UNIT-III

Primitive Roots and Indices

Order of an integer modulo n

Motivation: Euler's theorem $\left[a^{\phi(n)} \equiv 1 \bmod n \text{ whenever } \gcd(a,n)=1 \right.$

but still there are exponents k smaller than $\phi(n)$ s.t $a^k \equiv 1 \bmod n$. so definition as;

Definition: Let $n>1$ and $\gcd(a,n)=1$. Order of $a \in \mathbb{Z} \bmod n$ is the smallest positive integer k such that $a^k \equiv 1 \bmod n$.

Example:- $a=2$, $n=7$, find order of $2 \bmod 7$.

Euler's: $2^{\phi(7)} \equiv 1 \bmod 7$

$\Rightarrow 2^6 \equiv 1 \bmod 7$

Solution:

$2^1 \equiv 2 \bmod 7$

$2^2 \equiv 4 \bmod 7$

$2^3 \equiv 8 \equiv 1 \bmod 7$ $\therefore$ order$(2 \bmod 7) = 3$.

Theorem: If two integers a and b are congruent modulo n then they have same order modulo n.

Proof: given $a \equiv b \bmod n$ and Let $o(a \bmod n) = k$

$\Rightarrow a^k \equiv 1 \bmod n$

we know $a^k \equiv b^k \bmod n$

$\Rightarrow 1 \equiv b^k \bmod n$

$\Rightarrow o(b \bmod n) = k$ proved

note If $\gcd(a,n) > 1$ then $a^k \equiv 1 \bmod n$ does not hold.

Logic:- suppose contrary $a^k \equiv 1 \bmod n$

$\Rightarrow a\, a^{k-1} \equiv 1 \bmod n$

$\Rightarrow ax \equiv 1 \bmod n$ has solⁿ $x = a^{k-1}$

$\Rightarrow\Leftarrow$ ($\because$ if $\gcd(a,n) \neq 1$, $ax \equiv 1 \bmod n$ does not have solⁿ)

Theorem:- Let the integer a have order k modulo n then $a^h \equiv 1 \bmod n$ iff k/h (In particular $k/\phi(n)$)

Proof:-

given $k/h \Rightarrow h = km$ $m \in \mathbb{Z}$

$\because$ $o(a \bmod n) = k \Rightarrow a^k \equiv 1 \bmod n$

$\Rightarrow (a^k)^m \equiv (1)^m \bmod n$

$\Rightarrow a^h \equiv 1 \bmod n$ proved

Conversely; Let h be any +ve integer satisfying $a^h \equiv 1 \bmod n$

by division algorithm, $h = qk + r$ $\quad 0 \le r < k$

$\Rightarrow a^{qk+r} \equiv 1 \bmod n \Rightarrow (a^k)^q . a^r \equiv 1 \bmod n$

$\Rightarrow a^r \equiv 1 \bmod n$ (but k is least +ve int s.t $a^k \equiv 1 \bmod n$)

$\Rightarrow\Leftarrow$

$\therefore \boxed{r = 0}$

$\therefore h = qk \quad q \in \mathbb{Z}$

$\Rightarrow k/h$.

Theorem:- If the integer a has order k modulo n then $a^i \equiv a^j \pmod n$ iff $i \equiv j \bmod k$

Proof: suppose $i \ge j$, $a^i \equiv a^j \bmod n$ $\because \gcd(a,n) = 1$

$\therefore a^{-1}$ exist $\Rightarrow a^i . a^{-j} \equiv a^j . a^{-j} \bmod n$

$\Rightarrow a^{i-j} \equiv 1 \bmod n$

$\Rightarrow k / i-j \Rightarrow i \equiv j \bmod k$

$a^k \equiv 1 \bmod n$

$a^i \equiv a^j \bmod n$

$\Leftrightarrow i \equiv j \bmod n$

Conversely; Let $i \equiv j \bmod k \Rightarrow i = j + qk$

$a^i = a^{j+qk} = a^j . (a^k)^q \bmod n$

$a^i \equiv a^j \bmod n$.