CSCI 2312: Discrete Structures II: Modular Arithmetic

Definition 1: Given $m \in \mathbb{Z}^+$, $a \equiv b \; mod \; m$ if and only if $m|(b-a)$. If $a \equiv b \; mod \; m$, we say "a is congruent to b modulo m".

For example, $3 \equiv 10 \; mod \; 7$, $1 \equiv 3 \; mod \; 2$, $5 \equiv -4 \; mod \; 9$, etc.

Show the following using the proven divisibility results provided to you.

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 $0 \leq r < m$. Show that

$$a \equiv b \; mod \; m \Leftrightarrow a \; rem \; m = b \; rem \; m$$

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

$$a = q_a m + r_a$$

$$b = q_b m + r_b$$

2. Show in discussion next week: Congruence modulo m is an equivalence relation. Do not go into the weeds of the divisibility definition for this problem. The divisibility results are sufficient.