12.) Integers modulo n under addition

Let n be a fixed positive integer and $x, y \in \mathbb{Z}$ be any two elements. Define $x \equiv y$ if and only if n divides $x-y$ i.e. $x \equiv y \pmod{n}$. Then it can be easily checked that $\equiv$ is an equivalence relation on $\mathbb{Z}$. The set of equivalence classes denoted by $\mathbb{Z}/\equiv$ or $\mathbb{Z}_n$ or $\mathbb{Z}/(n)$ given by

$$\{\bar{0}, \bar{1}, \ldots \overline{n-1}\}, \quad \text{where for any } 0 \leq x < n,$$

$\bar{x}$ denote the equivalence class containing x.

For example,

$$\cancel{\bar{0} = \{ \cdots -4, -2, 0, 2, 4, 6,}$$

$$\bar{0} = \{ \ldots, -2n, -n, 0, n, 2n, \quad \}$$

$$\bar{1} = \{ \ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots \}$$

and so on.

The equivalence classes [i.e. the elements of $\mathbb{Z}_n$] are called the residue classes of integers mod n.

We can see in this example that integers a, b belong to the same equivalence class if and only if they differ by a multiple of n, and any two equivalence classes are either the same or disjoint. (i.e. $\bar{x} = \bar{y}$ iff $n \mid x-y$)

We define addition in $\mathbb{Z}_n$ as follows:

$$\bar{x} + \bar{y} = \overline{x+y}.$$

Now, the addition is well defined:

let $\bar{x} = \overline{x'}$ and $\bar{y} = \overline{y'}$

then $n \mid x-x'$ and $n \mid y-y'$

$$\Rightarrow n \mid (x-x') + (y-y')$$

$$\Rightarrow n \mid (x+y) - (x'+y')$$

$$\Rightarrow \overline{x+y} = \overline{x'+y'}$$

Hence addition is well-defined and $\overline{x+y} \in \mathbb{Z}_n$.

$\Rightarrow \mathbb{Z}_n$ is closed under addition.

Further, for any $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$,

$$(\bar{x}+\bar{y})+\bar{z} = \overline{(x+y)}+\bar{z} = \overline{(x+y)+z}$$

$$= \overline{x+(y+z)}, \quad \text{since associativity holds in } \mathbb{Z}.$$

$$= \bar{x} + \overline{(y+z)}$$

$$= \bar{x} + (\bar{y}+\bar{z})$$

$\Rightarrow$ Associative law holds in $\mathbb{Z}_n$.

Now, for any element $\bar{x} \in \mathbb{Z}_n$, since $\bar{0} \in \mathbb{Z}_n$

$$\therefore \quad \bar{x}+\bar{0} = \overline{x+0} = \bar{x} = \overline{0+x}$$

$$= \bar{0}+\bar{x}$$

$\Rightarrow$ $\bar{0}$ is identity element of $\mathbb{Z}_n$.

and for any integer $x \in \mathbb{Z}$, $\bar{x} \in \mathbb{Z}_n$ implies $-x \in \mathbb{Z}$ and so there exist some equivalence class containing $-x$ i.e. $\overline{(-x)} \in \mathbb{Z}_n$ such that

$$\bar{x} + \overline{(-x)} = \overline{x+(-x)}$$

$$= \bar{0}$$

$$= \overline{(-x)+x}$$

$$= \overline{(-x)} + \bar{x}$$

So, $\overline{(-x)}$ is the inverse of $\bar{x}$ for every element $\bar{x} \in \mathbb{Z}_n$.

Let us denote $\overline{(-x)}$ by $-\bar{x}$.

Also, for any element $\bar{x}, \bar{y} \in \mathbb{Z}_n$,

$$\bar{x}+\bar{y} = \overline{x+y} = \overline{y+x}$$

$$= \bar{y}+\bar{x}$$

$\Rightarrow$ $\mathbb{Z}_n$ is abelian under addition.

Hence all the properties of a group are satisfied and so $\mathbb{Z}_n$ is group.

13) Integers modulo n under multiplication.

Consider the set $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}$ as in Example 12. Let multiplication in $\mathbb{Z}_n$ be defined as:

$$\bar{x} \cdot \bar{y} = \overline{xy}.$$

Now, multiplication is well defined:

let $\bar{x} = \bar{x'}$

and $\bar{y} = \bar{y'}$

$\Rightarrow \quad n \mid (x - x')$ and $n \mid (y - y')$

$\Rightarrow \quad n \mid (x - x')(y - y')$

$\Rightarrow \quad n \mid (xy + x'y') - (xy' + x'y)$

$\Rightarrow \quad n \mid (xy + x'y') - (xy' + x'y) + (x'y' - x'y')$

$\Rightarrow \quad n \mid \{(xy - x'y') + x'(y' - y) + y'(x' - x)\}$

$\Rightarrow \quad n \mid xy - x'y'$

$\Rightarrow \quad \overline{xy} = \overline{x'y'}$

$\therefore$ multiplication is well-defined and $\bar{x} \cdot \bar{y} = \overline{xy} \in \mathbb{Z}_n$.

Further, for any $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$,

$$\begin{aligned}
(\bar{x} \cdot \bar{y}) \cdot \bar{z} &= (\overline{xy}) \cdot \bar{z} \\
&= \overline{(xy)z} \\
&= \overline{x(yz)} \quad , \text{ since associativity holds in } \mathbb{Z} \text{ under } \cdot. \\
&= \bar{x}\ \overline{yz} \\
&= \bar{x} \cdot (\bar{y} \cdot \bar{z})
\end{aligned}$$

$\Rightarrow$ associativity holds in $\mathbb{Z}_n$ under multiplication.

Now, for any element $\bar{x} \in \mathbb{Z}_n$, since $\bar{1} \in \mathbb{Z}_n$

$$\begin{aligned}
\therefore \quad \bar{x} \cdot \bar{1} &= \overline{x \cdot 1} = \bar{x} \\
&= \overline{1 \cdot x} \\
&= \bar{x}.
\end{aligned}$$

$\Rightarrow \bar{1}$ is identity element of $\mathbb{Z}_n$.

Hence $\mathbb{Z}_n$ is a monoid under multiplication.