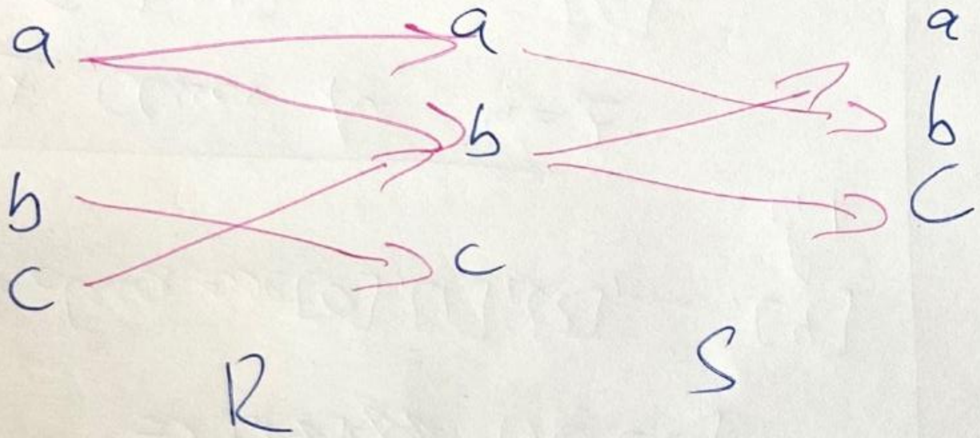
$R = \{(a,a),(a,b),(b,c),(c,b)\}$, $S = \{(a,b),(b,a),(b,c)\}$



Modular Arithmetic

$A = \mathbb{Z}$, Define relation $\sim$ or $\sim_m$: $a \sim b \overset{\text{def}}{\iff} m \mid (b-a)$

divides

congruent modulo m

$m \in \mathbb{Z}$, $m > 1$,

This is equiv. rel.:

reflexive: $m \mid 0 = (a-a) \Rightarrow a \sim a$

symmetric: $a \sim b \Rightarrow m \mid (b-a)$
$\Rightarrow m \mid (a-b) \Rightarrow b \sim a$

transitive: $a \sim b, b \sim c \Rightarrow m \mid (b-a)$
$m \mid (c-b)$
$\Rightarrow m \mid ((b-a)+(c-b)) = (c-a)$
$\Rightarrow c \sim a$

Equiv. classes:

Ex: $m = 5$

$[1] = \{1, 6, 11, -4, -9, 16, \ldots\}$

$[3] = \{3, 8, -2, 13, -7, \dots\}$

$\parallel$

$[-2]$

Then $\Rightarrow$ • every class has $c \geq 0$

• every class has elt $< m$.

$$\boxed{\text{Every class contains exactly one element } r :\ 0 \leq r \lneq m}$$

Ex: $17 = 3 \cdot 5 + 2$

$\Rightarrow$ $17 \in [2]$

The classes are $[0], [1], [2], \dots, \underset{\substack{\uparrow \\ m-1}}{[4]}$

Ex. Classes for $m = 7$:

$[0], [1], \dots [6]$

Now: Define arithmetic on equiv. classes:

$$[a] + [b] := [a+b]$$

Ex $(m=5)$: $[2] + [4]$

$= [2+4] = [6] = [1]$

This addition is independent of the choice of representative.

Similarly multiplication:

$$[a] \cdot [b] = [a \cdot b]$$

The usual rules for arithmetic hold

Ex: $m = 3$

Classes $[0], [1], [2]$

$\overline{0}$ $\overline{1}$ $\overline{2}$ ← shorthand notation

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\overline{1} = -\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\Rightarrow \overline{\tfrac{1}{2}} \bmod 3 = \overline{2}$

Ex: Solve equation $x + \overline{2} = \overline{1} \pmod 3$ $\quad | + \overline{1}$

$$\overline{x} = x + \underbrace{\overline{2} + \overline{1}} = \overline{1} + \overline{1} = \overline{2}$$

$$\overline{2} \cdot x = \overline{1} \quad | \cdot \overline{2}$$

$$x = \overline{1}x = \overline{2} \cdot \overline{2} \cdot x = \overline{1} . \overline{2} = \overline{2}$$