# Claim 2

Definitions:
$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$
$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers $a, b, c, d$ and positive integer $m$, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

# The Properties of Congruence We've Proven

- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

You may use these properties in your homework without re-proving them!

## Greatest Common Divisor

Definition:

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

For Example:

$\gcd(99,18) = 9$ $\quad\quad$ $\gcd(7,11) = 1$

$\gcd(100, 125) = 25$ $\quad\quad$ $\gcd(13,0) = 13$

## So…what's it good for?

Remember everything we're learning contributes to us eventually understanding RSA. This is a key step in generating keys.

Suppose I want to solve $7x \equiv 1 \ (mod\ n)$

Just multiply both sides by $\frac{1}{7}$…

Oh wait. We want a number to multiply by 7 to get 1.

What number can we pick?