PITHAPUR RAJAH'S GOVERNMENT COLLEGE (A), KAKINADA

DEPARTMENT OF MATHEMATICS

Laveti. Surya Bala Ratna Bhanu M.Sc ,B.Ed
Lecturer in Mathematics
Phone:7330946793 ,9704768781.
Email: bhanuasdgdc@gmail.com

Addition Modulo m: Let $a, b \in \boldsymbol{Z}$ and m be a fixed positive integer. If r is the reminder $(0 \leq r < m)$ when $a + b$ is divided by m, we define '$a +_m b$'$= r$ and we read $a +_m b$ as a 'addition modulo m'b.

Examples:

i. $20 +_6 5 = 1$ since 20+5=4(6)+1 i.e., 1 is the remainder when 20+5 divided by 6.

ii. $24 +_5 4 = 3$.

iii. $2 +_7 3 = 5$

iv. -32$+_4 5 = 1$ since -32+5=(-7)(4)=1.

Congruence: Let $a, b \in \boldsymbol{Z}$ and m be a fixed positive integer. If $a - b$ is divisible by m we say that a is congruent to b modulo m and we write it as $a \equiv b \ (mod\ m)$. This relation between the integers a and b is called congruence modulo m.

Thus: $a \equiv b \ (mod\ m) \Leftrightarrow m/a - b \ or\ m/b - a$

$$or$$

$$a - b = qm \ for\ q \in \boldsymbol{Z} \ and$$

$a \not\equiv b(mod\ m) \Leftrightarrow m$ does not divide $a - b$

or

$a - b \neq km$ for $k \in \boldsymbol{Z}$

Note: If $a \equiv b(mod\ m)$, then we get same remainder if $a$and b are separately divided by m. For example, if $22 \equiv 13(\text{mod } 3)$, then 1 is the remainder when 22 and 13 are separately divided by 3.

Definition: z_m={0,1,2,3,......$(m-1)$} is called the **complete set of least positive residues modulo $\boldsymbol{m}$** or simply **set of residues modulo $\boldsymbol{m}$**.

Problem: Prove that set $\boldsymbol{G} = \{0,1,2,3,4\}$ is an abelian group of order 5 w.r.to addition modulo 5.

Solution: Given $\boldsymbol{G} = \{0,1,2,3,4\}$

The composition table for $\boldsymbol{G}$ w.r.to $+_5$ is as follows:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

i) Since all entries in the composition table are elements in $\boldsymbol{G}$. Hence closure law holds in $\boldsymbol{G}$.

ii) Clearly $\boldsymbol{G}$ is associative w.r.to $+_5$.

iii) 0 is the identity element in $\boldsymbol{G}$

iv) Inverse of 0 is 0

Inverse of 1 is 4

Inverse of 2 is 3

Inverse of 3 is 2

Inverse of 4 is 1

v) Cleary $\boldsymbol{G}$ is commutative w.r.to $+_5$.

Hence $(\boldsymbol{G}, +_5)$ is an abelian group.

Multiplication Modulo m: If a and b are integers and p is a fixed positive integer and ab is divided by p such that r is the remainder $(0 \leq r < p)$.we define

$a \times_p b = r$.we read $a \times_p b$ as a "multiplication modulo p" b.

Examples:

i. $20 \times_6 5 = 4$(since 20× 5=100=16(6)+4

i.e., 4 is the remainder when 100 is divided by 6).

ii. $24 \times_5 4 = 1$.

ii. $2 \times_7 3$=6.

Problem: Prove that the set $\boldsymbol{G} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}\}$ is a finite abelian group of order 6 w.r.to. $\times_7$.

Solution: Given $\boldsymbol{G} = \{1,2,3,4,5,6\}$.

The composition table for $\boldsymbol{G}$ w.r.to $\times_7$ is as follows:

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

i) Since all entries in the composition table are elements in $\boldsymbol{G}$.

Hence closure law holds in $\boldsymbol{G}$

ii) Clearly $\boldsymbol{G}$ is associative w.r.to $\times_7$.

iii) 1 is the identity element in $\boldsymbol{G}$

iv) Inverse of 1 is 1

Inverse of 2 is 4

Inverse of 3 is 5

Inverse of 4 is 2

Inverse of 5 is 3

Inverse of 6 is 6

v) Cleary $\boldsymbol{G}$ is commutative w.r.to $\times_7$.

Hence $(\boldsymbol{G}, \times_7)$ is an abelian group.

Exercise Problems:

- **Find the order of each element of the group G ={0,1,2,3,4,5 } the composition being addition modulo 6**

Show that the set of integers { 1,3,5,7 }form an abelian group w.r.t X_8

Thank you