

You try---setup

Claim: for all integers a, b, c, n , with $n > 0$:

$$a \equiv b \pmod{n} \rightarrow a + c \equiv b + c \pmod{n}$$

Proof:

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 $a \equiv b \pmod{n}$ if and only if $n|(b - a)$

Another Proof (statement)

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

Signs you might want to use proof by contrapositive

1. The hypothesis of the implication you're proving has a "not" in it (that you think is making things difficult)
 2. The target of the implication you're proving has an "or" or "not" in it.
 3. There's a step that is difficult forward, but easy backwards
e.g., taking a square-root forward, squaring backwards.
 4. You get halfway through the proof and you can't "get ahold of" what you're trying to show.
e.g., you're working with a "not equal" instead of an "equals" or "every thing doesn't have this property" instead of "some thing does have that property"
- All of these are reasons you **might** want contrapositive. Sometimes you just have to try and see what happens!

GCD and LCM definitions

Greatest Common Divisor

The Greatest Common Divisor of a and b ($\gcd(a,b)$) is the largest integer c such that $c|a$ and $c|b$

Least Common Multiple

The Least Common Multiple of a and b ($\text{lcm}(a,b)$) is the smallest positive integer c such that $a|c$ and $b|c$.