ETF and Eular's Theorem

06 November 2021 15:26

ETF

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

$p \to$ all prime factors of n (distinct)

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

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

Eular's Theorem

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

$$a \equiv b \bmod (n) \Rightarrow a \% n = b$$

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

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

$\phi(M) = ETF$

if n is prime

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

$$a^b \% M = a^{b \% \phi(M)} \% M \to M \text{ is not prime}$$

$$a^b \% M = a^{b \% (M-1)} \% M \to M \text{ is prime}$$

Q. $50^{64^{32}} \% M$

$$= 50^{(64^{32} \% M - 1)} \% M$$

binExp again!