"Assignment"

1. Show that 2 is a primitive root modulo 11

Ans: we need to show that the smallest positive integer k for which

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

is $k = \phi(11) = 10$

Compute powers of 2 modulo 11:

$$2^1 \equiv 2 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^4 \equiv 16 \equiv 5 \pmod{11}$$
$$2^5 \equiv 10 \pmod{11}$$
$$2^6 \equiv 20 \equiv 9 \pmod{11}$$
$$2^7 \equiv 18 \equiv 7 \pmod{11}$$
$$2^8 \equiv 14 = 3 \pmod{11}$$
$$2^9 \equiv 6 \pmod{11}$$
$$2^{10} \equiv 12 \equiv 1 \pmod{11}$$

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

2. How many incongruent primitive roots does 14 have?

Ans:

First, find whether 14 has primitive roots.

A number n has primitive roots if and only if:

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

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

so 14 has primitive roots.

Number of incongruent primitive roots

$= \phi(\phi(14))$.

Compute:

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

$$\phi(\phi(14)) = \phi(6) = \phi(2 \times 3) = 1 \times 2 = 2$$

Therefore, 14 has 2 incongruent primitive roots.

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

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

Let $\text{ord}_n(q) = k$

Then by definition:

$$q^k \equiv 1 \pmod n$$

Take inverses on both sides:

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

so the order of q^{-1} divides k.

Similarly, if $(q^{-1})^m \equiv 1 \pmod n$, then $q^m \equiv 1 \pmod n$,

so the order of q divides m.

Hence, $\text{ord}_n(q) = \text{ord}_n(q^{-1})$.

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

since q is a primitive root,

$$\text{ord}_n(q) = \phi(n)$$

From (a),

$$\text{ord}_n(q^{-1}) = \text{ord}_n(q) = \phi(n)$$

Therefore, g^{-1} also has order $\phi(n)$, so it is also a primitive root modulo n.

$\therefore$ g^{-1} is also a primitive root modulo n.