MTHSC 412 Section 2.5 –Congruence of Integers

Kevin James

Congruence modulo n is an equivalence relation on $\mathbb{Z}$

Definition

Let $n > 1$. be an integer. For $x, y \in \mathbb{Z}$, we say that x is congruent to y modulo n and write $x \equiv y \pmod{n}$ if $n | (x - y)$.

Theorem

If $n > 1$ is an integer then $\equiv \pmod{n}$ is an equivalence relation on $\mathbb{Z}$.

Proof.

Let $n > 1$ be an integer.
Reflexive: For $x \in \mathbb{Z}$, $x - x = 0$ which divisible by n. So, $x \equiv x \pmod{n}$ and $\equiv \pmod{n}$ is reflexive.
Symmetric: Suppose that $x \equiv y \pmod{n}$.
Then $n|(x - y) \Rightarrow (x - y) = nk$ for some $k \in \mathbb{Z}$.
So, $(y - x) = n(-k)$. Thus, $n|(y - x)$ and $y \equiv x \pmod{n}$.
Thus $\equiv \pmod{n}$ is symmetric.
Transitive: Suppose that $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$
Then $(x - y) = nk$ and $(y - z) = nm$ for some $k, m \in \mathbb{Z}$.
So, $(x - z) = (x - y) + (y - z) = n(k + m)$ and $n|(x - z)$.
Thus $x \equiv z \pmod{n}$ and $\equiv \pmod{n}$ is transitive.
Since $\equiv \pmod{n}$ is reflexive, symmetric and transitive, it is an equivalence relation on $\mathbb{Z}$. $\square$

Fact

Suppose that $n > 1$ is an integer and that $x, y \in \mathbb{Z}$. $x \equiv y \pmod{n}$ if and only if x and y yield the same remainder upon division by n.

Proof.

Suppose that $n > 1$ is an integer and that $x, y \in \mathbb{Z}$ with $x \geq y$. Using the division algorithm we can write

$$\begin{aligned} x &= nq_1 + r_1 \\ y &= nq_2 + r_2 \end{aligned}$$

Thus $x - y = n(q_1 - q_2) + (r_1 - r_2)$ with $-n < (r_1 - r_2) < n$.
Now note that $n | (x - y)$ if and only if $n | (r_1 - r_2)$.
Finally since $-n < (r_1 - r_2) < n$, $n | (r_1 - r_2)$ if and only if $r_1 = r_2$. $\square$

Definition

We refer to the equivalence classes of $\equiv \pmod{n}$ as *residue classes* or *congruence classes*.

Fact

There are n distinct congruence classes modulo n.

Proof.

Let $x \in \mathbb{Z}$. Use the division algorithm to write $x = nq + r$ with $0 \leq r < n$.
Since, $x - r = nq$, $x \equiv r \pmod{n}$.
Thus each integer is in one of the congruence classes: $[0], [1], \ldots [n-1]$.
The fact that these are distinct follows from our last fact. $\square$

Addition and Multiplication Properties

Theorem

If $a \equiv b \pmod{n}$ *and* $x \in \mathbb{Z}$ *then*

$$a + x \equiv b + x \pmod{n} \quad \textit{and} \quad ax \equiv bx \pmod{n}.$$

Proof.

Suppose that $a \equiv b \pmod{n}$. Then $(a - b) = nk$ for some $k \in \mathbb{Z}$.
Thus $(a + x) - (b + x) = a - b = nk$ and
$ax - bx = x(a - b) = xnk$ and the result follows. □

Theorem

Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

$$a + c \equiv b + d \pmod{n} \quad \textit{and} \quad ac \equiv bd \pmod{n}.$$

Proof.

By our previous theorem, we have
$a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$, and
$c \equiv d \pmod{n} \Rightarrow bc \equiv bd \pmod{n}$.
Thus, $ac \equiv bc \equiv bd \pmod{n}$.
The proof of the other congruence is similar and is left as an exercise. $\square$

Theorem

If $ax \equiv ay \pmod{n}$ *and* $(a, n) = 1$*, then* $x \equiv y \pmod{n}$*.*

Proof.

$$\begin{aligned} ax \equiv ay \pmod{n} &\Rightarrow n|(ax - ay) \\ &\Rightarrow n|a(x - y) \quad \text{and} \quad (a, n) = 1 \\ &\Rightarrow n|(x - y) \\ &\Rightarrow x \equiv y \pmod{n} \end{aligned}$$

□

Theorem

If $(a, n) = 1$, the congruence $ax \equiv b \pmod{n}$ has a solution $x \in \mathbb{Z}$ and the solution is unique modulo *n, which means that any two such solutions are congruent modulo n.*

Proof.

Existence: Since $(a, n) = 1$, there are $s, t \in \mathbb{Z}$ such that

$$\begin{aligned} 1 = as + tn \quad &\Rightarrow \quad b = asb + tnb \\ &\Rightarrow \quad b - a(sb) = tbn \\ &\Rightarrow \quad b \equiv a(sb) \pmod{n} \end{aligned}$$

Thus $x = sb$ is a solution.
Uniqueness modulo n: Suppose that $x, y \in \mathbb{Z}$ are both solutions.
Then $ax \equiv b \equiv ay \pmod{n}$ and $(a, n) = 1$.
By the cancellation law, it follows that $x \equiv y \pmod{n}$. $\square$

Fact

Suppose that $a|c$ and $b|c$ with $(a, b) = 1$. Then $(ab)|c$.

Proof.

Since $a|c$, we can write $c = ak$ for some $k \in \mathbb{Z}$.
So, we have $b|c \Rightarrow b|ak$ and $(b, a) = 1$
which implies that $b|k$.
Thus, $k = br$ for some $r \in \mathbb{Z}$.
Then $c = ak = abr$.
Thus $(ab)|c$. $\square$

Corollary

If $n_1, n_2, \ldots, n_k$ is a set of pairwise coprime integers and if $n_i|c$ for $1 \leq i \leq k$, then $(n_1 n_2 \ldots n_k)|c$.

Theorem

Let $n_1, n_2, \ldots, n_k$ be pairwise coprime integers. Let $a_1, \ldots, a_k \in \mathbb{Z}$. There is $x \in \mathbb{Z}$ satisfying the system of congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k}. \end{cases}$$

Furthermore, the solution is unique modulo $(n_1 n_2 \ldots n_k)$.

Proof.

Existence: Let $N = (n_1 n_2 \dots n_k)$ and let
$N_i = \frac{N}{n_i} = n_1 n_2 \dots n_{i-1} n_{i+1} \dots n_k$.
Then $(N_i, n_i) = 1$ because the n_i are pairwise coprime.
Let M_i be a solution to $N_i x \equiv 1 \pmod{n_i}$.

Then $N_i M_i \equiv \begin{cases} 0 \pmod{n_j} & \text{if } i \neq j, \\ 1 \pmod{n_i} \end{cases}.$

Now let $x = \sum_{i=1}^{k} a_i N_i M_i$.
Then $x \equiv a_j N_j M_j \equiv a_j \pmod{n_j}$ for $j = 1, 2, \dots, k$.
Thus x is a solution.

Uniqueness: Suppose that $x, y \in \mathbb{Z}$ are two solutions.
Then $x \equiv y \pmod{n_i}$ for $i = 1, 2, \dots, k$.
Thus $n_i | (x - y)$ for $i = 1, 2, \dots, k$.
Since the n_i's are pairwise coprime, this implies that
$(n_1 n_2 \dots n_k) | (x - y)$.
Thus $x \equiv y \pmod{N}$ as desired. $\square$