12 Residue Classes

In *modular arithmetic*, a *residue class* is a set of integers that are congruent to each other modulo a given number. When working with congruences, these residue classes help us group numbers that share certain properties under a modulo operation.

Defintion Residue Class of a modulo m

Definition 12.1. Let $m > 0$ be given. For each integer a, we define

$$[a]_m = \bar{a} = \{x : x \equiv a \pmod{m}\}.$$

In other words, $[a]_m$ or $\bar{a}$ is the set of all integers that are congruent to a modulo m. We call $[a]_m$ the residue class of a modulo m. Some people also call $[a]_m$ the congruence class or equivalence class of a modulo m.

Example 12.1. Consider $m = 5$ and look at the residue class of $2 \mod 5$. We are looking for all integers that leave the same remainder as 2 when divided by 5. These integers are:

$$\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

Thus, the residue class of 2 modulo 5 is:

$$\bar{2} = [2]_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

Similarly, the residue class of $3 \mod 5$ would be:

$$\bar{3} = [3]_5 = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$$

Theorem 12.1. *For $m > 0$, we have*

$$\bar{a} = [a]_m = \{mq + a \mid q \in \mathbb{Z}\}.$$

Proof.

$$x \in [a]_m \iff x \equiv a \pmod{m} \iff m \mid (x - a) \iff x - a = mq \text{ for some } q \in \mathbb{Z}$$

$$\iff x = mq + a \text{ for some } q \in \mathbb{Z}.$$

□

Theorem 12.2. *For a given modulus $m > 0$, we have:*

$$[a]_m = [b]_m \iff a \equiv b \pmod{m}.$$

Proof. *"⇒"* Assume $[a] = [b]$. Since $a \equiv a \pmod{m}$, we have $a \in [a]$. Since $[a] = [b]$, we have $a \in [b]$. By the definition of $[b]$, this gives $a \equiv b \pmod{m}$.

"⇐" Assume $a \equiv b \pmod{m}$. We must prove that the sets $[a]$ and $[b]$.

Let $x \in [a]$. Then $x \equiv a \pmod{m}$. Since $a \equiv b \pmod{m}$, by transitivity, $x \equiv b \pmod{m}$, so $x \in [b]$.

Conversely, if $x \in [b]$, then $x \equiv b \pmod{m}$. By symmetry, since $a \equiv b \pmod{m}$, we also have $b \equiv a \pmod{m}$. Thus, by transitivity, $x \equiv a \pmod{m}$, and so $x \in [a]$.

This proves that $[a] = [b]$. □

Distinct Residue Classes modulo m

Theorem 12.3. *Given $m > 0$, there are exactly m distinct residue classes modulo m, namely,*

$$[0], [1], [2], \ldots, [m-1].$$

12.1 $\mathbb{Z}_m$ and Complete Residue Systems

Defintion Set of All Residue Classes

Definition 12.2. We define

$$\mathbb{Z}_m = \{[a] \mid a \in \mathbb{Z}\},$$

that is, $\mathbb{Z}_m$ is the set of all residue classes modulo m. We call $(\mathbb{Z}_m, +, \cdot)$ the **ring of integers modulo** m.

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}.$$

or

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}.$$

Example 12.2.

- For $m = 2$:

$$\mathbb{Z}_2 = \{[0], [1]\}$$

- For $m = 3$:

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

- For $m = 4$:

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$$

- For $m = 5$:

