

Warm-Up: Let  $d, n, m \in \mathbb{Z}$ . Prove that if  $d|n$  and  $d|m$ , then  $d|(n+m)$ .

---

Warning:  $d|n$  is the sentence "d divides n"  
 $d/n$  is the number  $\frac{d}{n}$

Note: When  $d \neq 0$ ,

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

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

- 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  $n = 0 \cdot k \Rightarrow n = 0$ .

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.

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

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

Proof: Suppose  $d|n$ . 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  $a|a$ . [Reflexivity]

② If  $a|b$  and  $b|a$ , then  $a=b$ . [Antisymmetry]

③ If  $a|b$  and  $b|c$ , then  $a|c$ . [Transitivity]

Proof: HW 10.

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

Another partial order is  $\leq$ .