# 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:

- state and prove the properties of addition and multiplication of residue classes
- add and multiply residue classes
- use the properties of residue classes
-

## Definition

*We define addition and multiplication of residue classes* $\overline{a}$ *and* $\overline{b}$ *in* $\mathbb{Z}_n$ *by* $\overline{a}+\overline{b}=\overline{a+b}$ *and* $\overline{a}\,\overline{b}=\overline{ab}$.

## Theorem (4.2.4 (i))

*Let* $n \geq 2$ *be a fixed modulus and let* $a, b, c \in \mathbb{Z}$. *Then in* $\mathbb{Z}_n$, $\overline{a}+\overline{b}=\overline{b}+\overline{a}$ *and* $\overline{a}\,\overline{b}=\overline{b}\,\overline{a}$.

**Proof:** (by definition above) (true in the integers) (by definition above) (justification for each equal sign)

$\overline{a}+\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}$ commutative rule in $\mathbb{Z}$

$\overline{a}\,\overline{b}=\overline{ab}=\overline{ba}=\overline{b}\,\overline{a}$.

product of equivalence classes = equivalence class of product = equivalence class of product with order reversed = product of equivalence classes with order reversed

## Theorem (4.2.4 (ii))

*Let $n \geq 2$ be a fixed modulus and let $a, b, c \in \mathbb{Z}$. Then in $\mathbb{Z}_n$, $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ and $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$.*

**Proof:**

$$\begin{aligned}
\overline{a} + (\overline{b} + \overline{c}) &\overset{\#}{=} \overline{a} + (\overline{b + c}) \overset{\#}{=} \overline{a + (b + c)} \\
&\overset{*}{=} \overline{(a + b) + c} \quad \text{associative rule in } \mathbb{Z} \\
&\overset{\#}{=} \overline{a + b} + \overline{c} \\
&\overset{\#}{=} (\overline{a} + \overline{b}) + \overline{c}
\end{aligned}$$

For each proof we use the definition of addition/multiplication of equivalence classes (#)
and properties of addition/multiplication of integers (*)

$$\begin{aligned}
\overline{a}(\overline{b}\overline{c}) &= \overline{a}(\overline{bc}) = \overline{a(bc)} \\
&= \overline{(ab)c} \quad \text{associative rule in } \mathbb{Z} \\
&= \overline{ab}\,\overline{c} \\
&= (\overline{a}\overline{b})\overline{c}
\end{aligned}$$

## Theorem (4.2.4 (iii)) (additive and multiplicative identities exist)

*Let $n \geq 2$ be a fixed modulus and let $a, b, c \in \mathbb{Z}$. Then in $\mathbb{Z}_n$, $\overline{a} + \overline{0} = \overline{a}$ and $\overline{a}\overline{1} = \overline{a}$. (i.e $\exists$ additive and multiplicative identity.)*

**Proof:**

$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a} = \overline{0 + a} = \overline{0} + \overline{a}$. zero in $\mathbb{Z}$.

$\overline{a}.\overline{1} = \overline{a.1} = \overline{a} = \overline{1.a} = \overline{1}.\overline{a}$. unity in $\mathbb{Z}$.

## Theorem (4.2.4 (iv)) (additive inverse exists)

*Let $n \geq 2$ be a fixed modulus and let $a, b, c \in \mathbb{Z}$. Then in $\mathbb{Z}_n$,*

$$\overline{a} + \overline{-a} = \overline{0}.$$

**Proof:**

$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0} = \overline{(-a) + a}$. additive inverse in $\mathbb{Z}$.

## Theorem (4.2.4 (v)) (multiplication distributes over addition)

*Let $n \geq 2$ be a fixed modulus and let $a, b, c \in \mathbb{Z}$. Then in $\mathbb{Z}_n$,*

$$\overline{a}(\overline{b}+\overline{c}) = \overline{a}\overline{b} + \overline{a}\overline{c}.$$

**Proof:**

$$\begin{aligned}
\overline{a}(\overline{b}+\overline{c}) &= \overline{a}(\overline{b+c}) \\
&= \overline{a(b+c)} \\
&= \overline{ab+ac)} \\
&= \overline{ab} + \overline{ac} \\
&= \overline{a}\overline{b} + \overline{a}\overline{c}.
\end{aligned}$$


Did you notice that nothing was said about multiplicative inverses? :) this will be discussed later.......

