Definition 1: Given $m \in \mathbb{Z}^+$, $a \equiv b \mod m$ iff $m \mid (a-b)$

1. Let a rem m be the remainder when a is divided by m. You may assume Euclid's remainder theorem, which says that, given any positive integer m and any integer a, $\exists$ a unique pair of quotient and remainder $q, r \in \mathbb{Z}$ such that $a = qm + r$ and $0 \le r < m$. Show that

$$a \equiv b \mod m \iff a \text{ rem } m = b \text{ rem } m$$

Begin by expressing a & b as follows using the remainder theorem:

$$a = q_a m + r_a$$
$$b = q_b m + r_b$$

I) a rem m = b rem m $\Rightarrow$ $\underline{a \equiv b \mod m}$ $(m \mid (a-b))$

$a = q_a m + r_a$ $\quad 0 \le r_a, r_b < m$

$b = q_b m + r_b$

We know $r_a = r_b$

Hence, $a = q_a m + r_a$

$b = q_b m + r_a$

$a - b = q_a m + r_a - (q_b m + r_a)$

$= q_a m + \cancel{r_a} - q_b m - \cancel{r_a}$

$= q_a m - q_b m$

$a - b = \underbrace{(q_a - q_b)}m$

Let $q = q_a - q_b$ $\because$ Integers are closed w.r.t subtraction (subtracting 2 integers results in an integer). $q_a, q_b \in \mathbb{Z}$

$\Rightarrow q \in \mathbb{Z}$

$\Rightarrow \exists q = q_a - q_b \in \mathbb{Z}$ s.t $a - b = qm$

$\Rightarrow m \mid (a-b)$ (Def of Divisibility)

$\Rightarrow a \equiv b \pmod m$ [Def of $a \equiv b \mod m$] (see above)

II) $a \equiv b \pmod m$ $\Rightarrow$ a rem m = b rem m

$a \equiv b \pmod m$

$\Rightarrow m \mid (a-b)$

$\Rightarrow \exists k \in \mathbb{Z}$ s.t. $(a-b) = k \cdot m$

$\Rightarrow \exists k \in \mathbb{Z}$ s.t. $\boxed{a = b + km}$

a can also be written as

$\boxed{a = q_a m + r_a}$ $\quad 0 \le r_a < m$ (Euclid's rem. theorem)

$\Rightarrow b + k \cdot m = q_a m + r_a$

$\Rightarrow b = q_a \cdot m - k \cdot m + r_a$ $\quad 0 \le r_a < m$

$\boxed{b = (q_a - k) m + r_a}$ $\quad \Downarrow$ a rem m

We know that $0 \le r_a < m$ and $q_a - k \in \mathbb{Z}$. By Euclid's remainder theorem, $\exists$ a <u>unique</u> q, r s.t. $b = \underbrace{(q_a - k)} m + \underbrace{r_a}$

$\Rightarrow r_a$ is the remainder when dividing b by m

$\Downarrow$

$\Rightarrow r_a = a$ rem m $\quad r_a = b$ rem m

$\Rightarrow a$ rem m = b rem m = r_a

$a \equiv b \pmod m \iff a$ rem = b rem