B.Sc Part II (Hons)
Unit III
Some Theorems on Residue classes

Theorem :- The set of all non-zero residue classes modulo a prime number p is a group w.r.t multiplication of residue classes.

Proof :- Let G be a set of all non-zero residue classes modulo a prime integer p so that

$G = \{[1], [2], [3], \ldots [p-1]\}$

Also divisors of p are only ± 1 and $\pm p$

To prove that $(G, \cdot)$ is a group.

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

Closure Property. $[a].[b] = [r]$, where r is the least non-negative remainder when ab is divided by p.

$\Rightarrow 0 \leq r \leq p$

$[a]$ and $[b] \in G \Rightarrow 0 < a < p,\ 0 < b < p$

$\Rightarrow$ Neither a nor b is divisible by p

Also p is prime.

$\Rightarrow$ ab is not divisible by p

$\Rightarrow$ remainder $r \neq 0$ But $0 \leq r < p$.

$\Rightarrow 0 < r < p \Rightarrow [r] \in G \Leftrightarrow [a][b] \in G$.

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

For L.H.S $= [ab][c]$ Where $(ab)c$ is reduced by p

$= [(ab).c]$, Where $(ab)c$ is reduced by p

$= [a(bc)]$, For $(ab)c = a(bc)$

$= [a][bc] = [a]([b][c]) =$ R.H.S

Existence of identity: $\exists$ identity element $[1] \in G$.

For $[a].[1] = [a] = [1].[a]$.

Existence of inverse: Every element $[a] \in G$ has its inverse $[a'] \in G$, Where $[a][a'] = [aa'] = [a'a] = [1]$

This $\Rightarrow aa' \equiv 1 \pmod{p}$.

Thus every element $[a] \in G$ has its inverse $[a^{-1}] \in G$ Such that $aa^{-1} \equiv 1 \pmod{p}$

Since $ax \equiv 1 \pmod{p}$ has a Solution x if p is prime Hence $[a]$ exists

Thus all the group postulates are Satisfied and hence $(G, \cdot)$ is a group

Theorem :- Let G be the set of non-zero residue Classes modulo a Composite positive integer m. So that

$$G = \{[1], [2], [3], [4], \ldots [m-1]\}.$$

Proof: To prove that $(G, \cdot)$ is not a group, where $(\cdot)$ denotes multiplication of residue classes.

m is a Composite integer $\Rightarrow \exists\ a, b \in N$ st $ab = m$

$\Rightarrow 0 < a < m,\ 0 < b < m$

$\Rightarrow [a] \cdot [b] \in G$

$\Rightarrow [ab] = [m] = [0]$, Since $m \equiv 0 \pmod{m}$

$\Rightarrow [ab] = [0] \notin G$

$\Rightarrow [a][b] = [ab] \notin G \Rightarrow [a]\,[b] \notin G$

Thus $[a] \cdot [b] \in G \Rightarrow [a]\,[b] \notin G$

This proves that G is not closed w.r.t the operation $(\cdot)$.

Hence $(G, \cdot)$ is not a group.

Arjani Kumar Singh.