Example 4. In $\mathbb{Z}_6$ compute $\overline{3}+\overline{5}$ and $\overline{3}.\overline{5}$.
$\overline{3}+\overline{5}=\overline{8}=\overline{2}$ because $8 \equiv 2 \pmod 6$.
$\overline{3}.\overline{5}=\overline{15}=\overline{3}$ because $15 \equiv 3 \pmod 6$.
$\overline{3}=\{\cdots, -9, -3, 3, 9, \cdots\}$ and $\overline{5}=\{\cdots, -7, -1, 5, 11, \cdots\}$.
Then check
$\overline{3}+\overline{-7}=\overline{-4}=\overline{2}$ because $-4 \equiv 2 \pmod 6$. or $\overline{3}+\overline{-7}=\overline{3}+\overline{5}=\overline{2}$ in $\mathbb{Z}_6$
$\overline{3}(\overline{-7})=\overline{-21}=\overline{3}$ because $-21 \equiv 3 \pmod 6$. or $\overline{3}(\overline{-7})=\overline{3}(\overline{5})=\overline{3}$ in $\mathbb{Z}_6$

You can add any element in {..., -9 , -3, 3 , $\boxed{9}$ ,...} $=\overline{3}$
to any element in {..., $\boxed{-7}$ , -1 , 5 , 11 ,...} $=\overline{5}$
and you will get some number in {..., -10 , -4 , $\boxed{2}$ , 8 ...} $=\overline{2}$

the idea behind adding residue classes

## Example (4.2.5 (1))

*What is the remainder when $4^{119}$ is divided by 9?*

We know $4^{119} \equiv r \pmod 9$ for some $0 \leq r < 9$.

We note that

$\overline{4^2} = \overline{16}$ so $\overline{4^2} = \overline{7}$ in $\mathbb{Z}_9$.

$\overline{4^3} = \overline{7.4} = \overline{28} = \overline{1}$ in $\mathbb{Z}_9$.

Finding the r value that makes $\overline{4^r}$ equal to $\overline{1}$ in $\mathbb{Z}_9$

Now $119 = 3.39 + 2$.

Division algorithm: n = 119, d = 3

Your calculator cannot work out $4^{119}$, it just can't.

It also cannot find the remainder when this huge number, $4^{119}$, is divided by 9...

But we can, using modular arithmetic!

So

$$\left.\begin{aligned} 4^{119} &= 4^{3.39+2} \\ &= 4^{3.39}.4^2 \\ &= (4^3)^{39}.4^2 \end{aligned}\right\} \text{just exponential laws}$$

Equate the equivalence classes of LHS and RHS

$$\left.\begin{aligned} \overline{4^{119}} &= \overline{(4^3)^{39}}.\overline{4^2} \\ &= \overline{(4^3)}^{39}.\overline{4^2} \\ &= \overline{1}^{39}.\overline{7} = \overline{7}. \end{aligned}\right\} \begin{array}{l}\text{Now use the} \\ \text{properties of} \\ \text{addition and} \\ \text{multiplication of} \\ \text{equivalence classes}\end{array}$$

So remainder $r$ where $4^{119}$ is divided by 9 is 7.

Part 3

E.M.B

739422 is divisible by 9 because 7+3+9+4+2+2=27 is divisible by 9. 24079 is not divisible by 9 because 2+4+7+9=22 is not divisible by 9.

## Example (4.2.5 (2))

*Casting out Nines. Show that a positive integer is divisible by 9 if and only if the sum of the digits is divisible by 9.*

Let $x$ be in $\mathbb{Z}^+$ We may write say $10^k \leq x < 10^{k+1}$
Then
$x = a_k 10^k + a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + \cdots + a_2 10^2 + a_1 10^1 + a_0$
where $0 \leq a_i \leq 9$ and $\forall i = 0, 1, 2, \cdots, k$.
i.e. $\{a_0, a_1, \cdots, a_k\}$ are $x's$ digits in the decimal representation.

It's like writing 284738 as $2(10^5)+8(10^4)+4(10^3)+7(10^2)+3(10)+8(10^0)$

Taking the equivalence class of * on previous page and using properties

Now

$$
\begin{aligned}
10 &\equiv 1 \pmod 9\\
10^2 &\equiv 1 \pmod 9\\
&\vdots\\
10^k &\equiv 1 \pmod 9
\end{aligned}
$$

All powers of 10 are congruent to 1 mod 9

$$
\begin{aligned}
\overline{x} &= \overline{a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0}\\
&= \overline{a_k 10^k} + \overline{a_{k-1}10^{k-1}} + \cdots + \overline{a_2 10^2} + \overline{a_1 10^1} + \overline{a_0}\\
&= \overline{a_k} + \overline{a_{k-1}} + \cdots + \overline{a_2} + \overline{a_1} + \overline{a_0}\\
&= \overline{a_k + a_{k-1} + a_{k-2} + \cdots + a_2 + a_1 + a_0}.
\end{aligned}
$$

$$
\begin{aligned}
\therefore \quad x &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0 \quad *\\
&\equiv a_k + a_{k-1} + a_{k-2} + \cdots + a_2 + a_1 + a_0 \pmod 9
\end{aligned}
$$