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

Definition 12.3. A set of m integers

$$\{a_0, a_1, \ldots, a_{m-1}\}$$

is called a **complete residue system modulo** m if

$$\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}.$$

12.2 Addition and Multiplication in $\mathbb{Z}_m$

Definition 12.4. For $[a], [b] \in \mathbb{Z}_m$, we define

$$[a] + [b] = [a + b]$$

and

$$[a] \cdot [b] = [ab].$$

Remark 12.1. For $m = 5$, we have

$$[2] + [3] = [5], \quad \text{and} \quad [2] \cdot [3] = [6].$$

Since $5 \equiv 0 \pmod 5$ and $6 \equiv 1 \pmod 5$, we obtain

$$[5] = [0] \quad \text{and} \quad [6] = [1],$$

so we can also write

$$[2] + [3] = [0], \quad [2] \cdot [3] = [1].$$

Theorem 12.4. *For any modulus $m > 0$, if $[a] = [b]$ and $[c] = [d]$, then*

$$[a] + [c] = [b] + [d]$$

and

$$[a] \cdot [c] = [b] \cdot [d].$$

Example 12.3. Take $m = 151$. Then $150 \equiv -1 \pmod{151}$ and $149 \equiv -2 \pmod{151}$, so

$$[150][149] = [-1][-2] = [2]$$

and

$$[150] + [149] = [-1] + [-2] = [-3] = [148]$$

since $148 \equiv -3 \pmod{151}$.

Example 12.4. Addition and Multiplication Tables for $\mathbb{Z}_4$

Addition Table

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Multiplication Table

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Theorem 12.5. *$\mathbb{Z}_n$ is a ring for any positive integer n.*

Proof. Let n be a positive integer. Define $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$.

Step 1: Proving $\mathbb{Z}_n$ is a Commutative Group under Addition

1. **Closure under addition:** $\forall [a], [b] \in \mathbb{Z}_n$, we have

$$[a] + [b] = [a+b] \quad (\text{mod } n).$$

Since $a+b$ is an integer, $[a+b] \in \mathbb{Z}_n$, Therefore, $\mathbb{Z}_n$ is closed.

2. **Associativity of addition:** For $[a], [b], [c] \in \mathbb{Z}_n$, we have

$$([a]+[b])+[c] = [a+b]+[c] = [a+b+c] = [a]+[b+c] = [a]+([b]+[c]).$$

Therefore, addition is associative.

3. **Commutativity of addition:** For $[a], [b] \in \mathbb{Z}_n$, we have

$$[a]+[b] = [a+b] = [b+a] = [b]+[a].$$

Thus, addition is commutative.

4. **Identity:** The element $[0] \in \mathbb{Z}_n$ is identity because for any $[a] \in \mathbb{Z}_n$, we have

$$[a]+[0] = [a+0] = [a].$$

5. **Inverse:** For each $[a] \in \mathbb{Z}_n$, there exists an element $[b] \in \mathbb{Z}_n$ such that

$$[a]+[b] = [0].$$

The additive inverse of $[a]$ is $[n-a]$, since

$$[a]+[n-a] = [a+(n-a)] = [n] = [0].$$

Therefore, every element has an additive inverse.

Thus, $\mathbb{Z}_n$ is a commutative group under addition.

Step 2: Proving $\mathbb{Z}_n$ is a Semigroup under Multiplication

1. **Closure under multiplication:** For any $[a], [b] \in \mathbb{Z}_n$, we have

$$[a] \cdot [b] = [a \cdot b] \pmod{n}.$$

   Since $a \cdot b$ is an integer, $[a \cdot b] \in \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ is closed.

2. **Associativity of multiplication:** For $[a], [b], [c] \in \mathbb{Z}_n$, we have

$$([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [a \cdot b \cdot c] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c]).$$

   Therefore, multiplication is associative.

Thus, $\mathbb{Z}_n$ is a semigroup under multiplication.

Step 3: Proving Distributivity of Multiplication over Addition

Finally, we show that multiplication distributes over addition in $\mathbb{Z}_n$. For $[a], [b], [c] \in \mathbb{Z}_n$, we need to prove that

$$[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c].$$

We have

$$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b + c)] = [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c].$$

Thus, multiplication distributes over addition.

Since $\mathbb{Z}_n$ satisfies the properties of a commutative group under addition, a semigroup under multiplication, and distributivity of multiplication over addition, we conclude that $\mathbb{Z}_n$ is a ring.

□