Congruence

Definition: Let a and b be integers with $a \neq 0$. We say that a *divides* b, written $a|b$, if there exists some integer c such that $b = ac$.

Definition: Let a and b be integers and let m be a positive integer. We say that a is *congruent to* b *modulo* m, written $a \equiv b \pmod{m}$, if m divides $a - b$.

Example: $34 \equiv 10 \pmod{6}$ since $34 - 10 = 24$ and 6 divides 24; however, $34 \not\equiv 10 \pmod{7}$ since 7 does not divide 24.

Theorem: Let a and b be integers and let m be a positive integer. Then the following are equivalent.

(i) $a \equiv b \pmod{m}$

(ii) $a = b + km$ for some $k \in \mathbb{Z}$

(iii) a **mod** $m = b$ **mod** m

Note: In order to prove (i $\leftrightarrow$ ii) $\wedge$ (ii $\leftrightarrow$ iii) $\wedge$ (iii $\leftrightarrow$ i), we only need to prove (i $\rightarrow$ ii) $\wedge$ (ii $\rightarrow$ iii) $\wedge$ (iii $\rightarrow$ i), since the other implications follow from the hypothetical syllogism rule of inference.

Proof:
First note that by the Division Algorithm (if a and b were divided by m) there exist integers q_1, q_2, r_1 and r_2 with $0 \leq r_1 < m$ and $0 \leq r_2 < m$ such that $a = mq_1 + r_1$ and $b = mq_2 + r_2$. Since $0 \leq r_1 < m$ and $0 \leq r_2 < m$, then $|r_1 - r_2| < m$. Moreover these remainders are (by definition) $r_1 = a$ **mod** m and $r_2 = b$ **mod** m.

(i $\rightarrow$ ii)
Assume $a \equiv b \pmod{m}$. Then $m|(a-b)$ and so $a-b = mk$ for some $k \in \mathbb{Z}$. Thus $a = b+km$.

(ii $\rightarrow$ iii)
Assume $a = b + km$ for some $k \in \mathbb{Z}$. Then $mq_1 + r_1 = mq_2 + r_2 + km$. Rearranging this equation gives us $r_1 - r_2 = mq_2 - mq_1 + km = m(q_2 - q_1 + k) = mj$, where $j = q_2 - q_1 + k$ is an integer. Therefore $|r_1 - r_2| = m|j|$, which implies $j = 0$ since $|r_1 - r_2| < m$. Since $j = 0$, then $|r_1 - r_2| = 0$, which means $r_1 = r_2$ and so a **mod** $m = b$ **mod** m.

(iii $\rightarrow$ i)
Assume a **mod** $m = b$ **mod** m. Then $r_1 = r_2$ and so $r_1 - r_2 = 0$. Therefore, $a - b = (mq_1 + r_1) - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2) = m(q_1 - q_2) = mk$ where $k = q_1 - q_2$ is an integer. Thus, $m|(a - b)$ and so $a \equiv b \pmod{m}$. ■

Example: $34 \equiv 10 \pmod{6}$ since $6|(34-10)$, $34 = 10+4\cdot 6$, and 34 **mod** $6 = 4 = 10$ **mod** 6.

Example: $40 \equiv 19 \pmod{7}$ since $7|(40-19)$, $40 = 19+3\cdot 7$, and 40 **mod** $7 = 5 = 19$ **mod** 7.