Primitive Root

A number 'α' is a primitive root modulo n if every number coprime to n is congruent to a power of 'α' modulo n.

Definition made easy:

'α' is said to be a primitive root of prime number 'p', if α^1 mod p, α^2 mod p, α^3 mod p, . . . , α^{p-1} mod p are distinct.

Primitive Root

Example 1: Is 2 a primitive root of prime number 5?

Solution:

2^1 mod 5	2 mod 5	2	✓
2^2 mod 5	4 mod 5	4	✓
2^3 mod 5	8 mod 5	3	✓
2^4 mod 5	16 mod 5	1	✓

Yes, 2 is a primitive root of prime number 5.

Example 2: Is 3 a primitive root of prime number 7?

Solution:

3^1 mod 7	3 mod 7	3	✓
3^2 mod 7	9 mod 7	2	✓
3^3 mod 7	6 mod 7	6	✓
3^4 mod 7	18 mod 7	4	✓
3^5 mod 7	12 mod 7	5	✓
3^6 mod 7	15 mod 7	1	✓

Yes, 3 is a primitive root of 7.

Example 3: Is 2 a primitive root of prime number 7?

Solution:

2^1 mod 7	2 mod 7	2	✓
2^2 mod 7	4 mod 7	4	✓
2^3 mod 7	8 mod 7	1	✓
2^4 mod 7	16 mod 7	2	✗
2^5 mod 7	4 mod 7	4	✗
2^6 mod 7	8 mod 7	1	✗

No, 2 is not a primitive root of 7.

Question 1: Is 2 a primitive root of 11?

Question 2: What are the primitive roots of number 5?

Hint:

$1^1 \bmod 5$	$2^1 \bmod 5$	$3^1 \bmod 5$	$4^1 \bmod 5$
$1^2 \bmod 5$	$2^2 \bmod 5$	$3^2 \bmod 5$	$4^2 \bmod 5$
$1^3 \bmod 5$	$2^3 \bmod 5$	$3^3 \bmod 5$	$4^3 \bmod 5$
$1^4 \bmod 5$	$2^4 \bmod 5$	$3^4 \bmod 5$	$4^4 \bmod 5$