1) Show that, 2 is a primitive root modulo 11.

Ans:-

A number g is a primitive root modulo p (prime) if its multiplicative order modulo p is $\varphi(p) = p-1$. for $p=11$ we need the order of 2 mod 11 to be 10.

$$2^1 \equiv 2 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^4 \equiv 16 \equiv 5 \pmod{11}$$
$$2^5 \equiv 32 \equiv 10 \pmod{11}$$
$$2^6 \equiv 64 \equiv 9 \pmod{11}$$
$$2^7 \equiv 128 \equiv 7 \pmod{11}$$
$$2^8 \equiv 256 \equiv 3 \pmod{11}$$
$$2^9 \equiv 512 \equiv 6 \pmod{11}$$
$$2^{10} \equiv 1024 \equiv 1 \pmod{11}$$

The only exponent ≤ 10 giving 1 is 10 itself, so the order of 2 modulo 11 is $10 = \varphi(11)$

Therefore, 2 is a primitive root modulo 11.

Showed

2) How many incongruent primitive roots does 14 have?

Ans:-

A primitive root modulo n is a number g such that the powers of g modulo n generate all numbers that are coprime to n.

- Coprime numbers $= 1, 3, 5, 9, 11, 13$.
- Total coprime numbers $= 6 \rightarrow \phi(14) = 6$

primitive roots exist only for numbers n of the form:

1. $n = 2$ or $n = 4$
2. $n = p^k$ (where, p odd prime)
3. $n = 2p^k$ (where p odd prime)

Here, $14 = 2 \cdot 7 \rightarrow$ form $2p$ ($p = 7$ odd prime)

So, primitive roots exist modulo 14.

The number of primitive roots modulo n is: $\phi(\phi(n))$

- $\phi(14) = 6$
- $\phi(6) = 2$

So, there are 2 primitive roots modulo 14.

3

(a.) Let $ord_n(a) = k$,

Then $a^k \equiv 1 \pmod n$

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

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

Hence, The two orders divided each other

so, They are equal

$$Ord_n(a) = Ord_n(a^{-1}) = k$$

(b.) a is a primitive root modulo n if

$$Ord_n(a) = \phi(n)$$

where, $\phi(n)$ = number of integers 1 to n-1 coprime to n.

we know,

$$Ord_n(a^{-1}) = ord_n(a) = \phi(n)$$

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

Since, a^{-1} must also be a primitive root modulo n.