10.7 MODULO SYSTEM

It is of common experience that railway time-table is fixed with the provision of 24 hours in a day and night. When we say that a particular train is arriving at 15 hours, it implies that the train will arrive at 3 p.m. according to our watch. Thus all the timing starting from 12 to 23 hours correspond to one of 0, 1, 2 ... 11 O'clock as indicated in watches. In other words all integers from 12 to 23 are equivalent to one or the other of integers 0, 1, 2 , 3, ... 11 with modulo 12. In saying like this the integers in question are divided into 12 classes.

In the manner described above the integer could be divided into 2 classes, or 5 classes or m (m being a positive integer) classes and then we would have written mod 2 or mod 5 or mod m. This system of representing integers is called **modulo system.**

Addition modulo m

We shall now define a new type of addition known as "addition modulo m" and written as $a +_m b$ where a and b are any integers and m is a fixed positive integer.

By definition, we have

$$a +_m b = r, 0 \le r < m$$

where r is the least non-negative remainder when $a + b$, *i.e.*, the ordinary sum of a and b, is divided by m.

For example, $5 +_6 3 = 2$, since $5 + 3 = 8 = 1\,(6) = 2$, *i.e.*, 2 is the least non-negative remainder when $5 + 3$ is divided by 6. Similarly, $5 +_7 2 = 0, 4 +_3 2 = 0;\ 3 +_3 1 = 1, 15 +_5 7 = 2$.

Thus to find $a +_m b$, we add a and b in the ordinary way and then from the sum, we remove integral multiples of m in such a way that the remainder r is either 0 or a positive integer less than m.

When a and b are two integers such that $a - b$ is divisible by a fixed positive integer m, then we write

$$a = b \pmod{m}$$

which is read as "a is congurent to b modulo m."

by dr. P.N. Singh

Scanned with CamScanner

Thus $a = b \pmod m$ if $a - b$ is divisible by m. For example $13 = 3 \pmod 5$ since $13 - 3 = 10$ is divisibly by 5, $5 = 5 \pmod 5$, $16 = 4 \pmod 6$; $-20 = 4 \pmod 6$.

Multiplication modulo p

We shall now define a new type of multiplication known as "multiplication modulo p" and written as $a \times_p b$ where a and b are any integers and p is a fixed positive integer.

By definition we have

$$a \times_p b = r, 0 \le r \le p,$$

where r is the least non-negative remainder when ab, *i.e.*, the ordinary product of a and b, is divided by p. For example $4 \times_7 2 = 1$, since $4 \times 2 = 8 = 1(7) + 1$.

It can be easily shown that if $a = b \pmod p$, then $a \times_p c = b \times_p c$

10.7.1 Additive Group of Integers Modulo m

The set $G = \{0, 1, 2, \ldots m-1\}$ of first m non-negative integers is a group. The composition being addition reduced mudulo m.

Closure Property. We have by definition of addition modulo m,

$$a +_m b = r$$

where r is the least non-negative remainder when the ordinary sum $a + b$ is divided by m. Obviously $0 \le r \le m - 1$. Therefore for all $a, b \in G$ we have $a +_m b \in G$ and thus G is closed with respect to the composition addition modulo m.

Associative Property. Let a, b, c be any arbitrary elements in G.. Then

$$(a + b) +_m c = (a +_m b) +_m c \qquad [\because\ b +_m c = b + c \pmod m]$$

= least non-negative remainder when $a + (b + c)$ is divided by m

= least non-negative remainder when $(a + b) + c$ is divided by m, since

$$a + (b + c) = (a + b) + c$$
$$= (a + b) +_m c \qquad [\text{by definition of } +_m]$$
$$= (a +_m b) +_m c \qquad [\because\ a + b = a +_m b \pmod m]$$

$\therefore$ '$+_m$' is an associative composition.

Existence of Identity Element : We have $0 \in G$. Also, if a is any element of G, then $0 +_m a = a = a +_m 0$. Therefore 0 is the identity element.

Existence of Inverse. The inverse of 0 is 0 itself. If $r \in G$ and $r \ne 0$, then $m - r \in G$. Also $(m - r) +_m r = 0 = r +_m (m - r)$. Therefore $(m - r)$ is the inverse of r.

Commutative Property. The composition '$+_m$' is commutative also. Since

$a +_m b =$ least-non-negative remainder when $a + b$ is divided by m

= least non-negative remainder when $b + a$ is divided by m

$= b +_m a$.

The set G contains m elements.

Hence $(G, +_m)$ is a finite abelian group of order m.

10.7.2 Multiplicative Group of Integers Modulo p where p is Prime

The set G of $(p-1)$ integers $1, 2, 3, \ldots p-1$, p being prime, is finite abelian group of order $p-1$ the composition being multiplication modulo p.

by dr. P.N. Singh

Scanned with CamScanner

Let $G = \{1, 2, 3, \ldots p-1\}$ where p is prime.

Closure Property. Let a and b be any elements of G. Then $1 \le a \le p-1, 1 \le b \le p-1$. Now by definition, $a \times_p b = r$ where r is the least non-negative remainder when the ordinary product ab is divided by p. Since p is prime, therefore ab is not exactly divisible by p. Therefore r can not be zero and we shall have $1 \le r \le p-1$. Thus $a \times_p b \in G \; \forall \; a, b \in G$. Hence the closure axiom is satsified.

Associative Law. Let a, b, c be any arbitrary elements of G.

