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 $\mathbb{Z}_n$, the integers modulo n, and its elements
- ♣ prove that any integer belongs to a residue class in $\mathbb{Z}n$
- ♣ find, for any integer, the residue class it belongs to in $\mathbb{Z}_n$
- ♣
- ♣

INTEGERS MODULO n

Definition (4.2.1) (of integers modulo n, the set denoted $\mathbb{Z}_n$)

The set $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ of all residue classes modulo n is called the set of integers modulo n, where $\overline{a} = [a]$ for $a = 0, 1, 2, \cdots, n-1$. (set of sets.)

Example:

$$\begin{aligned} \mathbb{Z}_2 &= \{\overline{0}, \overline{1}\} \\ \mathbb{Z}_3 &= \{\overline{0}, \overline{1}, \overline{2}\} \\ \mathbb{Z}_5 &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} \end{aligned}$$

(these are all sets containing equivalence classes)

Theorem (4.2.2) (proves 2 things about the elements in $\mathbb{Z}_n$)

If $n \geq 2$ and $a \in \mathbb{Z}$, then $\overline{a} = \overline{r}$ for some integer r where $0 \leq r < n$. Moreover, the residue classes modulo n, $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}$, are distinct and $|\mathbb{Z}_n| = n$.

PROOF: We use the Division algorithm. $a, n \in \mathbb{Z}$, $n \geq 2$ so $\exists q, r \in \mathbb{Z}$ such that $a = qn + r$ where $0 \leq r < n$. Thus $a - r = qn$ and so $a \equiv r \pmod{n}$. By Theorem 4.1.4 $[a] = [r]$, $0 \leq r < n$.
Since $\equiv \pmod{n}$ is an equivalence relation, we know $\overline{a} = \overline{b}$ iff $a - b = kn$, $k \in \mathbb{Z}$. But if $\overline{a} \neq \overline{b}$, $\overline{a}, \overline{b} \in \mathbb{Z}_n$, then $0 \leq a < n$. and $0 \leq b < n$. so $a - b \neq kn$, so elements of $\mathbb{Z}_n$ are distinct. Certainly $|\mathbb{Z}_n| = n$.

We have proved: 1) we may name the elements in $\mathbb{Z}_n$ using the integers from 0 to n-1

2) the elements in $\mathbb{Z}_n$ are disjoint as sets of integers...

Example (4.2.3 (1))

Locate $\overline{48}$ *and* $\overline{-16}$ *in* $\mathbb{Z}_7$.

a) $48 \equiv 6 \pmod 7$, so $\overline{48} = \overline{6}$.
i.e. find the **remainder** r when 48 is divided by 7.

b) $-16 = -3.7 + 5 \therefore \quad -16 \equiv 5 \pmod 7$, so $\overline{-16} = \overline{5}$.

Here we use the division algorithm...

a) 48 = 6(7)+6, so 48 and 6 are in the same residue class.

b) the remainder when -16 is divided by 7 is 5

Note: The remainder $0 \leq r < 7$ in this example.
The remainder gives the name of the equivalence class the integer is in...

Example (4.2.3 (2))

If a is an odd integer, show that $\overline{a} = \overline{1}$ or $\overline{a} = \overline{3}$ in $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

If a is odd, $\Rightarrow \quad a = 2k + 1, \quad k \in \mathbb{Z}$. There are two cases

(i) k even, $k = 2m, \quad m \in \mathbb{Z}$.
$a = 2k + 1 = 2(2m) + 1 = 4m + 1$ and $a \equiv 1 \pmod 4$
$\therefore \quad \overline{a} = \overline{1}$.

(ii) k odd, $k = 2m + 1, \quad m \in \mathbb{Z}$.
$a = 2k + 1 = 2(2m + 1) + 1 = 4m + 3$ and $a \equiv 3 \pmod 4$
$\therefore \quad \overline{a} = \overline{3}$.

Example (4.2.3 (3))

In $\mathbb{Z}_4$, show that $\overline{a} = \overline{0}$ iff $4|a$.

(justification for the implication $\Rightarrow$)

$$\Rightarrow \quad \overline{a} = \overline{0} \Rightarrow a \equiv 0 \pmod 4$$ (equivalence classes are equal)

$$\Rightarrow a = 4k \Rightarrow 4|a$$ (by definition of congruence mod 4) (definition of divisor)

$$\Leftarrow \quad 4|a \Rightarrow a = 4k \Rightarrow a - 0 = 4k \Rightarrow \overline{a} = \overline{0}.$$

Theorem

Congruence modulo n is compatible with addition and multiplication of integers. Let $a, a_1, b, b_1 \in \mathbb{Z}$. *If* $a \equiv a_1 \pmod{n}$ *and* $b \equiv b_1 \pmod{n}$, *then*

- (i) $a + b \equiv a_1 + b_1 \pmod{n}$.
- (ii) $ab \equiv a_1 b_1 \pmod{n}$.

We have created a set $\mathbb{Z}_n$ with a new type of element...

The elements are equivalence classes... $\overline{0}$, $\overline{1}$, ... $\overline{n\text{-}1}$.

The question we ask here is:

Can we add these elements?

Can we multiply these elements

How do we define addition and multiplication of equivalence classes? (in this theorem addition and multiplication in $\mathbb{Z}_n$ is linked to addition and multiplication in $\mathbb{Z}$)

Proof: Let (1) be $a - a_1 = pn$ and (2) be $b - b_1 = qn$ where $p, q \in \mathbb{Z}$. adding (1) and (2), we get

$$(a+b)-(a_1+b_1) = (p+q)n \Rightarrow \quad (a+b) \equiv (a_1+b_1) \pmod{n}$$

Similarly, multiplying $a = a_1 + pn$ and $b = b_1 + qn$, we get $ab \equiv a_1 b_1 \pmod{n}$.

These manipulations permit the arithmetic properties of the set of integers to be extended naturally to $\mathbb{Z}_n$.