

Fermat's little theorem extension:-

If p is prime no.

$$(a^{p-2}) \bmod p = (a^{-1}) \bmod p$$

this can be calculated using modular exponentiation.

multiplicative mod inverse

suppose $a \times b \equiv 1$

b is multiplicative inverse of a . and $b \equiv a^{-1}$

now $(a \times b) \bmod m \equiv 1$ here b is multiplicative mod inverse of a .

Def: definition:- a mein aisa kya multiply karoon k multiplication k baad mod by m karne k baad 1 aa jaye

$$b \equiv (a^{-1}) \bmod m$$

now you will have to find b using a and m .

and fermat's says that if m is prime then $a^{-1} \bmod m \equiv (a^{m-2}) \bmod m$.

let $a \equiv 3$ $m \equiv 11$, we can tell that you should multiply $a(3)$ with 4. so that $3 \times 4 \equiv 12 \div 11 \equiv 1$.