MTHSC 412 Section 2.1 –Congruence and Congruence Classes

Kevin James

Definition

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say that <u>a is congruent to b modulo n</u> and write $a \equiv b \pmod{n}$ when $n|(a-b)$.

Example

1. $1 \equiv 5 \pmod{4}$.
2. $2 \equiv 17 \pmod{3}$.
3. $16 \equiv 4 \pmod{3}$.
4. $1 \not\equiv 5 \pmod{3}$.

Theorem

Let $0 < n \in \mathbb{Z}$. Then $\equiv \pmod{n}$ is an equivalence relation on $\mathbb{Z}$. That is, $\equiv \pmod{n}$ satisfies the following three properties.

Reflexivity $x \equiv x \pmod{n}$ *for all* $x \in \mathbb{Z}$.

Symmetry *If* $x \equiv y \pmod{n}$ *then* $y \equiv x \pmod{n}$.

Transitivity *If* $x \equiv y \pmod{n}$ *and* $y \equiv z \pmod{n}$ *then* $x \equiv z \pmod{n}$

Proof.

Let $n > 0$ 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. □

Theorem

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

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

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. $\square$

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.

Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.
Then $a - b = nj$ and $c - d = nk$ for some $j, k \in \mathbb{Z}$.
So, $(a + c) - (b + d) = (a - b) + (c - d) = nj + nk = n(j + k)$.
Thus, $a + c \equiv b + d \pmod{n}$.
Similarly, we have

$$\begin{aligned} ac - bd &= ac - bc + bc - bd = (a - b)c + b(c - d) \\ &= njc + bnk = n(jc + bk). \end{aligned}$$

Thus $ac \equiv bd \pmod{n}$. $\square$

Definition

Let $0 < n \in \mathbb{Z}$. Then for any $a \in \mathbb{Z}$ we define the <u>congruence class of a modulo n</u> as $[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$.

Note

$$\begin{aligned} [a] &= \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} \\ &= \{b \in \mathbb{Z} \mid n|(b-a)\} \\ &= \{b \in \mathbb{Z} \mid (b-a) = nk \text{ for some } k \in \mathbb{Z}.\} \\ &= \{a + nk \mid k \in \mathbb{Z}\}. \end{aligned}$$

Example

Suppose $n = 5$. Then $[9]$ is an infinite set which contains -6,-1,4,9,14,19 and 24.

Theorem

Suppose that $0 < n \in \mathbb{Z}$ *and* $a, c \in \mathbb{Z}$. *Then* $a \equiv c \pmod{n}$ *if and only if* $[a] = [c]$.

Proof.

Suppose that $0 < n \in \mathbb{Z}$ and $a, c \in \mathbb{Z}$.
($\Rightarrow$): Suppose that $a \equiv c \pmod{n}$.
Let $x \in [a]$.
Then $x \equiv a \pmod{n}$.
Since $a \equiv c \pmod{n}$ and since $\equiv \pmod{n}$ is transitive, $x \equiv c \pmod{n}$.
Thus $x \in [c]$.
We have now shown that $[a] \subseteq [c]$.
Similarly, we can show that $[c] \subseteq [a]$ and so we can conclude that $[a] = [c]$.
($\Leftarrow$): Suppose now that $[a] = [c]$.
By reflexivity, $a \in [a] = [c]$.
Thus, $a \equiv c \pmod{n}$. $\square$

Corollary

Suppose that $0 < n \in \mathbb{Z}$ *and* $a, c \in \mathbb{Z}$. *Either* $[a] \cap [c] = \emptyset$ *or* $[a] = [c]$.

Proof.

Suppose that $0 < n \in \mathbb{Z}$ and $a, c \in \mathbb{Z}$ and that $[a] \cap [c] \neq \emptyset$.
Let $x \in [a] \cap [c]$.
So, we have $x \equiv a \pmod{n}$ and $x \equiv c \pmod{n}$.
By symmetry, we have $a \equiv x \pmod{n}$ and $x \equiv c \pmod{n}$.
By transitivity we have $a \equiv c \pmod{n}$.
By our previous theorem, we now have that $[a] = [c]$. $\square$

Corollary

Let $1 < n \in \mathbb{Z}$.

1. *If* $a \in \mathbb{Z}$ *and* $a = nq + r$ *(e.g.* r *could be the remainder produced when* a *is divided by* n*.), then* $[a] = [r]$.
2. *There are exactly* n *distinct congruence classes modulo* n*, namely* $[0], [1], \ldots, [n-1]$.

Proof.

(1): Suppose that $a = nq + r$.
Then $a - r = nq$.
Thus, $a \equiv r \pmod{n}$.
So, by our theorem, $[a] = [r]$.
(2): Suppose that $a \in \mathbb{Z}$.
Then we can write $a = nq + r$ with $0 \leq r \leq (n-1)$.
So, it follows from part (1) that $[a] = [r]$.
So, we just need to see that $[0], [1], \ldots, [n-1]$ are distinct.
Suppose that $0 \leq i, j \leq (n-1)$ and $[i] = [j]$.
Then $-n < (i-j) < n$ and $i \equiv j \pmod{n} \Rightarrow n \mid (i-j)$.
Thus, $i - j = 0 \Rightarrow i = j$.
Therefore $[0], [1], \ldots, [n-1]$ are distinct. $\square$

Definition

The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$.

Note

From above we see that

$$\begin{aligned} \mathbb{Z}_n &= \{[a] \mid a \in \mathbb{Z}\} \\ &= \{[0], [1], [2], \ldots, [n-1]\}. \end{aligned}$$