# 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:

$g^k \equiv \mathrm{a}\ (\mathrm{mod\ n})$

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

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

**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 $p(p < \phi(n)\ )$ that $a^p \equiv 1(\mathrm{mod\ n})$

Additionally, if this $p$ 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 divisor d satisfy : $d \mid \frac{\phi(n)}{p_i}$

## DISCRETE ROOT

Eq : $x^k\ \%\ mod = r$ , $mod$ is prime

Corner case: if $r = 0 => x = 0$

Suppose we know $g$, primitive root of $mod$ , then by definition there exists a $y$ that : $g^y\ \%\ mod = x$

Then :

- ⇨ $(g^y)^k \%\ mod = r$
- ⇨ $(g^k)^y \%\ mod = r$

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