mathbb{Z}$.

Divide z by n to get

$$z = nq + r$$

where $q, r \in \mathbb{Z}$ and $\underbrace{0 \le r < n}_{\text{same as } 0 \le r \le n-1}$

Then, $z - r = nq$.

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

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

Hence, $\overline{z} = \overline{r}$.

Thus, $\overline{z} \in S = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$

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

Hence $\mathbb{Z}_n \subseteq S$.

So, $\mathbb{Z}_n = S$.

Why are all the elements

of $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ distinct?

Suppose $\boxed{0 \leq x \leq y \leq n-1}$
with $\boxed{\bar{x} = \bar{y}}$.

Let's show this implies $x = y$.

Since $\bar{x} = \bar{y}$ we know that $x \equiv y \pmod{n}$.

super duper equiv. rel. thm. $\bar{x} = \bar{y}$ iff $x \sim y$

Thus, $n \mid (y-x)$.

Hence $\boxed{y - x = nk}$ for some $k \in \mathbb{Z}$.

Note $0 \leq y - x$ from above and $n \geq 2 > 0$, thus $k \geq 0$.

Since $x \leq y \leq n-1$ by

subtracting x we get

$$0 \le y - x \le n - 1 - x.$$

Since $0 \le x$ we know

$$n - 1 - x < n.$$

Thus, $\boxed{0 \le y - x < n}$

Summary so far:

$$\boxed{\begin{array}{l} y - x = nk \text{ with } k \geq 0 \\ \text{and } 0 \le y - x < n \end{array}}$$

Let's show $k = 0$.

Suppose instead that $k > 0$.

If so, then

$$0 \le y - x < n \le nk = y - x$$

assuming $k > 0$
ie $k \geq 1$

But then $y - x < y - x$
which can't happen.

Hence $k = 0$.

So, $y - x = nk = n(0) = 0$.

Thus, $y = x$.

$\boxed{\text{FINITO}}$

Ex:

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

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

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

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

Def: A partition of a set S is a family of sets $\mathcal{A}$ where

① every $A \in \mathcal{A}$ satisfies $A \subseteq S$,

② $\bigcup_{A \in \mathcal{A}} A = S$

③ If $A, B \in \mathcal{A}$ and $A \neq B$, then $A \cap B = \phi$.

Ex: $S = \{1, 2, 3, 4, 5, 6\}$

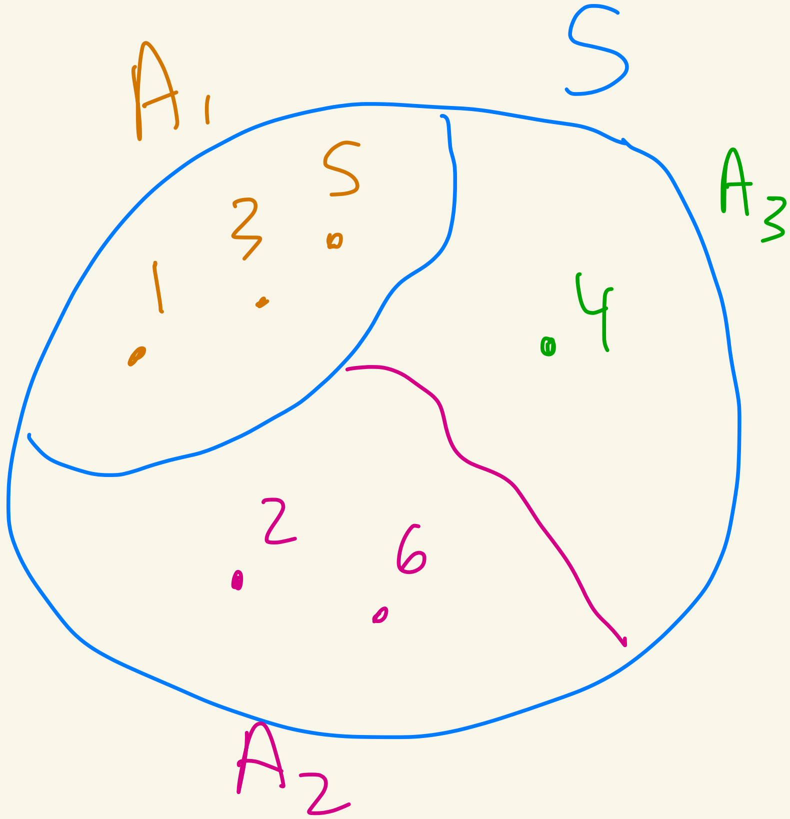
$$\mathcal{A} = \{ \underbrace{\{1,3,5\}}_{A_1}, \underbrace{\{2,6\}}_{A_2}, \underbrace{\{4\}}_{A_3} \}$$

