Divisibility

Defn Let $a, b \in \mathbb{Z}$. We say that a *divides* b iff there exists $k \in \mathbb{Z}$ such that $ka = b$.

We also say a is a *divisor* or *factor* of b, and b is a *multiple* of a.

We write $a \mid b$ for "a divides b".

We also write $a \nmid b$ as abbreviation for $\neg(a \mid b)$.

Ex

$3 \mid 6$ ✓ $(k = 2)$

$5 \nmid 16$

$5 \mid -15$ ✓ $(k = -3)$

$4 \mid 4$ ✓ $(k = 1)$

$4 \mid 8$ ✓ $(k = 2)$

$8 \nmid 4$

$0 \nmid 3$

$3 \mid 0$ ✓ $(k = 0)$

$0 \mid 0$ ✓ $(k = 0$, or $k = 29$, etc.)

divides is reflexive.

→ divides relation is not symmetric.

Theorem

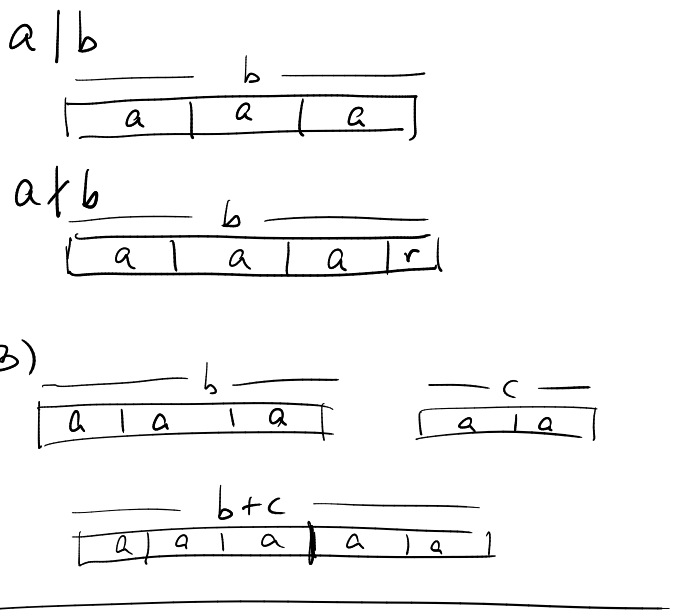
For all $a, b, c \in \mathbb{Z}$,

1. $a \mid a$ (ie. $\mid$ is reflexive)
2. if $a \mid b$ and $b \mid c$, then $a \mid c$ (transitive)
3. if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
4. if $a \mid b$, then $a \mid bc$.

Proof of (3). Let $a, b, c \in \mathbb{Z}$ be arbitrary, and suppose $a \mid b$ and $a \mid c$. That is, there is some $k \in \mathbb{Z}$ such that $ka = b$ (know) and some $j \in \mathbb{Z}$ such that $ja = c$ (know).

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

So $a \mid (b+c)$, since $b+c$ equals some integer times a.



Note:

restrict to $\mathbb{N}$.

$$(a \mid b) \longleftrightarrow (\exists k \in \mathbb{N}.\ k \cdot a = b)$$

$$(a \leq b) \longleftrightarrow (\exists k \in \mathbb{N}.\ k + a = b)$$

≤ is to + as | is to ×.