The divisionibility relation on $\mathbb{Z}$:

Say $a \mid b$ if $\exists\, k \in \mathbb{Z}$ s.t. $b = a \cdot k$

- If $k \in \mathbb{Z}$ $\quad x = 1 \cdot x \Rightarrow x \mid x \Rightarrow$ "$\mid$" is Reflexive

Let $x, y, z \in \mathbb{Z}$ s.t. $\begin{matrix} x \mid y \\ y \mid z \end{matrix} \Rightarrow$

$\Rightarrow \exists\, k_1, k_2 \in \mathbb{Z}$ s.t. $\left.\begin{matrix} y = k_1 \cdot x \\ z = k_2 \cdot y \end{matrix}\right\} \Rightarrow$

$\Rightarrow z = x(\underbrace{k_1 \cdot k_2}_{\in \mathbb{Z}}) \Rightarrow x \mid z \Rightarrow$ "$\mid$" is transitive

When is "$a \mid b$ and $b \mid a$"?

Def If $a \mid b$ and $b \mid a$ we say that a and b are **associated in divisibility**.

$a \mid b \Rightarrow b = a \cdot k_1$

$b \mid a \Rightarrow a = b \cdot k_2$

$k_1, k_2 \in \mathbb{Z} \Rightarrow$

$\Rightarrow b = b(k_1 \cdot k_2)$

if $b \neq 0 \Rightarrow k_1 \cdot k_2 = 1 \Rightarrow$

$\Rightarrow k_1 = k_2 = 1$ or $k_1 = k_2 = -1 \Rightarrow$

$\Rightarrow a = b$ or $a = -b$

if $b = 0 \Rightarrow a = 0$

Prop: Let $a, b \in \mathbb{Z}$

Then $a \mid b$ and $b \mid a \Leftrightarrow b = \pm a$

$2 \mid -2$

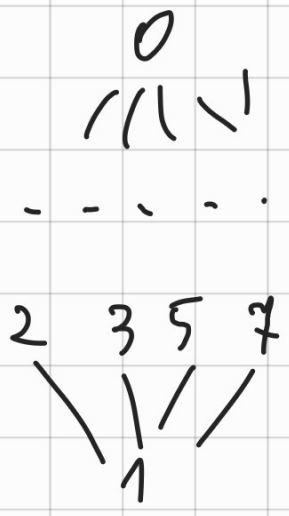
$-2 \mid 2$

$2 \neq -2$ $\Rightarrow (\mathbb{Z}, \mid)$ not an ordered relation on $\mathbb{Z}$

If we restrict to $\mathbb{N} \Rightarrow (\mathbb{N}, \mid)$ is ordered set

$1 \mid a$, $\forall a \in \mathbb{N} \Rightarrow 1$ is the first element in $(\mathbb{N}, \mid)$ "minimum"

$a \mid 0$, $\forall a \in \mathbb{N}$ $0 = 0 \cdot a \Rightarrow 0$ is the largest element in $(\mathbb{N}, \mid)$ "maximum"



Remark: Assume $a \mid b_1$ and $a \mid b_2$

$(a, b_1, b_2) \in \mathbb{Z}$

Then $a \mid u \cdot b_1 + v \cdot b_2 \quad \forall\, u, v \in \mathbb{Z}$

Proof: $b_1 = a \cdot k_1$ for some $k_1, k_2 \in \mathbb{Z}$
$b_2 = a \cdot k_2$

$$u \cdot b_1 + v \cdot b_2 = a(u \cdot k_1 + v \cdot k_2) \Rightarrow$$

$$\Rightarrow a \mid u \cdot b_1 + v \cdot b_2$$

Theorem (Division with reminder in $\mathbb{Z}$)

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then $\exists\, q, r \in \mathbb{Z}$ s.t. $a = bq + r$ and $0 \leq r < |b|$

q and r are unique with those properties

q = "the quotient" of dividing a by b

r = "the reminder"

a = "the dividend" ("deîmpărțit")

b = "the divisor" ("împărțitor")

Proof: $A = \{a - b \cdot x \mid x \in \mathbb{Z},\ a - bx \geq 0\}$

Claim 1: $A \neq \emptyset$

- if $a \geq 0$: $a = a - b \cdot 0 \geq a \in A$
- if $a < 0$:
  - $b > 0$: $a - ba = \overset{<0}{a}(1 - \overset{<0}{b}) \geq 0 \Rightarrow a - ba \in A$
  - OR
  - $b < 0$: HWK

$A \neq \emptyset \Rightarrow$ Let $r := \min A \Rightarrow$

$\Rightarrow \exists\, q \in \mathbb{Z}$ with $a - bq = r$

Claim 2: $0 \leq r < |b|$

$A \subset \mathbb{N} \Rightarrow r \geq 0$

Assume by contradiction that $r > |b|$

$r = a - bq \geq |b|$

$a - bq - |b| \geq 0$

$r - |b| = a - b[q + \operatorname{sgn}(b)] \geq 0$

$\Rightarrow r - |b| \in A$

$\min A = r$

$r - |b| < r$

$\Rightarrow$ contradiction $\Rightarrow r < |b|$

Claim 3 r and q with the given properties are unique

Say $a = bq + r = b \cdot q_1 + r_1$, with $q_1, r_1 \in \mathbb{Z}$, $0 \leq r_1 < |b|$

$b(q - q_1) = r_1 - r$

$|r_1 - r| < |b| \Leftrightarrow$

$\Leftrightarrow |b| \cdot |q - q_1| < |b|$

If $|q - q_1| \neq 0 \Rightarrow 1 \leq |q - q_1|$

$|b| \leq |b| \cdot |q - q_1| < |b|$ false

$\Rightarrow |q - q_1| = 0 \Rightarrow q - q_1 = 0 \Leftrightarrow q = q_1 \Rightarrow$

$\Rightarrow r_1 - r = b(q - q_1) \Leftrightarrow r_1 - r = 0 \Leftrightarrow r_1 = r$

Example: Divide

- $a = 23$ to $b = 4$

  $a \quad b \quad q \quad r$

  $23 = 4 \cdot 5 + 3$

- $a = -23$ to $b = 4$

~~$-23 = 4 \cdot (-5) + (-3)$~~

  $a \quad b \quad q \quad r$

  $-23 = 4 \cdot (-6) + 1$