Divisor

Example. The following mean the same thing:

- 24 is a multiple of 4.
- 4 is a divisor of 24. (**Notation:** $4 \mid 24$.)

Not the same as $\frac{24}{4}$.

Non-example. The following mean the same thing:

- 32 is *not* a multiple of 7.
- 7 is *not* a divisor of 32. (**Notation:** $7 \nmid 32$.)

Discuss in your group:

(a) Is 6 a divisor of 72? Why or why not?

(b) Is 7 a divisor of 90? Why or why not?

(c) Write down a precise definition of "d is a divisor of n."

Note: Here, d and n are integers.

(d) Find the greatest common divisor of 5 and 8.

(e) Find integers x and y such that $5x + 8y = 1$.

Examples:

$n = d \cdot k$

- 6 is a divisor of 72, because $72 = 6 \cdot 12$.
- 7 is *not* a divisor of 90. There's no integer k where $90 = 7 \cdot k$.

Definition. Let $d, n \in \mathbb{Z}$. We say that d is a divisor of n when $n = d \cdot k$ for some integer k (and we write $d \mid n$).

Examples:

- $\gcd(5, 8) = 1$. (Thus, 5 and 8 are *relatively prime*.)
- $5x + 8y = 1$ has an integer solution, e.g., $(-3, 2)$. $(5, -3)$ $(-11, 7)$

Theorem (GCD theorem): Let $\overset{5}{a}, \overset{8}{b} \in \mathbb{Z}$. If $\gcd(a, b) = 1$, then there exist integers x and y such that $ax + by = 1$.

Remark. We will not prove the GCD theorem today.

Instead, we will use it to prove a bunch of other statements.

Theorem: If there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$, then $\gcd(a, b) = 1$.

Proof: Assume there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$. Let $d = \gcd(a, b)$.

Thus, $d \mid a$, $d \mid b$, and $d > 0$.

So, $a = dk$ and $b = dj$ where $k, j \in \mathbb{Z}$.

Now
$$ax + by = (dk)x + (dj)y = d(kx + jy).$$

Hence $d(kx + jy) = 1$ so that $d \mid 1$.

So, $d = 1$ or -1, but $d > 0$. Then $d = 1$.

Thus, $\gcd(a, b) = 1$.

Rough draft:

$d = \gcd(a, b)$.

$\Rightarrow d \mid a, \; d \mid b \quad (d > 0)$.

$\Rightarrow a = dk, \; b = dj$.

$$ax + by = (dk)x + (dj)y = d(kx + jy).$$

$\Rightarrow d(kx + jy) = 1, \; d \mid 1$

$\Rightarrow d = 1$ or $\cancel{-1}$.

$d = 1$. :)