CSci 2312: Discrete Structures II: Modular Arithmetic

Poorvi L. Vora

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.

Recall the definition of equivalence relations in Discrete I. An equivalence was something like an equality, but not quite an equality. We showed in class that $\equiv_m$ is an equivalence relation.

Theorem: $\equiv_m$ is an equivalence relation

Proof: We show that $\equiv_m$ is reflexive, symmetric and transitive.

Reflexive: We need to show that $x \equiv_m x \; \forall \; x \; \in \mathbb{Z}$, that is, that $x \equiv x \; mod \; m$ and that $m \mid (x-x)$.

We show this as follows:

$$0 = 0.m \; and \; 0 \; \in \; \mathbb{Z} \Rightarrow m \mid 0 \Rightarrow m \mid (x-x) \; \forall \; x \; \in \; \mathbb{Z} \; \Rightarrow x \; \equiv \; x \; (mod \; m) \; \forall \; x \; \in \; \mathbb{Z}$$

Hence $x \equiv x \; mod \; m$ and $\equiv_m$ is reflexive.

Symmetric: We need to show that $x \equiv y \; mod \; m \Rightarrow y \equiv x \; mod \; m$.

$$x \equiv y \, mod \, m \Rightarrow m \mid (y-x) \Rightarrow \exists c \in \mathbb{Z} \; such \; that \; y-x = cm \Rightarrow \exists d = -c \in \mathbb{Z} \; such \; that \; x-y = dm \Rightarrow m \mid (x-y)$$

Hence $x \equiv y \; mod \; m \Rightarrow y \equiv x \; mod \; m$ and $\equiv_m$ is symmetric.

Transitive: We need to show that $x \equiv y \; mod \; m \; and \; y \equiv z \; mod \; m \Rightarrow x \equiv z \; mod \; m$

$$x \equiv y \; mod \; m \; and \; y \equiv z \; mod \; m \Rightarrow \exists c_1, c_2 \in \mathbb{Z} \; suchthat (y-x) = c_1 m \; and \; (z-y) = c_2 m$$

$$\Rightarrow (z-x) = (c_1 + c_2)m \Rightarrow (z-x) = dm \; d = (c_1 + c_2) \in \mathbb{Z} \Rightarrow m \mid (z-x) \Rightarrow x \equiv z \; mod \; m$$

Hence $x \equiv y \; mod \; m \; and \; y \equiv z \; mod \; m \Rightarrow x \equiv z \; mod \; m$ and $\equiv_m$ is transitive.

Note that 10, 3, 17, 24, 87, are congruent among themselves $modulo$ 7, because $87-17$ or $17-10$ or $24-87$ are all divisible by 7. In fact, numbers are congruent among themselves when their remainders are the same on division by m. To examine this further, we first need a simple fact.

Theorem: (recall) Let n and m be two integers. There exist unique integers q and r such that $n = qm + r$, and $0 \leq r < m$. r is often denoted $n \; rem \; m$.

From the above examples it appears that the equivalence partitions the set of integers into m sets, each consisting of integers with the same remainder when divided by m. For example, we can show this easily for $m = 2$.

Theorem: Let $x, y \in \mathbb{Z}$, $m = 2$ and x even. Then $x \equiv_2 y \Leftrightarrow y \; is \; even$.

Proof:

$\Rightarrow$

$$x \equiv_2 y \Rightarrow 2 \mid (y-x) \Rightarrow \exists \; c \; in \; \mathbb{Z} \; such \; that \; (y-x) = 2c$$

Because x is even, $\exists n \in \mathbb{Z}$ such that $x = 2n$. Hence

$$\Rightarrow (y - 2n) = 2c \Rightarrow y = 2(n + c) \Rightarrow \exists d = n + c \in \mathbb{Z}\ such\ that\ y = 2d \Rightarrow 2 \mid y$$

and y is even.

$\Leftarrow$ Suppose y is even.

$$y\ even\ \Rightarrow \exists c' \in \mathbb{Z}\ such\ that\ y = 2c' \Rightarrow y - x = 2(c' - c) \Rightarrow \exists d' = c - c' \in \mathbb{Z}\ such\ that\ y - x = 2d'$$

$$\Rightarrow 2 \mid (y - x) \Rightarrow x \equiv y\ mod\ m$$

Hence we have shown that, if x is even, $x \equiv_2 y \Leftrightarrow y\ even$. For practice, you can consider showing that, if x is odd, $x \equiv_2 y \Leftrightarrow\ y\ is\ odd$.

We can show this more generally for all values of m, and not just 2.

Theorem: $a \equiv b \Leftrightarrow a\ rem\ m = b\ rem\ m$.

For example, $10\ rem\ 7 = 3$. Also, $-4\ rem\ 7 = 3$, and $87\ rem\ 7 = 3$, $17\ rem\ 7 = 3$. That is, all of $10, -4, 87, 17, 3$ are equivalent modulo 7 because their remainders when dividing by 7 are identical. That is, $10 \equiv -4\ mod\ 7$, $10 \equiv 87\ mod\ 7$, $-4 \equiv 17\ (mod\ 7)$ etc.