① $A_1 \subseteq S$, $A_2 \subseteq S$, $A_3 \subseteq S$

② $\bigcup_{A \in \mathcal{A}} A = A_1 \cup A_2 \cup A_3 = S$

③ $A_1 \cap A_2 = \phi$
$A_1 \cap A_3 = \phi$
$A_2 \cap A_3 = \phi$

Thus, $\mathcal{A}$ is a partition of S



Ex:

$S = \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Consider the equivalence classes modulo $\boxed{n=3}$. They are

$\bar{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$\overline{1} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$

$\overline{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$

The set of equivalence classes is a partion of $\mathbb{Z}$.

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

Theorem Let S be a non-empty set. Let $\sim$ be an equivalence relation on S. Then the set of equivalence classes

$$S/\sim \; = \{ \bar{a} \mid a \in S \}$$

is a partition of S.

Ex: when $\sim$ is mod 3 then $S/\sim \; = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

proof:

(1) Let $\bar{a} \in S/\sim$ where $a \in S$.

Then,

$$\overline{a} = \{ b \mid b \in S \text{ where } a \sim b \} \subseteq S$$

② We have that

① $\overline{a} \subseteq S$

$$S = \bigcup_{a \in S} \{a\} \subseteq \bigcup_{a \in S} \overline{a} = \bigcup_{\overline{a} \in S/\sim} \overline{a} \subseteq S$$

super duper thm $a \in \overline{a}$

$S/\sim \; = \{ \overline{a} \mid a \in S \}$

Thus, $S = \displaystyle\bigcup_{\overline{a} \in S/\sim} \overline{a}.$

③ By the super-duper equivalence class theorem, if $a, b \in S$ and $\overline{a} \neq \overline{b}$, then $\overline{a} \cap \overline{b} = \phi$.

Theorem

Let S be a non-empty set.
Let $\mathcal{A}$ be a partition of S.
Define a relation $\sim$ on S by the following:

Given $a, b \in S$, then $a \sim b$ if and only if there exists $A \in \mathcal{A}$ where $a \in A$ and $b \in A$.

Then:

1. $\sim$ is an equivalence relation on S
2. $S/_{\sim} = \mathcal{A}$

Proof: (don't prove in class, mention proof in notes)

(1)

(reflexive)

Let $x \in S$.

By the def of partition, $S = \bigcup_{A \in \mathcal{A}} A$.

So, $x \in \bigcup_{A \in \mathcal{A}} A$.

Thus, there exists $A \in \mathcal{A}$ with $x \in A$.

So, $x \sim x$.

(symmetric)

Let $x, y \in S$ with $x \sim y$.

Then there exists $A \in \mathcal{A}$ with $x \in A$ and $y \in A$.

So, $y \in A$ and $x \in A$.

Thus, $y \sim x$.

(<u>transitive</u>) Let $x, y, z \in S$ with $x \sim y$ and $y \sim z$.

Since $x \sim y$ there exists $A \in \mathcal{A}$ with $x \in A$ and $y \in A$.

Since $y \sim z$ there exists $B \in \mathcal{A}$ with $y \in B$ and $z \in B$.

Since $y \in A \cap B$ we know $A \cap B \neq \emptyset$.

Since $\mathcal{A}$ is a partition and $A, B \in \mathcal{A}$ with $A \cap B \neq \emptyset$ by property 3 of partitions we must have $A = B$.

Thus, $x \in A$ and $z \in A$.

So, $x \sim z$.

(2) We want to show that $S/_{\sim} = \mathcal{A}$

$\boxed{\subseteq}$: Let $\bar{a} \in S/_{\sim}$.

Pick the unique $A \in \mathcal{A}$ where $a \in A$.

Then $\bar{a} = A$ by def of $\sim$.

So, $\bar{a} \in \mathcal{A}$.

$\boxed{\supseteq}$: Let $A \in \mathcal{A}$

Pick any $a \in A$.

Then by the def of $\sim$ we have $\bar{a} = A$.

So, $A = \bar{a} \in S/_{\sim}$.

$\blacksquare$