$\mathbb{Z}_m$ AND A TASTE OF MODULAR ARITHMETIC

<u>Def</u>: Let $m \in \mathbb{N}$. The relation congruence modulo m is

$$R = \{ (a,b) \in \mathbb{Z}^2 : m \mid (a-b) \}$$

$$\underbrace{(a,b) \in R \iff \text{"} a \equiv b \text{ mod } m \text{"} \iff m \mid (a-b)}_{a \text{ is congruent to } b \text{ modulo } m.}$$

<u>Def</u>: The set of equivalence classes for the relation congruence modulo m is detoted

$$\mathbb{Z}_m := \mathbb{Z}/_R$$

<u>Recall</u>: <u>The Division Algorithm</u>

$\forall\ a, b \in \mathbb{Z}$, $b \neq 0$ there exist <u>unique</u> integers q and r such that

$$a = b \cdot q + r, \quad \text{with } \underbrace{0 \leq r < |b|}_{0 \leq r \leq |b|-1}$$

quotient

remainder

<u>Proposition 1</u>: $\forall\ a, b \in \mathbb{Z}$, $a \equiv b \pmod m$ if and only if a and b have the same remainder when divided by m.

<u>Example</u>: $m = 4$

* $20 = 4 \cdot 5 + 0$
* $500 = 4 \cdot 125 + 0$
* $22 = 4 \cdot 5 + 2$
* $72 = 4 \cdot 18 + 0$

Since $\forall\ x \in \mathbb{Z}$, $0 \leq x \leq m-1$, the remainder of x in the division by m is exacly x:

$$x = m \cdot 0 + x$$

Then every integer is congruent to one among $0, 1, 2, \dots, m-1$.

Example

$m = 4$

possible remainders: $0, 1, 2, 3$.

$0 \longrightarrow 0$

$1 \longrightarrow 1$

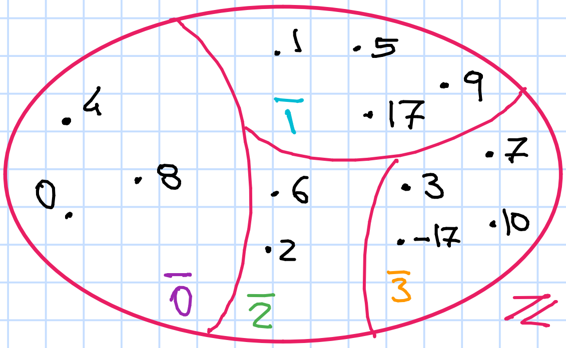
$2 \longrightarrow 2$

$3 \longrightarrow 3$

$4 = 4 \cdot 1 + 0 \longrightarrow 0$

$5 = 4 \cdot 1 + 1 \longrightarrow 1$

$6 = 4 \cdot 1 + 2 \longrightarrow 2$



$-17 = 4 \cdot (-5) + 3 \longrightarrow 3$

but $17 = 4 \cdot 4 + 1 \longrightarrow 1$

Proposition 2: $\mathbb{Z}_m$ consists of m different equivalence classes:

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$$

Proof in Theorem 3.2.4

So we have that $\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$ is a partition of $\mathbb{Z}$

$$\mathbb{Z} = \bigsqcup_{k=0}^{m-1} \bar{k}$$

disjoint union

So $\mathbb{Z}_m$ is a finite set with m elements.

We can equip $\mathbb{Z}_m$ with an algebraic structure, i.e. we can define two well-defined binary operations:

$(\mathbb{Z}_m, +, \cdot)$ is a ring

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$$
$$(\bar{a}, \bar{b}) \longmapsto \bar{a} + \bar{b} := \overline{a+b}$$

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$$
$$(\bar{a}, \bar{b}) \longmapsto \bar{a} \cdot \bar{b} := \overline{ab}$$

$(\mathbb{Z}_m, +, \cdot)$ is a ring

$$\begin{cases} + : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m \\ \quad (\bar{a}, \bar{b}) \longmapsto \bar{a} + \bar{b} \overset{\circledast}{:=} \overline{a+b} \\ \cdot : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m \\ \quad (\bar{a}, \bar{b}) \longmapsto \bar{a} \cdot \bar{b} \overset{\circledast}{:=} \overline{ab} \end{cases}$$

I'll prove you that sometimes we also have
$\bar{2} + \bar{2} = \bar{0}$, $\bar{3} \cdot \bar{3} = \bar{1}$, ...

$m = 4$. In $\mathbb{Z}_4$...

$$\bar{2} + \bar{2} \overset{\circledast}{=} \overline{2+2} = \bar{4} = \bar{0}$$

