Show that :

$\forall a,b \in \mathbb{Z},\ a,b \neq 0$

$a|b$ and $b|a \Leftrightarrow a = \pm b$

You may use the fact that the product of two integers is 1 iff both are 1 or both are -1.

$6|18$ $\qquad 18 \nmid 6$

$3|3$ $\qquad 3|3$

$5|-5$ $\qquad -5|5$

(1) $a|b$ and $b|a \Rightarrow a = \pm b$

$a|b \Rightarrow \exists n \in \mathbb{Z}$ s.t. $b = na$ [Def of divisibility]

$b|a \Rightarrow \exists m \in \mathbb{Z}$ s.t. $a = mb$ [Def of divisibility]

$\Rightarrow b = n(mb)$

$\Rightarrow nm = 1$

The product of 2 integers is 1 iff both are 1 or both are -1.

$n = m = \pm 1$

Plug in above, gives that $a = \pm b$

(2) $a = \pm b \Rightarrow a|b$ and $b|a$

$\Rightarrow a = n \cdot b$ for $n = \pm 1 \in \mathbb{Z}$

$\Rightarrow b|a$ [Def of divisibility]

$b = \pm a$

$\Rightarrow b = na$ for $n = \pm 1 \in \mathbb{Z}$

$\Rightarrow a|b$

$a = \pm b \Rightarrow a|b$ and $b|a$

Double-tap to enter text

Modular

Definition

Double-tap to enter text

Double-tap to enter text

Double-tap to enter text

Double-tap to enter text

Def: If $a,b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a is congruent to b modulo m iff

$m|(a-b)$

Notation: $\boxed{a \equiv b \pmod m}$ "is congruent to"

$a \not\equiv b \pmod m$

$a \equiv b \pmod m\ \forall m \in \mathbb{Z}^+$

iff

$m|(a-b)$

Is $\overset{a}{17}$ congruent to $\overset{b}{5}$ modulo $\overset{m}{6}$?

$6|(17-5)$

$6|12$?

Yes!

$17 \equiv 5 \pmod 6$

$24 \overset{?}{\equiv} 14 \pmod 6$

$6|(24-14)$

$6 \nmid 10$

No!

$24 \not\equiv 14 \pmod 6$

Are 5 and -4 congruent modulo 3?

$3|(5-(-4))$

$3|9$ ✓

Yes!

$5 \equiv (-4) \bmod 3$

What are 2 numbers that are congruent modulo 3?

$a = 10 \quad b = 4$

$3|(10-4)$

$3|6$ ✓

Theorem: Let a rem m be the remainder when a is divided by m.

$\boxed{a \equiv b \pmod m \Leftrightarrow a \text{ rem } m = b \text{ rem } m}$

That is, $a \equiv b \pmod m$ iff a & b have the same remainder when divided by m

e.g. $17 \equiv 5 \pmod 6$

17 rem $6 = 5$

5 rem $6 = 5$

You may assume Euclid's remainder theorem which says that given any $m \in \mathbb{Z}^+$ and any $a \in \mathbb{Z}$ $\exists$ a unique pair of quotient and remainder $q, r \in \mathbb{Z}$ s.t.

$a = qm + r \qquad 0 \leq r < m$

$\frac{101}{11} \Rightarrow 101 = 11 \cdot \boxed{9} + \boxed{2}$

(I) $\underbrace{a \text{ rem } m = b \text{ rem } m}$ $\Rightarrow a \equiv b \pmod m$

$a = q_a m + r_a \qquad 0 \leq r_a, r_b < m$

$b = q_b m + r_b$

We know: $r = r_a = r_b$ b/c a rem m = b rem m

$\Rightarrow a = q_a m + r \qquad r = a - q_a m$

$b = q_b m + r \qquad r = b - q_b m$

$a - q_a m = b - q_b m$

$\Rightarrow a - b = q_a m - q_b m$

$\Rightarrow a - b = (q_a - q_b) m$

$q' = q_a - q_b$

We know that $q' \in \mathbb{Z}$ b/c integers are closed w.r.t. subtraction

$\Rightarrow \exists q' \in \mathbb{Z}$ s.t $(a-b) = q'm$

$\Rightarrow m|(a-b)$