# Algebra

## Modular Multiplicative Inverse (MMI)

Modular multiplicative inverse of a number **a mod m** is number **x** where

Ex. m = 7, a = 4, then x = 2 as (4 \* 2) mod 7 = 1

Multiplicative inverse of 4 mod 7 is 2.

**Rules**

* (a + b) mod m = ((a mod m) + (b mod m)) mod m
* (a – b) mod m = ((a mod m) – (b mod m)) mod m
* (a \* b) mod m = ((a mod m) \* (b mod m)) mod m
* Division is not distributed so can do like (a / b) mod m = (a \* b-1 ) mod m

### Fermat’s Theorem for MMI

If **m** is a prime number then

Ex. m = 5 (prime) , a = 3 then 3(5-1)  mod 5 = 1

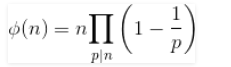
**MMI**

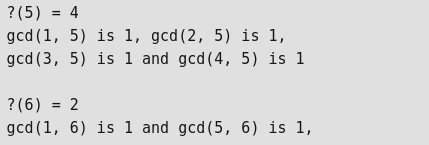
It can be written as so here is the multiplicative inverse.

What if when **m** is non-prime, there we will use **Euler Totient** theorem

### Euler Totient

Euler Totient function for an input **n** finds the numbers from {1,2,3 …. n} which are relative prime to **n** i.e. the numbers whose GCD with n is 1





**MMI**

If **a** and **m** are co-prime i.e. GCD(a,m) = 1 then where and leads to is the **MMI.**