

Lectured by Dr. H.K. Yadav
Dept. of Mathematics, Naraina College, Gurgaon, Haryana
B.Sc. Part-II (H), Paper-I Date: 06-05-2020
Algebra (Group)

Q.1. State and prove Fermat's Theorem.

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

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

If $a \not\equiv 0$. Let G be the multiplicative group of residue classes modulo p , then G contains $(p-1)$ distinct elements namely

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

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

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

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

Now, since p is prime. Hence

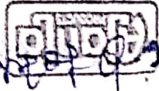
$$a^{p-1} \cdot a \equiv 1 \cdot a \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$$

Q.2. State and prove Euler's Theorem

Sol. 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

proof 

Rest part of Q.2.
of order $\phi(n)$ with identity element, residue class $[1]$.

Now, we have,

$$\begin{aligned} [a] \in U &\Rightarrow [a]^{\phi(n)} = [1] \Rightarrow [a]^{\phi(n)} = [1] \\ &\Rightarrow [a][a] \dots \text{up to } \phi(n) \text{ times} = [1] \\ &\Rightarrow [a \cdot a \dots \text{up to } \phi(n) \text{ times}] = [1] \\ &\Rightarrow [a^{\phi(n)}] = [1] \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n} \end{aligned}$$

proved.

Q.3. Let H and K be finite subgroups 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 $D = HK$, 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 $DK_1, DK_2, \dots, DK_n$ are the distinct right cosets of D in K then we have

$$K = DK_1 \cup DK_2 \cup \dots \cup DK_n = \bigcup_{i=1}^n DK_i$$

We should see that $K_1, K_2, \dots, K_n$ are some distinct element in K . Then,

$$\begin{aligned} HK &= H \left(\bigcup_{i=1}^n DK_i \right) = \bigcup_{i=1}^n HDK_i = \bigcup_{i=1}^n HK_i \quad [\because D \subseteq H \Rightarrow HD = D] \\ &= HK_1 \cup HK_2 \cup \dots \cup HK_n. \end{aligned}$$

Now, we shall show that the cosets $HK_1, HK_2, \dots, HK_n$ are pairwise distinct. We have,

$$\begin{aligned} HK_i &= HK_j \Rightarrow K_i K_j^{-1} \in H \\ &\Rightarrow K_i K_j^{-1} \in HK \\ &\Rightarrow K_i K_j^{-1} \in D \Rightarrow DK_i = DK_j \\ &\Rightarrow K_i = K_j \quad [\because DK_i, DK_j \text{ are distinct cosets}] \end{aligned}$$

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.