# The Theory of Indices

Concept of Index was introduced by Gauss in his Disquisitiones Arithmeticae.

Let $n$ be any integer that admits a primitive root $r$.
As we know the first $\phi(n)$ powers of $r$.
$r, r^2, r^3, \ldots, r^{\phi(n)}$ are congruent modulo $n$ in some order to those integers less than $n$ and relatively prime to $n$, then $a$ can be expressed in the form

i.e $r^k \equiv a \mod n$, $1 \leq k \leq \phi(n)$

**Definition :-** Let $r$ be a primitive root of $n$. If $\gcd(a,n)=1$ then smallest positive integer $k$ s.t. $a \equiv r^k \mod n$, is called index of $a$ relative to $r$.

**Example:** The integer 2 is a primitive root of 5

$\therefore r=2,\ n=5,\ \phi(n)=4$

$\therefore r, r^2, r^3, r^4$ are congruent modulo 5 to the integers $a$ s.t $a<n$ and $\gcd(a,n)=1$

Let $a=2$, $\gcd(2,5)=1$

$r^1 \equiv 2 \mod 5$

$2^1 \equiv 2 \mod 5$ ✓ $\therefore$ index of 2 relative to 2 $=1$

$2 \not\equiv 2^2 \mod 5$

$2 \not\equiv 2^3 \mod 5$

$2^4 \equiv 2 \mod 5$

If $a=3$, $\gcd(3,5)=1$

$3 \equiv r^k \mod 5$

$3 \equiv 2^1 \mod 5$ ✗

$3 \equiv 2^2 \mod 5$ ✗

$3 \equiv 2^3 \mod 5$ ✓ $\therefore$ index of 3 w.r.t 2 $=3$

customarily,

$\boxed{ind_r a = \text{Index of a relative to } r}$

$a = r^K$

$K = \log_r a$

clearly $1 \le ind_r a \le \phi(n)$ and

$\because r^{ind_r a} \equiv a \bmod n$ or $r^K \equiv a \bmod n$, $\gcd(a,n)=1$

Ex. $r = 2$ is primitive root of 5.

$r^k \equiv a \bmod n \quad \gcd(a,n)=1 \quad \cancel{a < \phi(n)}$

$a < n$

$2^1 \equiv 2 \bmod 5 \qquad ind_2 4 = 2$

$2^2 \equiv 4 \bmod 5 \qquad ind_2 2 = 1$

$2^3 \equiv 3 \bmod 5 \qquad ind_2 3 = 3$

$2^4 \equiv 1 \bmod 5 \qquad$ ~~Index~~ $ind_2 1 = 4$

# If $a \equiv b \bmod n$ and $\gcd(a,n)=1$, $\gcd(b,n)=1$

$\because r$ is primitive root of $n$ then $ind_r a = ind_r b$

$\because r^{ind_r a} \equiv a \bmod n \qquad r^{ind_r b} \equiv b \bmod n$

$\because a \equiv b \bmod n \Rightarrow r^{ind_r a} \equiv r^{ind_r b} \bmod n$

$\Rightarrow ind_r a \equiv ind_r b \bmod \phi(n)$

**Theorem:-** If $n$ has a primitive root $\gamma$ and $ind_\gamma a$ denotes the index of $a$ relative to $\gamma$, then the following properties hold;

(a) $ind(ab) \equiv ind\, a + ind(b) \mod \phi(n)$

(b) $ind\, a^k \equiv k\, ind\, a \mod \phi(n)$ for $k > 0$

(c) $ind\, 1 \equiv 0 \mod \phi(n)$, $ind\, \gamma \equiv 1 \mod \phi(n)$

**Proof:** (1) by the defⁿ of index,

$\gamma^{ind\, a} \equiv a \mod n$ ①

$\gamma^{ind\, b} \equiv b \mod n$ ②

multiplying ① and ②

$\gamma^{ind\, a + ind\, b} \equiv ab \mod n$

$\gamma^{ind\, a + ind\, b} \equiv \gamma^{ind(ab)} \mod n$

$\Rightarrow ind(ab) \equiv (ind\, a + ind\, b) \mod \phi(n)$

(2) Since $\gamma^{ind\, a^k} \equiv a^k \mod n$ — ①

and $\gamma^{k\, ind\, a} = (\gamma^{ind\, a})^k \equiv a^k \mod n$ ②

from ① and ②, $\gamma^{ind\, a^k} \equiv \gamma^{k\, ind\, a} \mod n$

$\Rightarrow ind\, a^k \equiv k\, ind\, a \mod \phi(n)$

(3) $\gamma^{ind\, 1} \equiv 1 \mod n$ from ② $ind\, 1$

$\gamma^{ind\, 0} \equiv 0 \mod n$

# Application of Indices

Consider $x^K \equiv a \bmod n$ $K \geq 2$
where $n$ is +ve integer having primitive root and

$gcd(a,n)=1$

from Thm part ⓐ & ⓑ

$K\, \underline{ind\, x} \equiv ind\, a \bmod (\phi(n))$

if $d = gcd(K, \phi(n))$ and $d \nmid ind\, a$, there is no soln. but $d \mid ind\, a$ then there are exactly $d$ values of $ind\, x$.

$\Rightarrow$ there are $d$ incongruent sol$^n$s of $x^K \equiv a \bmod n$

<u>note</u>: If $K=2, n=p$ the congruence

$\boxed{x^2 \equiv a \bmod p}$

has a soln iff $2 \mid ind\, a$, ~~when~~

infact $x^2 \equiv a \bmod p$ has exactly two solutions.

<u>Ex</u>: Solve $4x^9 \equiv 7 \bmod 13$

<u>sol$^n$</u> first of all fix a primitive root $r = 2 \bmod 13$