$$\bar{3} \cdot \bar{3} \overset{\circledast}{=} \bar{9} = \bar{1}$$

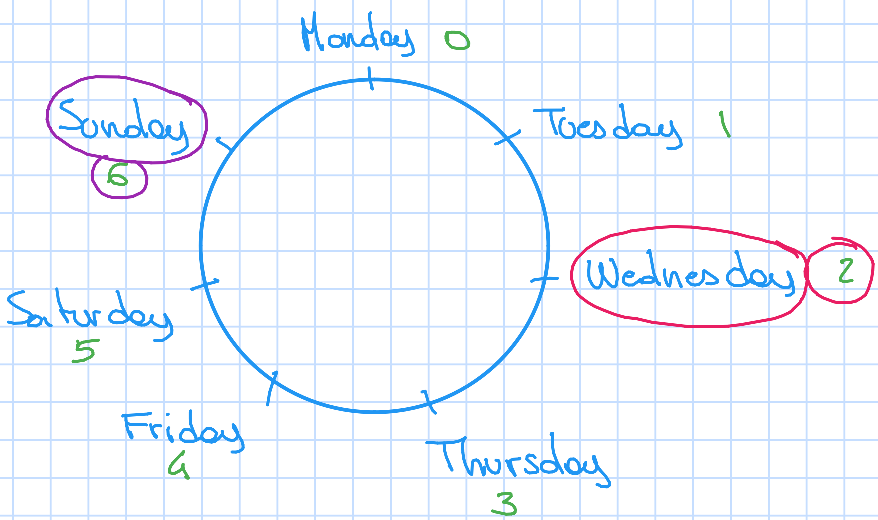
$$\underset{\substack{\| \\ \bar{2}}}{\overline{18}} + \underset{\substack{\| \\ \bar{2}}}{\overline{26}} = \overline{18+26} = \overline{44} = \bar{0}$$

$\forall\ x, y \in \bar{2}$, $x + y \in \bar{0}$

$\forall\ x, y \in \bar{3}$, $x \cdot y = \bar{1}$

$\Rightarrow$ the operations $\bar{2} + \bar{2} = \bar{0}$ and $\bar{3} \cdot \bar{3} = \bar{1}$ are well-defined.

Problem: Today is Wednesday. Which day of the week will be in 2020 days?



$m = 7$

$2020 = 7 \cdot 288 + 4$

$$\underset{\substack{\uparrow \\ \text{Wednesday}}}{\bar{2}} + \overline{2020} = \overline{2022} = \overline{7 \cdot 288 + 6} = \underset{\substack{\uparrow \\ \text{Sunday}}}{\bar{6}}$$

Video Lecture Quiz

Def: Let A, B be sets. A function from A to B is a relation from A to B such that

1) $\mathrm{Dom}(f) = A$
2) $\forall x, y, z$ s.t. $(x, y) \in f$ and $(x, z) \in f$ then $y = z$

Remark: $(x, y) \in f \iff y = f(x)$

x: input, y: output

Question 1 — 1 pts

Which among the following are functions from $A = \{a, b, c\}$ to $B = \{1, 2, 3, 4\}$? Select all that apply.

- [ ] $\{(a, 1), (a, 2), (b, 3), (c, 4)\}$ — but $y \neq z$
- [ ] $\{(1, a), (2, b), (3, a), (4, b)\}$ — not a subset of $A \times B$ ($1 \notin A$, $b \notin B$)
- [x] $\{(a, 4), (c, 1), (b, 1)\}$
- [x] $\{(a, 2), (b, 3), (c, 1)\}$ $\leftarrow$ $\mathrm{Rng}(f) = \{1, 2, 3\} \subsetneq B$

Question 2 — 1 pts

If f is a function from A to B, then...

(Select all that apply)

- [ ] $(x, y), (y, z) \in f \Rightarrow (x, z) \in f$ — transitivity
- [ ] If $(x_1, y) \in f$ and $(x_2, y) \in f$ then $x_1 = x_2$ — injectivity
- [ ] $\mathrm{Rng}(f) = B$ — $\mathrm{Rng}(f) \subseteq B$, $\mathrm{Rng}(f) = \{y \in B : \exists x \in A \text{ s.t. } (x, y) \in f\}$
- [x] $\mathrm{Dom}(f) = A$
- [x] f is a subset of $A \times B$

Question 3

1 pts

Select all the true statements:

- [x] All functions are relations
- [ ] Every relation is a function
- [x] Some relations are functions
- [x] Some functions are relations

Question 4

1 pts

For the function

$$f = \{(x, y) \in \mathbb{R} : y = x^2 + 3\}$$

select all the true statements.

- [x] $4 = f(1) = f(-1)$
- [x] 7 is the image of 2 $\quad 2^2 + 3 = 7$
- [ ] 3 is the unique pre-image of 12 $\quad 3^2+3=12, \quad (-3)^2+3=12$
- [ ] 4 is a pre-image of 1 $\quad 4^2+3 \neq 1 \quad ↯$
- [x] 0 is a pre-image of 3 (x, y) $\quad 0^2 + 3 = 3$

Question 5

1 pts

Consider the relation

$$R = \{(x, y) \in \mathbb{R}^2 : y = \sqrt{x+16}\}.$$ can not be $(-\infty, \infty)$ since $-30 \notin \mathrm{Dom}(f)$

Then R defines a functions f : [Select] domain $\longrightarrow$ $\mathrm{Dom}(f) = [-16, \infty)$

[Select] codomain. The range of f is [Select] $[0, \infty)$.

cannot be $(0, \infty)$ since $0 \in \mathrm{Rng}(f)$ and $\mathrm{Rng}(f) \subseteq$ codomain.

$\Rightarrow$ Codomain $= (-\infty, \infty)$.

Question 6 1 pts

For the function

$$f = \{(x, y) \in \mathbb{R}^2 : y = \sin(x)\}$$

describe the set of all the pre-images of 0.

Solve $\sin(x) = 0$:

$$x = k\pi, \quad \forall \, k \in \mathbb{Z}.$$