Then $a \times (_p b \times_p c) = a \times_p (bc)$ $[\because \; b \times_p c = bc \pmod p]$

= least non-negative remainder when $a(bc)$ is divided by p

= least non-negative remainder when $ab(c)$ is divided by p

$= (ab) \times_p c$

$= (a \times_p b) \times_p c$ $[\because \; ab = a \times_p b \pmod p]$

$\therefore$ '$\times p$' is an associative composition.

Existence of left identity. We have $1 \in G$. Also if a is any element of G, then $1 \times_p a = a$. Therefore 1 is the left identity.

Existence of left inverse. Let s be any member of G.

Then $1 < s < p-1$.

Let us consider the following $(p-1)$ products :

$$1 \times_p s, 2 \times_p s, 3 \times_p s, \ldots (p-1) \times_p s.$$

All these are elements of G. Also no two of these can be equal as shown below :
Let i and j be two unequal integers such that

$$1 \le i \le p-1, 1 \le j \le p-1 \text{ and } i > j.$$

Then $i \times_p s = j \times_p s$

$\Rightarrow$ is and js leave the same least non-negative remainder when divided by p

$\Rightarrow$ $is - js$ is divisibly by p.

$\Rightarrow$ $(i-j)s$ is divisible by p.

Since $1 \le (i-j) < p-1; 1 \le s \le p-1$ and p is prime, therefore $(i-j)$ s cannot be divided by p.

$\therefore$ $i \times_p s \ne j \times_p s$.

Thus $1 \times_p s, 2 \times_p s, \ldots (p-1) \times_p s$ are $(p-1)$ distinct elements of the set G. Therefore one of these elements must be equal to 1.

Let then $s' \times_p s = 1$. Then s' is the left inverse of s.

Commutative Law. The composition 'X_p' is commutative, since

$a \times_p b =$ least no-negative remainder when ab is divisible by p

= least non-negative remainder when ba is divided by p

$= b \times_p a$

$\therefore$ $(G, \times_p)$ is a finite abelian group of order $p-1$.

Theorem 1. *The residue classes modulo form a finite group with respect to addition of residue classes.*

by dr. P.N. Singh

Scanned with CamScanner

Proof. Let G be the set of residue classes (mod m), then

$$G = \{\{0\}, \{1\}, \ldots \{r_1\}, \ldots \{r_2\}, \ldots \{m-1\}\}$$

or
$$G = \{0, 1, 2, \ldots r_1, \ldots r_2 \ldots m-1 \pmod m\}$$

Closure axiom. $\{r_1\} + \{r_2\} = \{r_1 + r_2\} = \{r\} \in G$,

where r is the least positive integer obtained as remainder when $r_1 + r_2$ is divided by m $(0 \le r < m)$.

Thus, the closure axiom is satisfied.

Associative axiom. The addition is associative.

Identity axiom. $\{0\} \in \{G\}$ and $\{0\} + \{r\} = \{r\}$. Hence the identity for addition is $\{0\}$.

Inverse axiom. Since $\{m-r\} + \{r\} = \{m\} \equiv \{0\}$, the additive inverse of the element $\{r\}$ is $\{m-r\}$.

Hence G is a finite group with respect to addition modulo m.

Theorem 2. *The set of non-zero residue classes modulo p, where p is a prime, forms a group with respect to multiplication of residue classes.*

Proof. Let $I = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ be the set of integers. Let $a \in I$, then $\{a\}$ is residue class modulo p of I, if $\{a\} \cong \{x : x \in I$ and $x - a$ is divisible by $p\}$.

If $p \nmid a$ then $\{a\} = \{0\}$ which is called the zero residue class. Let G be the set of non-zero residue classes mod p (p being prime) then

$$G = \{1, 2, 3, \ldots, (p-1)\}$$

Closure axiom. Let $r_1, r_2 \in G$ then

$$r_1 \cdot r_2 = r \pmod p$$

where r is the least non-negative integer such that $0 \le r \le p-1$ obtained after dividing r_1, r_2 by p.

Also, since p is prime r_1, r_2 is not divisible by p. Hence r cannot be zero.

Hence, $r_1 \cdot r_2 = r = G$.

Thus closure axiom is satisfied.

Associative axiom. Multiplication of residue classes is associative.

Existence of Identity. $1 \in G$ and $a \cdot 1 = 1 \cdot a = a \; \forall \; a \in G$.

Therefore 1 is the identity element in G with respect to multiplication.

Existence of Inverse. Let $s \in G$ then $1 \le s \le p-1$. Let us consider following $(p-1)$ elements.

$$1 \cdot s, 2 \cdot s, 3 \cdot s \ldots, (p-1) \cdot s.$$

All these elements are elements of G because the closure law is true. All these elements are distinct as otherwise if

$$i \cdot s = j \cdot s \text{ for } i \ne j \text{ and } i, j \in G$$

then $i \cdot s = j \cdot s \Rightarrow i \cdot s - j \cdot s$ is divisible by p

$\Rightarrow$ $(i-j) \cdot s$ is divisibly by p

$\Rightarrow$ $(i-j)$ is divisibly by p $\quad [\because \; 1 \le s < p-1]$

$\Rightarrow$ $i = j$ which is contrary to our assumption that $i \ne j$,

Therefore above $(p-1)$ elements are the same as the elements of G. Hence some one of them should be 1 also. Let $s' \cdot s = 1$ where $1 \le s' \le p-1$. Hence s' is inverse of s. Hence inverse axiom is also satisfied.

by dr. P.N. Singh

Scanned with CamScanner

$\therefore$ G is a grouip under multiplication mod p.

Note : Since $r \,.\, s = s \,.\, r \;\forall\; r, s \in G$.

G is finite abelian group of order $(p-1)$.

Dr. P.N. Singh

Scanned with CamScanner