# PRIMITIVE ROOT

**Definition:** $g$ is a primitive root modulo $n$ if and only if for any integer $a$ such that $\gcd(a, n) = 1$, there exists an integer $k$ such that:

$$g^k \equiv \text{a} \pmod{\text{n}}$$

**Definition**: Let $n > 1$ and $\gcd(a, n) = 1$. The order of $a$ modulo $n$ is the smallest positive integer $k$ such that $a^k \equiv 1 \pmod{\text{n}}$

**Theorem:** Primitive root modulo $n$ exists if and only if $n = 1, 2, 4, p^k, 2p^k$ *, where p is odd prime*

**How to find the primitive root:**

If $g$ is primitive root modulo $n$, then $\gcd(g, n) = 1$ and $g$ is of order $\phi(n)$

Hence, to know if a number is a primitive root modulo $n$, we must check that there is no such a $p < \phi(n)$ such that $a^p \equiv 1 \pmod{\text{n}}$

Additionally, if $p$ exists, it has to be a divisor of $\phi(n)$

Hence, we just have to check all the divisors of the form $\frac{\phi(n)}{p_i}$ ($p_i$ *is prime factor of* $\phi(n)$) because other divisors $d$ satisfy : $d \mid \frac{\phi(n)}{p_i}$

## DISCRETE ROOT

Eq : $x^k \equiv r \ (mod\ m)$, $m$ is prime

Corner case: if $r = 0 \Longrightarrow x = 0$

Suppose we know $g$, primitive root of $m$ , then by definition there exists a $y$ that : $g^y \ \equiv x \ (mod\ m)$

Then:

$\Longrightarrow (g^y)^k \equiv r \ (mod\ m)$

$\Longrightarrow (g^k)^y \equiv r \ (mod\ m)$

We can find $y$ by discreteLog and then the answer is $g^y$.

If, additionally, $\gcd(m-1, k) = 1$ then

$x = r^u$ is a solution, where $ku - (m-1)v = 1$

That's because

$$x^k \equiv r^{ku}(mod\ m) \equiv r^{(m-1)v+1}(mod\ m)$$

$$\equiv r \cdot (r^{m-1})^v (mod\ m)$$

$$\equiv r \ (mod\ m)$$ (using Fermat's Little Theorem)