→ Large Exponentiation with ETF & Euler's Theorem

50

Scanned with CamScanner

∴ Now, If we have something like this : $(a^{b^c}) \% M$

$\Rightarrow ((a \% M)^{(b^c \% M)}) \% M$ ⇒ We can't solve it like this,

This is wrong.

e.g. $(50^{64^{32}}) \% M$

here, $b = 64^{32}$, ∴ It is too large no. for a power.

∴ We will reduce this first in some other form.

Imp: What is co-prime number?

→ If we have some number: a, b then gcd (a, b) = 1

→ EPF ⇒ (Euler Patient Function) (ϕ)

It is represented as $\phi(N)$

where N → count K such that $1 \le K \le N$

where, N, K are coprime.

e.g $N = 5 \rightarrow 1, 2, 3, 4, \cancel{5}$

$\phi(5) = 4$

e.g $N = 6 \rightarrow 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}$

$\phi(6) = 2$

→ Mathematical formula for $\phi(n)$

$$\boxed{\phi(n) = n \times \prod_{n|p} \left(1 - \frac{1}{p}\right)}$$

IMP

$\prod$ → Multiplication symbol, just like Σ of addition.

p → All prime factors of N.

NOTE: We will consider only unique value of p.

e.g: $n = 5$

$$\phi(n) = n \times \prod_{n|p} \left(1 - \frac{1}{p}\right)$$

$$\phi(5) = 5\left(1 - \frac{1}{5}\right) = 4$$

e.g: $n = 6$

$$\phi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$$

$$= \cancel{6} \times \frac{1}{\cancel{2}} \times \frac{2}{\cancel{3}}$$

$$\Rightarrow 2$$

→ Euler's Theorem:

$$\boxed{a^b \equiv a^{b \bmod \phi(n)} \bmod (n)}$$

($\equiv$ → congruent to)

→ What this ≡ (congruency) symbol determine:

e.g.: $a \equiv b \bmod (n)$

It ~~means~~ means, if we divide a with ~~b~~ n then we will get b as remainder. $(a \% n) = b$

→ Now following Euler's Theoram:

$a^b \equiv a^{b \bmod \phi(n)} \bmod (n)$

$$\boxed{\Rightarrow (a^b \% n) = (a^{b \% \phi(n)}) \% n}$$

∴ Now, If we have to calculate

$(a^b \% M)$ where b is a very large no.

We can reduce it to: $(a^{b \% \phi(m)}) \% M$

→ In most of the cases, we have M a prime number.

∴ If n is prime

$\phi(n) = n\left(1 - \frac{1}{n}\right)$

$\Rightarrow n - 1$

$\therefore$ Finally we have two reduced formulas:

1) If M is any no.

$$\boxed{a^b \% M = a^{b \% \phi(M)} \% M}$$

2) If M is prime no.

$$\boxed{a^b \% M = a^{b \% (M-1)} \% M}$$