1. Show that 2 is a primitive root of modulo 11.

Ans: An integer g is a primitive root modulo 11

$$\mathrm{Ord}_n(g) = \phi(n)$$

where ϕ is the Euler's totient function.

Step-1: compute $\phi(11)$

Since 11 is prime

So, we must show, $\mathrm{Ord}_{11}(2) = 10$

Step-2: compute powers of 2 modulo 11

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

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

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

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

$\cancel{2^6 = 20}$

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

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

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

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

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

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

The smallest exponent for which $2^k \equiv 1 \pmod{11}$ is $k = 10$

$\therefore$ 2 is a primitive root modulo 11.

2. How many incongruent primitive roots does 14 have?

Ans: Primitive root only exist for:

$n = 1, 2, 4, p^k, 2p^k$ (p odd prime)

$14 = 2.7$

This matches the form $2p^k$, so primitive roots exist modulo 14.

compute $\phi(14)$

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

so, $\phi(6) = 2$

Conclusion, 14 has exactly 2 incongruent primitive roots.

3. Let a^{-1} be the multiplicative inverse of $a \pmod{n}$

3(a) Show that $\text{ord}_n a = \text{ord}_n(a^{-1})$

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

Ans:

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

proof:

Let, $\text{ord}_n(a) = k$, then $a^k \equiv 1 \pmod{n}$

Take inverse on both sides

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

Since, $(a^k)^{-1} \equiv (a^{-1})^k$

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

so, $\text{ord}_n(a^{-1}) \mid k$

Repeating the same arguement starting from $(a^{-1})^m \equiv 1$ shows:

$\text{ord}_n(a) \mid \text{ord}_n(a^{-1})$

Thus; $\text{ord}_n(a) = \text{ord}_n(a^{-1})$

yes, If a is a primitive root modulo n, then a^{-1} is also a primitie root.

P.T.O

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

<u>Proof</u>: If a is a primitive root modulo n,

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

From part (a):

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

so:

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