Warm-Up: Let $x, y \in \mathbb{Z}$. Show that if xy is even, then x is even or y is even.

Divisibility

Def: Let d and n be integers. We say <u>d divides n</u> if there exists an integer k such that $n = dk$.

Note on definitions: A definition is a $\Leftrightarrow$ statement, but it is often written as a $\Rightarrow$ statement.

So

$$d \text{ divides } n \Leftrightarrow (\exists k \in \mathbb{Z})(n = dk)$$

Notation: $d \mid n$ means "d divides n"

Ex: $2 \mid n \Leftrightarrow n = 2k$ for some $k \in \mathbb{Z}$
$\Leftrightarrow n$ is even.

Ex: $3 \mid n \Leftrightarrow n = 3k$ for some $k \in \mathbb{Z}$

So 3 divides 3 $(3 = 3 \cdot 1)$
" " 9 $(9 = 3 \cdot 3)$
" " -6 $(-6 = 3 \cdot (-2))$
" " 0 $(0 = 3 \cdot 0)$

Ex: • Every integer d divides 0, because $0 = d \cdot 0$.

• 1 divides every integer n, because $n = 1 \cdot n$.

• 0 only divides itself, because $n = 0 \cdot k \Rightarrow n = 0$.

Def: When $d \mid n$, we say d is a <u>divisor</u> of n and n is a <u>multiple</u> of d.

Ex: The divisors of 15 are $\pm 1, \pm 3, \pm 5, \pm 15$.

Warning: $d \mid n$ is the <u>sentence</u> "d divides n"
d/n is the <u>number</u> $\frac{d}{n}$

Note: When $d \neq 0$,

$$d \mid n \text{ is true} \iff n = d \cdot k \text{ for some } k \in \mathbb{Z}$$
$$\iff \frac{n}{d} \text{ is an integer}$$

We usually avoid division, as that can take us out of the integers.

Thm: Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $(-d) \mid n$.

Proof: Suppose $d \mid n$. Then there exists $k \in \mathbb{Z}$ such that $n = dk$. Then

$$n = [(-1)\cdot(-1)]\cdot dk = (-d)(-k)$$

Since $-k \in \mathbb{Z}$, this shows $(-d) \mid n$. ■

For this reason, we often only list positive divisors.

Thm: Let $d, n \in \mathbb{N}$. If $d \mid n$, then $d \leq n$.

Proof: Suppose $d \mid n$. Then there exists $k \in \mathbb{Z}$ such that

$$n = dk.$$

Now, $k \leq 0$ or $k \geq 1$.

Suppose, for the sake of contradiction, that $k \leq 0$. Since $d > 0$, $n = dk \leq 0$, which contradicts $n \in \mathbb{N}$.

So $k \geq 1$. Multiply by d to get

$$dk \geq d$$

i.e. $n \geq d$. ∎

Thm: For any $a, b, c \in \mathbb{N}$,

1. $a \mid a$. [Reflexivity]
2. If $a \mid b$ and $b \mid a$, then $a = b$. [Antisymmetry]
3. If $a \mid b$ and $b \mid c$, then $a \mid c$. [Transitivity]

Proof: HW 10.

This theorem says divisibility is a <u>partial order</u> on $\mathbb{N}$.

Another partial order is $\leq$.