Multiplicative Modulo Inverse

Multiplicative Inverse

If there exist two integers such that

$$\mathbf{A.B = 1}$$

then B is known as the multiplicative inverse of A. Therefore $\mathbf{B = A^{-1}}$, i.e. B is the multiplicative inverse of A.

Multiplicative Modulo Inverse

Let's say, there exist two integers x and y such that

$$\mathbf{(x.y) \bmod m = 1}$$

then y is multiplicative modulo inverse of x and is denotes by x^{-1}

Now,

$$(x.y) \bmod m = 1$$
$$(x.y-1) \bmod m = 0$$

This means that x.y -1 is divisible by m

$$x.y - 1 = mq, \text{ for some integer } q$$
$$x.y - mq = 1$$
$$x.y + m(-q) = 1$$
$$\mathbf{x.y + mQ = 1}$$

Now the above equation resembles the linear diophantine equation, therefore for some integers y and Q, gcd(x, m) should be a factor of 1.

So gcd(x. m) = 1.

This means that a and m are co-prime.

Now, the Extended Euclid algorithm can be used to find the values of y and Q on the above equation.