

# Euclidian Division In $\mathbb{Z}$

Definition: -----

for  $a, b \in \mathbb{Z}^+ \times \mathbb{Z}_*$  we say that  $b$  divides  $a$ :

$\exists q \in \mathbb{Z}, a = q \cdot b$  and we denote by  $b|a$

-----

1) if  $a|1$  if and only if  $a = \pm 1$

Proof:

$$\begin{aligned} a|1 &\Leftrightarrow \exists q \in \mathbb{Z}, 1 = q \times a \text{ this is true only if } q = a = 1 \text{ or } q = a = -1 \\ &\Leftrightarrow a = \pm 1 \end{aligned}$$

2)  $\forall a \in \mathbb{Z}^*, a|0$

Proof:

$$\forall a \in \mathbb{Z}^* a|0 \Leftrightarrow \exists q \in \mathbb{Z}, 0 = q \times a \text{ this is always true for } q = 0$$

3)  $a|b$  and  $b|a$  if and only if  $a = \pm b$

Proof:

$$\begin{aligned} a|b &\Leftrightarrow \exists q \in \mathbb{Z}, b = q \times a \\ b|a &\Leftrightarrow \exists q' \in \mathbb{Z}, a = q' \times b \\ &\Leftrightarrow b = q \times q' \times b \text{ this is true only if } q = q' = 1 \text{ or } q = q' = -1 \\ &\Leftrightarrow a = \pm b \end{aligned}$$

4) if  $a|b$  and  $b|c$  then  $a|c$

Proof:

$$\begin{aligned} a|b &\Leftrightarrow \exists q \in \mathbb{Z}, b = q \times a \\ b|c &\Leftrightarrow \exists q' \in \mathbb{Z}, c = q' \times b \\ &\Leftrightarrow q'' = q \times q' \in \mathbb{Z}, c = q'' \times a \\ &\Leftrightarrow a|c \end{aligned}$$

5) if  $b|a$  and  $b|c$  then  $\forall k, l \in \mathbb{Z} \quad b|ka + lc$

Proof:

$$\begin{aligned} b|a &\Leftrightarrow \exists q \in \mathbb{Z}, a = q \times b \\ b|c &\Leftrightarrow \exists q' \in \mathbb{Z}, c = q' \times b \\ &\Leftrightarrow \forall k, l \in \mathbb{Z} \quad ka + lc = (kq + lq') \times b \text{ and } q'' = kq + lq' \in \mathbb{Z} \\ &\Leftrightarrow b|ka + lc \end{aligned}$$