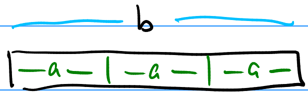
Number Theory.

The study of $\mathbb{N}$ (and $\mathbb{Z}$).

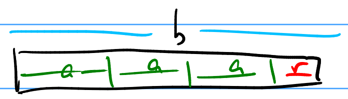
Divisibility (idea: generalize "even": "threeven", etc.)

Def'n If $a, b \in \mathbb{Z}$ we say a (evenly) divides b if there exists an integer $k \in \mathbb{Z}$ such that $k \cdot a = b$.

Intuitively:



a divides b



a does not divide b.

We write $a \mid b$ to mean "a divides b".

(Not in DISCO: have to write a divides b.)

Properties of divisibility relation?

Theorem For all $a, b, c \in \mathbb{Z}$:

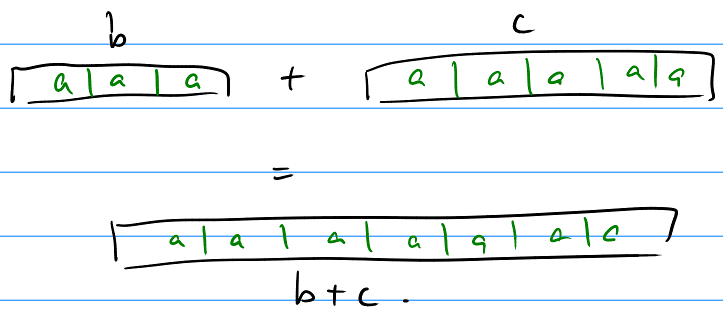
(i) if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$.

(ii) $a \mid a$.

(iii) If $a \mid b$, then $a \mid bc$.

(iv) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Let's prove (i). First, a picture:



Proof. $\forall a,b,c : \mathbb{Z}.\ ((a \mid b) \wedge (a \mid c)) \longrightarrow (a \mid (b+c))$.

Let a,b,c be arbitrary integers.

- Suppose $(a \mid b)$ and $(a \mid c)$, that is there exist integers j and k such that $ja = b$ and $ka = c$.
  We must show $a \mid (b+c)$, that is, there is some ℓ such that $\ell a = b+c$.

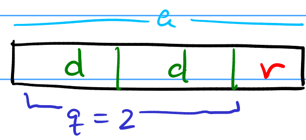
$$\begin{aligned}
& b+c \\
= & \quad \{\text{subst.}\} \\
& ja + ka \\
= & \quad \{\text{factor}\} \\
& (j+k)a
\end{aligned}$$

So we can take $\ell = j+k$. ∎

The Division Algorithm (not actually an algorithm! It's a theorem)

Thm Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ (positive integers). Then there exist unique integers q and r such that:

1. $a = qd + r$
2. $0 \le r < d$.



Proof? Later — requires induction.

$$\begin{array}{r} 2 \text{ R } 1 \\ 3 \overline{)\,7} \end{array}$$

q is called quotient, r is called remainder.

$q = a \text{ div } d$ (Java: a / d; Python, Disco: $a // d$)

$r = a \text{ mod } d$ (Java, python, C++, disco: $a \% d$)

Ex. What is quotient & remainder when 101 is divided by 11?

$101 \text{ div } 11 = q = 9$

$101 \text{ mod } 11 = r = 2$.

want
- $101 = 11q + r$ ✓
- $0 \le r < 11$. ✓

Ex. $7 \text{ div } 11 = 0$ check: $7 = 11 \cdot 0 + 7$ ✓

$7 \text{ mod } 11 = 7$ $0 \leq 7 < 11$ ✓

Ex. $-24 \text{ div } 11 = -3$! want: $-24 = 11 \cdot q + r$

$-24 \text{ mod } 11 = 9$ $0 \leq r < 11$