Primitive Root

1. Question : Show that 2 is a primitive root modulo 11

Ans: Given that,

A number g is a primitive root modulo 11,

Since 11 is prime, we need the order of 2 modulo 11 to be $\varphi(11) = 10$.

Compute powers of 2 mod 11 :

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^3 \equiv 8$

$2^4 \equiv 16 \equiv 5$

$2^5 \equiv 2^4 \cdot 2 = 5 \cdot 2 = 10$

$2^6 \equiv 10 \cdot 2 = 20 \equiv 9$

$2^7 \equiv 9 \cdot 2 = 18 \equiv 7$

$2^8 \equiv 7 \cdot 2 = 14 \equiv 3$

$2^9 \equiv 32 \equiv 6$

$2^{10} \equiv 6 \cdot 2 = 12 \equiv 1$

we reached 1 first exponent 10. So the order of 2 mod 11 is $\cancel{10} = \varphi = \varphi(11)$

Therefore 2 is a primitive root modulo 11.

2. How many incogruent primitive roots does 14 have?

Ans: Primitive roots exist for $n = 2, 4, p^k$ or $2p^k$ with odd prime p. Since $14 = 2 \cdot 7$, primitive roots exist.

Compute:

$$\phi(K) = \phi(2)\phi(7) = 1 \cdot 6 = 6$$

So number of primitive roots $= \phi(6) = 2$

(Ans)

3.

(a) Show that,

$$\text{Ord}_n(a) = \text{Ord}_n(a^{-1})$$

Let. $\text{Ord}_n(a) = k$

That means: $a^k \equiv 1 \pmod{n}$

Now, $(a^k)^{-1} \equiv 1^{-1} \pmod{n}$

Simplify: $(a^{-1})^k \equiv 1 \pmod{n}$

That means the order of a^{-1} divides k.

Hence the two orders divided each other.

So, they are equal.

$$\text{Ord}_n(a) = \text{Ord}_n(a^{-1})$$

(b) yes.

If is a primitive root mod n,

then $ord_n(a) = \phi(n)$

From part (a), $ord_n(a^{-1}) = ord_n(a) = \varphi(n)$

so, a^{-1} also has order $\phi(n)$

Therefore, a^{-1} is also a primitive root modulo n.

(Ans)