

~~if~~ if b value is going to increase

$$(50 \cdot 69^{32}) \bmod 109+7 \rightarrow ①$$

(a, b) are coprime when $\gcd(a, b) = 1$
 without 1, there is no common factors.

ETF \rightarrow Euler's totient function.

$N \rightarrow$ no ETF will be the number of coprime with N which is less than 1 from N. shortly,

$N \rightarrow$ count k such that $1 \leq k \leq N$ and k is coprime to N.

ETF represent by ϕ .

coprime with 5 = 1, 2, 3, 4. $\rightarrow 4$ total.

So, $\phi(5) = 4$

The formula for finding number of coprime,

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

\downarrow
 unique numbers of prime

If ~~there is~~ $n = p \times q \times r$ where
 p, q, r prime numbers. Then,

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

for $n = 6$, $6 = 2 \times 3$

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

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

$$= 2$$

$$\boxed{\phi(n) = n - 1}$$

For, prime numbers,

Euler's theorem: $(a^b) \% m$, $b \in \mathbb{Z}$

mod term ~~express~~ ~~is~~ ~~for~~
 expressing, we will use euler's

theorem.

Euler's theorem:

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

→ congruency of numbers

$a \equiv b \pmod{n}$, it means if we divide a by n , the remainder will be b .

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

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

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

if n is prime, then,

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

for prime m , $\phi(m) = (m-1)$

So, $50^{6432} \% m$

As m is prime number.

So, $\Rightarrow 50^{6432 \% m-1}$

\downarrow
 $92m \pmod m$
~~convert~~
 convert.

exponential

After binary exponential, it returns a small value of $m-1$.

Something integer value
50 % m

second binary exponentials.

$a * a \rightarrow a = 10^8$ greater than. So, it is not possible.

$a * a = a + a + a + \dots + a$ times.

example: $5 * 2 = 5 + 5 = 10$

means, 5, 2 times addition.

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

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

As M is prime

bitwise exponential