More proofs

Show that if $a \equiv b (mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Step 1: What do the words mean?

Step 2: What does the statement as a whole say?

Step 3: Where do we start?

Step 4: What's our target?

Step 5: Now prove it.

Another Proof

Show that if $a \equiv b (mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let a, b, c, d, n be integers, $n \geq 0$
and suppose $a \equiv b (mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$n??= bd - ac$

$n|(bd - ac)$

$ac \equiv bd (mod\ n)$

GCD and LCM

Greatest Common Divisor

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

Least Common Multiple

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

Try a few values…

gcd(100,125)

gcd(17,49)

gcd(17,34)

gcd(13,0)

lcm(7,11)

lcm(6,10)