Lectured By Dr. A.K. Yadav
Deptt. of Mathematics Marwari College, Darbhanga.
B.Sc. part-I(H), paper-I Date-06-05-2020.

Algebra (Group)

Q.1. State and prove Fermat's Theorem

Soln. Statement: If a is any integer and p is prime, then $a^p \equiv a \pmod p$.

Proof: If $a=0$, then theorem is obviously true.

If $a \neq 0$. Let G be the multiplicative group of residue classes modulo p, then G contains $(p-1)$ distinct elements namely

$$[1], [2], \ldots, [p-1]$$

$$\Rightarrow o(G) = p-1 \text{ and } [e]=1$$

Then, by theorem we know that if G be a finite group of order n and $a \in G$ then $a^n = e$.

We have, $[a^{p-1}] = [1] \Rightarrow a^{p-1} \equiv 1 \pmod p$

Now, since p is prime. Hence

$$a^{p-1}.a \equiv 1.a \pmod p \Rightarrow a^p \equiv a \pmod p.$$

Q.2. State and prove Euler's Theorem

Soln. Statement:- If n is a positive integer and a is any integer relatively prime to n, then

$$a^{\phi(n)} \equiv 1 \pmod n.$$

Proof: Let us suppose that $[x]$ denote the residue class of the set of integer mod n, for any integer n.

Now, we have, the residue classes G is a group

22/05/20

Rest part of Q.2.

of order $\phi(n)$ with identity element, residue class $[1]$.

Now, we have,

$$[a] \in G \Rightarrow [a]^{o(G)} = [1] \Rightarrow [a]^{\phi(n)} = [1]$$
$$\Rightarrow [a][a] \ldots \text{up to } \phi(n) \text{ times} = [1]$$
$$\Rightarrow [a.a \ldots \text{up to } \phi(n) \text{ times}] = [1]$$
$$\Rightarrow [a^{\phi(n)}] = [1] \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

Proved.

Q.3. Let H and K be finite subgroup of a group G, then

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)}$$

Proof: Let G be a group and H and K are two subgroups of G. Then HK is a subset of G, not necessarily the subgroup of G.

Let $D = H \cap K$, then D is a subgroup of G and $D \subseteq K$. Therefore D is a subgroup of K also.

Since, K is finite, therefore, the number of distinct right cosets is finite. Let it be n. Then, by Lagrange's theorem, we have

$$n = \frac{o(K)}{o(D)}$$

Let $Dk_1, Dk_2, \ldots Dk_n$ are the distinct right cosets of D in K then we have

$$K = Dk_1 \cup Dk_2 \cup \ldots \cup Dk_n = \bigcup_{i=1}^{n} Dk_i$$

We should see that $k_1, k_2, \ldots k_n$ are some distinct element in K. Then, $HK = H\left(\bigcup_{i=1}^{n} Dk_i\right) = \bigcup_{i=1}^{n} HDk_i = \bigcup_{i=1}^{m} Hk_i$ $[\because D \subseteq H \Rightarrow HD = D]$

$$= Hk_1 \cup Hk_2 \cup \ldots \cup Hk_n.$$

Now, we shall show that the cosets $Hk_1, Hk_2, \ldots Hk_n$ are pairwise distinct. We have, $Hk_i = Hk_j \Rightarrow k_i k_j^{-1} \in H$

$$\Rightarrow k_i k_j^{-1} \in H \cap K$$
$$\Rightarrow k_i k_j^{-1} \in D \Rightarrow Dk_i = Dk_j$$
$$\Rightarrow k_i = k_j \quad [\because Dk_i, Dk_j \text{ are distinct cosets}]$$

The number of elements in $HK = n \times o(H)$

$$\Rightarrow o(HK) = n \times o(H) = \frac{o(K)}{o(D)} \cdot o(H) = \frac{o(K)\,o(H)}{o(H \cap K)}$$

Proved.