Modular Multiplicative inverse

Arabic Animated intuition

Modular Multiplicative Inverse

$A*B=1$

find B such that it satisfies the equation

$B=1/A$

or

A^{-1}

$1/A=A^{-1}$

$1/A^2=A^{-2}$

$1/A^3=A^{-3}$

please don't forget the above rules

Modular Multiplicative Inverse

What's modular multiplicative inverse ?

find B such it that satisfies the following equation:

(A*B)%M=1

Here B is the modular multiplicative inverse of A under modulo M.

B is said to be modular multiplicative inverse of A under modulo M
if it satisfies the following equation:

$$A.B \equiv 1 (mod M)$$

B in range(0,m-1)

Modular Multiplicative Inverse

(A*B)%M=1

B is said to be modular multiplicative inverse of A under modulo M if it satisfies the following equation:

$$A.B \equiv 1(modM)$$

(A*B)%M=1%M

$$A \equiv B(\mathrm{mod}\ C)$$

Congruence modulo
meaning A%C=B%C

B in range(0,m-1)

B in range(0,m-1)
(A*B)%M=((A%M)*(B%M))%M
and B%M in range 0 to m-1

Modular Multiplicative Inverse

(A*B)%M=1,

B is said to be modular multiplicative inverse of A under modulo M if it satisfies the following equation:

$$A.B \equiv 1(modM)$$

Existence of modular multiplicative inverse :

An inverse exists only when A and M are coprime .
gcd(A,M)=1

Modular Multiplicative Inverse

(A*B)%M=1

B is said to be modular multiplicative inverse of A under modulo M if it satisfies the following equation: $A.B \equiv 1(mod M)$

Ax+By=gcd(A,B) bezout's theorem

Ax+My=gcd(A,M)

Ax+My=1 let's take %M

(Ax+My)%M=1%M

((Ax)%M+(My))%M)%M=1%M

(Ax)%M=1%M

we want to prove that
A and M coprime gcd(A,M)=1
then an inverse exists

$$ax \equiv 1 \mod m.$$

Modular Multiplicative Inverse

input : A,M   (A*B)%M=1   find B such that it satisfies the equation

approach 1 brute force

```
int modInverse(int A,int M)
{
    A=A%M;
    for(int B=1;B<M;B++)
        if((A*B)%M)==1)
            return B;
}
```

Modular Multiplicative Inverse

input : A,M   (A*B)%M=1   find B

Approach 2

B is said to be modular multiplicative inverse of A under modulo M $A.B \equiv 1(modM)$

Ax+By=gcd(A,B) bezout's theorem

Ax+My=gcd(A,M)

Ax+My=1   let's take %M

(Ax+My)%M=1%M

((Ax)%M+(My))%M)%M=1%M

(Ax)%M=1%M

$$ax \equiv 1 \mod m.$$

```
int d,x,y;
int modInverse(int A, int M)
{
    extendedEuclid(A,M);
    return (x%M+M)%M;    //x may be negative
}
```

Modular Multiplicative Inverse

input : A,M   (A*B)%M=1   find B such that it satisfies the equation

Approach 3 (used only when M is prime)

B=A^{-1}

This approach uses Fermat's Little Theorem.
The theorem specifies the following:
if p is prime

$$a^{p-1} \equiv 1 \pmod{p}.$$

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

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

```
int modInverse(int A,int M)
{
    return modularExponentiation(A,M-2,M);
}
```