Sub: IT-24651

Day

Time: Date: / /

Ques 1| Show that 2 is a primitive root modulo 11.

Ans:-| A primitive root modulo 'n' is an integer 'g' that is coprime to 'n' such that the smallest positive integer 'd' satisfy $g^d \equiv 1 \pmod{n}$ where, 'd' is exactly equal to $\varphi(n)$. and φ is Euler's totient function.

Here, $n=11$, therefore, $\varphi(11)=10$ [11 is a prime]

Now, we need to show that the power of 2 mod 11 is 10.

$$2^1 \equiv 2 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^4 \equiv 5 \pmod{11}$$
$$2^5 \equiv 10 \pmod{11}$$
$$2^6 \equiv 9 \pmod{11}$$
$$2^7 \equiv 7 \pmod{11}$$
$$2^8 \equiv 3 \pmod{11}$$
$$2^9 \equiv 6 \pmod{11}$$
$$2^{10} \equiv 1 \pmod{11}$$

Then, $2^{10} \equiv 1 \pmod{11}$ proves that,

2 is a primitive root modulo 11.

Sub : IT-24651

Day

Time : Date : / /

Ques 2| How many incongruent primitive roots does 14 have?

Ans:| Primitive roots exist modulo 'n' if,

$n = 2, 4, p^k$ or $2p^k$ where, p is an odd prime and $k \geq 1$.

Here, $14 = 2^1 \times 7^1$, So, primitive root exists.

The number of incongruent primitive roots modulo 'n' is $\varphi(\varphi(n))$.

Therefore,

$$\varphi(14) = \varphi(2 \times 7) = \varphi(2) \times \varphi(7)$$
$$= 1 \times 6 = 6$$

and,
$$\varphi(6) = \varphi(2 \times 3) = \varphi(2) \times \varphi(3)$$
$$= 1 \times 2$$
$$= 2$$

So, there are 2 primitive roots modulo 14.

Sub : IT-24651

Day Time : Date : / /

Ques 3| Suppose 'n' is a positive integer and a^{-1} is a multiplicative inverse of 'a' (mod n)

a) Show that, $ord_n(a) = ord_n(a^{-1})$

Ans:| Let, $ord_n(a) = k$

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

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

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

Therefore, the order of (a^{-1}) is multiple of 'k' which is the order of (a)

So, $ord_n(a) =$ order (a^{-1}) over modulo 'n',

b) If 'a' is a primitive root modulo 'n', must a^{-1} be a primitive root?

Ans:| Yes.

To prove it,

If 'a' is a primitive root under modulo 'n',

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

From, part (a) we see,

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

~~So, $\phi(n)$ a^{-1} is also~~.

So, order of a^{-1} is equal to $\phi(n)$.

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