Abstract of Algebra: Group of residue classes

Definition:- Consider the set Z of integers so that

$$Z = \{0, \pm1, \pm2, \pm3, \pm4, --\}.$$

Let $a, b \in Z$ be arbitrary and n a fixed positive integer.

We define a relation $\equiv (\text{mod } n)$ on Z as follows:

$$a \equiv b \,(\text{mod } n)$$

iff $a-b$ is divisible by n i.e. iff $a-b = qn$ for some $q \in Z$.

$a \equiv b \,(\text{mod } n)$ is read as a is congruent to b modulo n.

For $-9 \equiv 5 \,(\text{mod } 7)$, $2 \equiv 11 \,(\text{mod } 3)$

$20 \equiv 2 \,(\text{mod})$ etc.

Theorem:- The set of residue classes modulo m is a group w.r.t. addition of residue classes.

Proof:- Let Z_m denote the set of all residue classes modulo m

so that $Z_m = \{[0], [1], [2], [3], -- [m-1]\}$.

Let $[a], [b] \in Z_m$ be arbitrary.

To prove that $(Z_m, +)$ is a group.

Closure Property..

$$[a], [b] \in Z_m \Rightarrow [a] + [b] \in Z_m.$$

For $[a] + [b] = [r]$, where r is the ~~least~~ least non-negative remainder when $a+b$ is divided by m.

This $\Rightarrow 0 \le r < m \Rightarrow [r] \in Z_m \Rightarrow [a] + [b] \in Z_m$.

Associativity: $([a]+[b])+[c] = [a]+([b]+[c])$

For L.H.S $=([a]+[b])+[c]$, where $a+b$ is reduced by m.

$= [(a+b)+c]$, where $(a+b)+c$ is reduced by m.

$= [a+(b+c)]$ $\because (a+b)+c = a+(b+c)$

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

$=$ R.H.S.

Existence of identity element: There exists identity element $[0] \in Z_m$.

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

Existence of Inverse: Every element $[a] \in Z_m$ has its inverse

$[m-a] \in Z_m$.

For $[a]+[m-a] = [0] = [m-a]+[a]$, where $a \neq 0$

Thus all the group postulates are Satisfied and hence $(Z_m, +)$ is a group.

Prove of

Problem – Do the sets of residue classes modulo 7 from a group w.r.t. addition?

Solution:– Let Z_7 denote the set of all residue classes modulo 7, so that $Z_7 = \{[0], [1], [2], [3], [4], \ldots [6]\}$.

To determine the nature of the system $(Z_7, +)$

Putting $m = 7$ we get the solution

$O(4) = 7$, Since Z_7 Contains 7 elements.

Finally we have prove that $(Z_7, +)$ is an abelian group of order 7.