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

Soln:

We must show that 2 generates all nonzero residues modulo 11.

The residues modulo 11 are:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Let's compute successive powers of 2 (mod 11):

$2^1 \equiv 2 \pmod{11}$

$2^2 \equiv 4 \pmod{11}$

$2^3 \equiv 8$

$2^4 \equiv 16 \equiv 5 \pmod{11}$

$2^5 \equiv 10 \pmod{11}$

$2^6 \equiv 20 \equiv 9 \pmod{11}$

$2^7 \equiv 18 \equiv 7 \pmod{11}$

$2^8 \equiv 14 \equiv 3 \pmod{11}$

$2^9 \equiv 6 \pmod{11}$

$2^{10} \equiv 12 \equiv 1 \pmod{11}$

The smallest exponent giving 1 is 10, so 2 is a primitive root modulo 11.

2) How many incongruent primitive roots does 14 have?

Soln:

We know,

Number of primitive roots of $n = \varphi(\varphi(n))$ if and only if $n = 2, 4, p^k, 2p^k$ (where p is an odd prime).

Here, $14 = 2 \times 7$, which fits the form $2p$.

After computation,

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

$$\varphi(\varphi(14)) = \varphi(6) = 2$$

Therefore, there are 2 incongruent primitive roots modulo 14.

3) Suppose, n is a positive integer, and a^{-1} is the multiplicative inverse of $a \pmod{n}$.

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

Soln:

Let, $ord_n(a) = k$.

That means:

$$a^k \equiv 1 \pmod{n}$$

Multiply both sides by $(a^{-1})^k$:

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

So, the order of a^{-1} also divides k.

Similarly, by symmetry, $a^k \equiv 1$ implies the reverse,

So, $ord_n(a) = ord_n(a^{-1})$. (proved)

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

Soln:

If a is a primitive root mod n, then:

$$\text{ord}_n(a) = \varphi(n)$$

from part (a):

$$\text{ord}_n(a^{-1}) = \text{ord}_n(a) = \varphi(n)$$

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