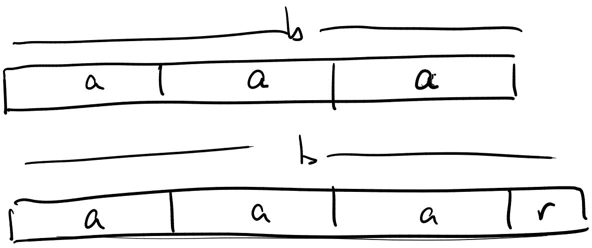
Divisibility

Defn If $a, b \in \mathbb{Z}$, we say a divides b iff there exists some $k \in \mathbb{Z}$ such that $b = ak$.

We say
- b is a multiple of a
- a is a divisor of b
- a is a factor of b.



a divides b

a does not divide b.

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

$a \nmid b$ to mean "a does not divide b", i.e. $\neg(a \mid b)$.

Eg.

$3 \mid 6$ ✓ $(k=2)$

$5 \mid 16$ ✗

$5 \mid -15$ ✓ $(k=-3)$

$4 \mid 4$ ✓ $(k=1)$

$8 \mid 4$ ✗

$4 \mid 8$ ✓

divisibility relation is not symmetric.

$0 \mid 3$ ✗

$3 \mid 0$ ✓ $(k=0)$

$0 \mid 0$ ✓ $(k=172)$

Note it is reflexive.

Theorem. Let $a, b, c \in \mathbb{Z}$. Then:

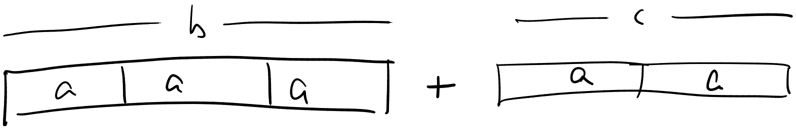
(i) $a \mid a$ (reflexive)

(ii) if $a \mid b$ and $b \mid c$ then $a \mid c$ (transitive).

(iii) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$. ←

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

Proof of (iii).



Let a, b, c be arbitrary integers. Suppose $a \mid b$ and $a \mid c$; we will show $a \mid (b+c)$.

Since $a \mid c$, there is some integer k such that $\boxed{c = ka.}$ know.
Since $a \mid b$, " " " " j " " $\boxed{b = ja.}$
Now $\underline{b+c} = ja + ka = (j+k)a$. $j+k$ is an integer, so by definition $a \mid (b+c)$, since we showed that $b+c$ = some integer times a. ∎

Aside:

$$(a \mid b) \longleftrightarrow (\exists k : \mathbb{Z}.\ k \cdot a = b)$$
$$(a \leq b) \longleftrightarrow (\exists k : \mathbb{N}.\ k + a = b)$$

Divisibility : multiplication :: $\leq$: addition

Division Algorithm

positive integers.

Theorem. Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there exist unique integers q and r such that $0 \leq r < d$ and $a = qd + r$.

q is the quotient and r is the remainder. We will write

$q = a \text{ div } d$ —— / in Java*, // in Python, 'div' in Haskell or disco
$r = a \bmod d$. —— % in Java*, Python, etc., mod in Disco, Haskell, etc.

* WRONG.

eg. What are the quotient + remainder when 101 is divided by 11?

Want q, r such that $101 = \underline{11q + r}$, $\underline{0 \le r < 11}$.

$q = 9$, $r = 2$. ✓

eg. 55 divided by 11?

$q = 5$, $r = 0$.

eg. 7 divided by 11? $7 = 11q + r$, $0 \le r < 11$

$7 \text{ div } 11 = 0$

$7 \bmod 11 = 7$

eg. -24 divided by 11? $-24 = 11q + r$, $0 \le r < 11$

$-24 \text{ div } 11 = -3$

$-24 \bmod 11 = 9$.