Multiplicative inverse mod n

If GCD(a,n) = 1, then a has a multiplicative inverse mod :

$$a^{-1} * a \bmod n = a * a^{-1} \bmod n = 1$$

- The inverse can be calculated by writing down the equations which are the steps of Euclid's algorithm, when GCD(a,n) is calculated.

- Then we go backwards from bottom up eliminating the remainders, until we get gcd (= 1) as a linear combination of a and n.

- The coefficient of a in the combination is the required inverse.

Example: Calculate $13^{-1} \bmod 23$

GCD steps

$23 = 1*13 + 10$

$13 = 1*10 + 3$

$10 = 3*3 + 1 = gcd$

$3 = 3*1 + 0$

Linear combination steps

$1 = 10 - 3*3$

Start from the 3rd line of gcd

$1 = 10 – 3*\mathbf{(13 - 10)}$

$1 = 10+3*10 – 3*13$

$1 = -3*13 + 4*10$

Replace remainder 3 with combination obtained from 2nd line of gcd:

3 => 13 - 10

$1 = -3*13 + 4*(23 – 13)$

$1 = – 3*13 – 4*13 + 4*23$

$1 = -7*13 + 4*23$

Replace remainder 10 with combination obtained from 1st line of gcd

10 => 23 - 13

Inverse of 13 = -7 mod 23 =

23 – 7 = **16**

a^{-1} mod n using Euler's theorem

If we know the factors of modulus n, we can calculate easily the value of Euler's totient function $\varphi(n)$.

By Euler's theorem $a^{\varphi(n)} \bmod n = 1$

Multiplying the equation with a^{-1} we conclude , that if inverse exists, it is

$$\boxed{a^{-1} = a^{\varphi(n)-1} \bmod n}$$

In the famous RSA algorithm $n = p*q$ (product of two primes),

and $\varphi(n) = (p-1)(q-1)$. Hence

$$\boxed{a^{-1} = a^{(p-1)(q-1)-1} \bmod n \text{ , if } n = p*q\text{, where } p,q \text{ are primes}}$$