

\* Last time: Equivalence relations & equivalence classes

Example:  $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \text{ is even}\}$ . [\* If  $(a, b) \in R$   
we say  $a \sim b$ .]

There are two equivalence classes: {odds} & {evens}

Main result: Let  $R$  be an equivalence relation on  $S$ .

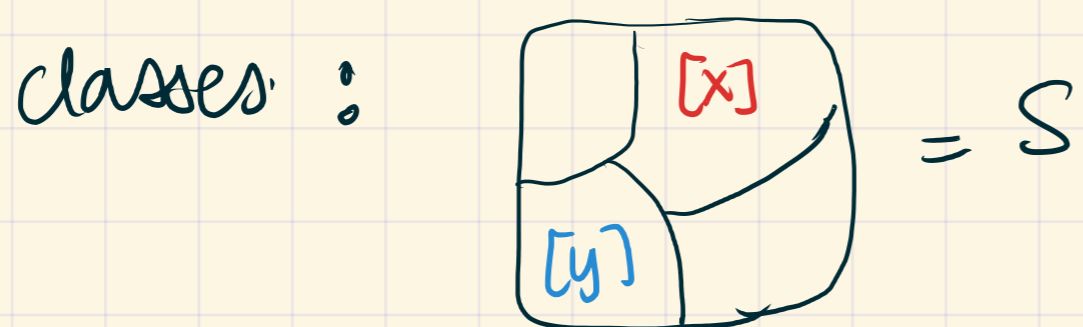
For any  $x \in S$ , set  $[x] = \{y \in S \mid x \sim y\}$ , called the "equivalence class of  $x$ ".

Then:

\*  $[x]$  consists of exactly those elements of  $S$  that are related to  $x$ , and nothing else.

\* If  $y \in [x]$  then  $[x] = [y]$ , so equivalence classes can only overlap if they are equal, and

\*  $S$  is partitioned into a disjoint union of equivalence classes:



Note:  $S = S_1 \cup S_2 \cup \dots \cup S_n$  is a partition if

$S_i \cap S_j = \emptyset$  for  $i \neq j$ . This is also written as

$S = S_1 \bigsqcup S_2 \bigsqcup \dots \bigsqcup S_n$ , or more concisely,

$$S = \bigsqcup_{i=1}^n S_i$$

### Modular arithmetic

\* You have all seen modular arithmetic before, even if you think you haven't!

Baby example :  $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \text{ is even}\}$ .

$$\mathbb{Z} = [0] \perp [1] = [248] \perp [55] \\ = [42] \perp [-11] \\ \dots$$

Since  $[248] = [0]$ , we say that 0 is a representative of the equiv. class  $[0]$ , and 248 is also a representative of  $[0]$ .

$$\begin{array}{ccccccc} 42 & + & 6 & = & 48 & & \\ \uparrow & & \uparrow & & \uparrow & & \\ [0] & & [0] & & [0] & & \text{even} + \text{even} = \text{even} \end{array}$$

$$\begin{array}{ccccccc} 42 & + & 9 & = & 51 & & \\ \uparrow & & \uparrow & & \uparrow & & \\ [0] & & [1] & & [1] & & \text{even} + \text{odd} = \text{odd} \\ & & & & & & \text{odd} + \text{even} = \text{odd} \end{array}$$

$$\begin{array}{ccccccc} 9 & + & 11 & = & 20 & & \\ \uparrow & & \uparrow & & \uparrow & & \\ [1] & & [1] & & [0] & & \text{odd} + \text{odd} = \text{even} \end{array}$$

