Divisors

Definition

Let $n \in \mathbb{Z}$. The set of *divisors* of n, denoted D_n, is given by:

$$D_n = \{d \in \mathbb{Z} \mid d \mid n\}$$

Theorem

$$D_0 = \mathbb{Z}$$

Proof

$\implies$ By definition, $D_0 \subseteq \mathbb{Z}$.

$\impliedby$ Assume $d \in \mathbb{Z}$

$$\begin{aligned}
&0 \in \mathbb{Z} \\
&0d = 0 \\
&d \mid 0 \\
&d \in D_0 \\
&\mathbb{Z} \subseteq D_0
\end{aligned}$$

$\therefore D_0 = \mathbb{Z}$

Theorem

Let $n \in \mathbb{Z}, n \neq 0$:

$$0 \notin D_n$$

Proof

ABC: $0 \in D_n$
$\exists\, k \in \mathbb{Z}, k0 = 0 = n$
CONTRADICTION!
$\therefore 0 \notin D_n$

Theorem

$$\forall\, n \in \mathbb{Z}, D_n = D_{-n}$$

Proof

Assume $n \in \mathbb{Z}$

$$\begin{aligned} d \in D_n &\iff d \mid n \\ &\iff \exists\, k \in \mathbb{Z}, kd = n \\ &\iff \exists\, -k \in \mathbb{Z}, (-k)d = -n \\ &\iff d \mid -n \\ &\iff d \in D_{-n} \end{aligned}$$

Theorem

$\forall\, n \in \mathbb{Z}, D_n \neq \emptyset$. In fact:

$$\forall\, n \in \mathbb{Z}, \{\pm 1, \pm n\} \subseteq D_n$$

Proof

Assume $n \in \mathbb{Z}$

$1 \in \mathbb{Z}$
$n1 = n$
$\therefore 1, n \in D_n$

$-n \in \mathbb{Z}$
$-1 \in \mathbb{Z}$
$(-n)(-1) = n$
$\therefore -1, -n \in D_n$

Theorem

Let $n \in \mathbb{Z}, n \neq 0$. D_n is finite. In fact:

$$\forall\, d \in D_n, 1 \leq |d| \leq |n|$$

Proof

Assume $d \in D_n$

$|d| \geq 0$
$0 \neq D_n$
$1 \in D_n$
$\therefore 1 \leq |d|$

$\exists\, k \in \mathbb{Z}^+, k\,|d| = |n|$
But $k\,|d| \geq |d|$, since $k \geq 1$
$\therefore |d| \leq |n|$