MMI

06 November 2021 16:10

Modular Multiplicative Inverse.

$$(A/B)\%M \neq \left(\frac{A\%M}{B\%M}\right)\%M$$

$$(A/B)\%M = (A \times B^{-1})\%M$$

$$= \left((A\%M) \times \underbrace{(B^{-1}\%M)}_{\text{MMI of B}}\right)\%M$$

$A * B = 1$

B is MI of A

$(A * B)\%M = 1$

$\Rightarrow$ B is MMI of A.

$$1 \leq B < M-1$$

MMI is defined if A and M are coprimes.

Method 1 Looping from 1 to M-1

if $(A*B)\%M == 1$

B is MMI. $O(M)$ Complexity.

Method 2 Fermet's little Theorem

$$A^{M-1} = 1 \mod(M)$$

M is prime
A is not multiple of M.

$$A^{M-2} \equiv A^{-1} \mod(M)$$

$$(A^{M-2}\%M) = A^{-1}$$

binExp(A, M-2)
(log(M) comp.)

If M is not a prime,
MMI is calculated using Extended Euclid Algo.