We have defined a new addition : on the set  $\{[0], [1]\}$  :

$$[0] + [0] := [0]$$

$$[0] + [1] := [1]$$

$$[1] + [0] := [1]$$

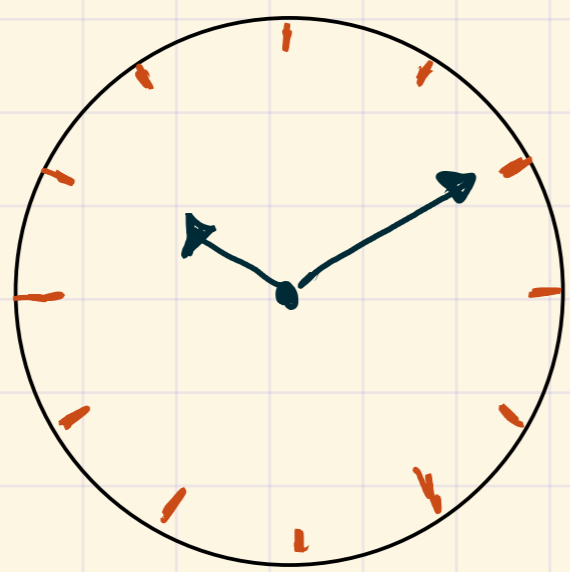
$$[1] + [1] := [0]$$

← Loops  
back to  $[0]$ !

Q : Why does it make sense?  
What does that even  
mean?

Rmk :  $\{[0], [1]\} \neq \{0, 1\}$   
+  
 $\mathbb{Z}$

\* But you know this already:



$$10 \text{ (am)} + 9 \text{ (hrs)} = 7 \text{ (pm)}$$
$$[10] + [9] = [7]$$

$$5 \text{ (pm)} + 20 \text{ (hrs)} = 1 \text{ (pm)}$$
$$[5] + [20] = [1]$$

$$2 \text{ (am)} - 4 \text{ (hrs)} = 10 \text{ (pm)}$$
$$[2] - [4] = [10]$$

(Similar for 24-hour clock)

\* We're treating 20 & 8 as equivalent

---

Fix a positive  $d \in \mathbb{N}$ ; we'll call this the modulus.

Let's construct an equivalence relation

$$R = \sim_d = \{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \mid (x-y) \text{ is divisible by } d \}$$

"  
 $d \mid (x-y)$

If  $(x, y) \in R$ , we say  $x \sim_d y$ , or more traditionally,  
we write  $x \equiv y \pmod{d}$

( $x$  is congruent to  $y$  modulo  $d$ )

Note: If  $x \sim_d y$ , then there is some integer  $n \in \mathbb{Z}$   
(positive, negative, or zero) such that

$$x - y = n \cdot d.$$

\* Exercise: Check that this is an equivalence relation.

Equivalence classes:

$$\text{E.g. } [0] = \{ 0, d, -d, 2d, 5d, -2d, -3d, \dots \}$$

$$[1] = \{ 1 + 3d, 1 - 7d, 1, \dots \}$$



We (think we) have  $d$  equiv. classes:

$[0], [1], \dots, [d-1]$ , because  $[d] = [0]$

Q: Why are they all different?

(Euclid's division algorithm: if  $x \in \mathbb{Z}$ , and  $d \in \mathbb{N}$ , then there is a unique equation

$$x = qd + r, \text{ with } 0 \leq r < d.)$$

In fact, they are all different.

Let's define an addition operation:

$$[x] + [y] = [x+y]$$

Q: Why does this make sense?

That is, if  $[x] = [a]$ , then is it true that  $[x+y] = [a+y]$ ?

In this case, if  $[x] = [a]$ , then  $x-a = nd$ .

$$\text{Then } (x+y) - (a+y) = (x-a) = nd$$

$$\Rightarrow [x+y] = [a+y]$$

Therefore, this addition is well-defined.

E.g. if  $d=3$ :

$$[1] + [2] = [0]$$

$$[1] + [1] = [2]$$

$$[2] + [2] = [4] = [1]$$

This is modular addition

Q: Can you multiply modular numbers?

$$[x] \cdot [y] := [xy]$$

[This is a new definition and we now check that it is sensible]

Does this make sense?

Suppose  $[x] = [a]$ , i.e.  $x - a = nd$  for some  $n \in \mathbb{Z}$ .

We want  $[xy] \stackrel{?}{=} [ay]$

i.e. is  $xy - ay$  a multiple of  $d$ ?

$$xy - ay = nyd \quad \text{so yes!}$$

$\Rightarrow [xy] = [ay]$ , so it is well-defined.

E.g.: If  $d = 3$ :

$$[1] \cdot [1] = [1]$$

$$[2] \cdot [2] = [1]$$