Chapter 4: CONGRUENCES AND THE INTEGERS MODULO n

Mphako-Banda

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG
SCHOOL OF MATHEMATICS

LEARNING OUTCOMES FOR THE LECTURE

By the end of this lecture, students will be able to:

- define congruence modulo n on $\mathbb{Z}$
- prove that congruence modulo n is an equivalence relation
- define an equivalence class
- show when two equivalence classes are equal

CONGRUENCE MODULO n

Definition (4.1.1 CONGRUENT MODULO) For a,b $\in$ $\mathbb{Z}$.

Let $n \geq 2$ be an integer. On $\mathbb{Z}$ define $\equiv$ as follows $a \equiv b$ iff $a - b = kn$, $k \in \mathbb{Z}$ iff $n|(a-b)$. In this case we write $a \equiv b \pmod{n}$ and refer to n as the modulus.

Theorem (4.1.2)

$a \equiv b \pmod{n}$, $n \geq 2$ is an equivalence relation on $\mathbb{Z}$. [Congruence modulo n is an equivalence on $\mathbb{Z}$.]

RECALL: n|(a-b) means n divides a-b

PROOF: (Show 'congruence mod n'is an equivalence relation)

(i) $a - a = 0 = 0.n$ so $a \equiv a \pmod{n}$, $0 \in \mathbb{Z}$ ($\therefore \ \equiv$ is reflexive)

(ii) $a \equiv b \pmod{n} \Rightarrow \quad a - b = kn \Rightarrow \quad b - a = (-k)n$

$\Rightarrow \quad b \equiv a \pmod{n}$ as $-k \in \mathbb{Z}$ if $k \in \mathbb{Z}$. ($\therefore \ \equiv$ is symmetric)

(iii) $a \equiv b \pmod{n}$ and $b \equiv d \pmod{n}$

$\Rightarrow \quad a - b = kn$ and $b - d = ln \qquad k, l \in \mathbb{Z}$

$\Rightarrow \quad (a - b) + (b - d) = (k + l)n \qquad k + l \in \mathbb{Z}$

$\Rightarrow \quad a - d = (k + l)n$

$\Rightarrow \quad a \equiv d \pmod{n}$ ($\therefore \ \equiv$ is transitive)

$\therefore \quad \equiv \pmod{n}$ is an equivalence relation on $\mathbb{Z}$.

EQUIVALENCE CLASS

From definition 3.1.2 (this is the most general statement)

$$
\begin{aligned}
[a] &= \{b \in \mathbb{Z} \mid \quad b \equiv a \pmod{n}\} \\
&= \{b \in \mathbb{Z} \mid \quad b - a = kn, \quad k \in \mathbb{Z}\} \\
&= \{b \in \mathbb{Z} \mid \quad b = a + kn, \quad k \in \mathbb{Z}\} \\
&= \{a + kn \mid \quad k \in \mathbb{Z}\} \\
&= \{\cdots, a-3n, a-2n, a-n, a, a+n, a+2n, a+3n, \cdots\}
\end{aligned}
$$

={all b in ℤ such that b is equivalent to a}

We work toward finding a list of elements from the general statement...

From definition 3.1.2

What is the one word that says what an equivalence class is?

A number?

A relation?

A set?

See last slide...

Example: Let $n = 5$.

$$
\begin{aligned}
[0] &= \{0 + 5k| \quad k \in \mathbb{Z}\} \\
&= \{\cdots, -15, -10, -5, 0, 5, 10, 15 \cdots\} \\
&= [5] = [-5] = [10] \qquad \text{(multiples of 5)}
\end{aligned}
$$

$$
\begin{aligned}
[1] &= \{1 + 5k| \quad k \in \mathbb{Z}\} \\
&= \{\cdots, -14, -9, -4, 1, 6, 11, 16 \cdots\} \\
&= [6] = [-9] \qquad \text{((multiples of 5)-1)}
\end{aligned}
$$

all b in Z such that n|(b-a)

[a] contains all elements of Z that are congruent to the number a modulus n...

Definition (4.1.3)

The equivalence class $[a]$ *is called the residue class of a modulo n and may also be denoted by* $\overline{a}$.

Theorem (4.1.4)

Given $n \geq 2$, $[a] = [b]$ *if and only if* $a \equiv b \pmod{n}$.

PROOF: From Theorem 3.2.1, part (ii)***[***$[a] = [b]$ ***if and only if*** $a \approx b$***.]*** We know that $[a] = [b]$ if and only if $a \equiv b$. In this case $[a] = [b]$ if and only if $a \equiv b \pmod{n}$.

We proved in theorem (3.2.1) the conditions for two equivalence classes to be equal, so in the proof of this theorem (4.1.4) we apply the earlier theorem (3.2.1)

.... an equivalence class is a set