Md. Nazmul Hasan
IT 24629

28.11.25

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

Ans: We need the order of 2 (mod 11) to be $\phi(11) = 10$. Compute powers of 2 modulo 11:

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

No smaller positive exponent gives 1, so the order of 2 mod 11 is 10. Hence

-2 is a primitive root modulo 11.

2. How many incongruent primitive roots does 14 have?

Ans: primitive roots modulo n (when they exist) come in number $\phi(\phi(n))$.

For $n=14$, we have, $\phi(14)$

$$= 14\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)$$

$$= 14 \cdot \frac{1}{2} \cdot \frac{6}{7}$$

$$= 6$$

Thus the number of primitive roots modulo 14 is,

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

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

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

b. If a is a ~~positive~~ primitive root modulo n, must a^{-1} also be a primitive root?

Ans:

(a) Let, $\text{Ord}_n(a) = k$

then by definition,

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

and k is the smallest positive integer for which this is true.

Now, multiply both sides by a^{-k}:

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

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

Thus, the order of a^{-1} be m.

Then, $(a^{-1})^m \equiv 1 \pmod{n}$

Taking inverses of both sides gives,

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

Hence, the order of a divides m.

Since, the order of a divides the order of a^{-1} and vice-versa, we conclude:

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

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

If a is a primitive root mod n, then, $\text{ord}_n(a) = \phi(n)$

From part (a),

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

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