Divides

For integers $x, y$ we say $x|y$ ("$x$ divides $y$") iff there is an integer $z$ such that $xz = y$.

Which of these are true?

2|4  4|2  2|−2
5|0  0|5  1|5

A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
There exist unique integers $q, r$ with $0 \leq r < d$
Such that $a = dq + r$

Remember when non integers were still secret, you did division like this?

$q$ is the "quotient"
$r$ is the "remainder"
Claim: for all \( a, b, c, n \in \mathbb{Z}, n > 0 \): \( a \equiv b \mod n \rightarrow a + c \equiv b + c \mod n \)

Before we start, we must know:
1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

**Divides**

For integers \( x, y \) we say \( x|y \) ("\( x \) divides \( y \)"") iff there is an integer \( z \) such that \( xz = y \).

**Equivalence in modular arithmetic**

Let \( a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z} \) and \( n > 0 \).
We say \( a \equiv b \mod n \) if and only if \( n|(b - a) \).

---

**Another Proof**

For all integers, \( a, b, c \): Show that if \( a \nmid (bc) \) then \( a \nmid b \) or \( a \nmid c \).

Proof:

Let \( a, b, c \) be arbitrary integers, and suppose \( a \nmid (bc) \).
Then there is not an integer \( z \) such that \( az = bc \)
...

So \( a \nmid b \) or \( a \nmid c \)