Modular Arithmetic for Competitive Programming

If a is dividend, b is divisor, q is quoitent and r is remainder, then

```
a mod b = r
a / b = q
a = b*q + r
```

Here a mod b is only possible when both are integer and 0 <= r <= b-1

Division Rules:

```
If a | b and a | c, then a | (b + c)                 (a | b : a divides b, i.e. b/a)
If a | b, then a | (b*c) for all integers c
If a | b and b | c, then a | c
```

Generally 'a mod m' is the biggest multiple of m which is less than (or equal to) a. So,

```
-13 mod 3 = ?
as, -13 = 3*(-5) + 2
so, -13 mod 3 = 2                 (mod value is always positive)
```

Congurency

Let a and b two integers such that a ≠ b, and m is co-prime of both a and b, and

```
a mod m = p
b mod m = q
```

Then a and b is congurent iff

```
p = q
so, a mod m = b mod m
written as, a ≡ b (mod m)
```

If a is congurant to b modulo m, then it can be said that m divides a-b:

```
a-b / m = k       (k is any integer)
```

If a □ b (mod m) and c □ d (mod m), then

```
a+c ≡ b+d (mod m)
a*c ≡ b*d (mod m)
```

Sum, Multiplication and Division Rule in Modular Arithmetic

Sum rule states that

```
a + b = ( (a mod m) + (b mod m) ) (mod m)
```

Multiplication rule states that

```
a * b = ( (a mod m) * (b mod m) ) (mod m)
```

Division rule states that

```
a / b = ( a * (1/b) ) (mod m)       (1/b is modular inverse of m, described below)
```

Modular Operation on exponentiation

```
(a ^ b) (mod m) = ( a ^ (b (mod mod-1)) ) (mod m)           (According to Fermat
Theorem)
```

Modular Inverse:

For any value, a and modulo m, where gcd(a, m) = 1 (This states that a and m is co-prime). If the modular inverse is b, then

```
a * b ≡ 1 (mod m)
or, 1 ≡ a*b (mod m)                      (Side Changing, as a % m ≡ b % m, is same
as: b % m ≡ a % m)
or, b ^ (-1) ≡ a (mod m)                 (Shifting a from right to left)
Finally,   b ^ (-1) ≡ a (mod m)          ( b^(-1) is the modular inverse of a mod
m)
```

So, to find modular inverse of a mod b, we need to search for such a value, so that the mod of a * b is 1. To find modular inverse of any value a mod m, we may iterate through 1 to m-1 and check if the mod of their multiplication is equal to 1. Example, a = 3, m = 8: 3 * 1 (mod 8) = 3 3 * 2 (mod 8) = 6 3 * 3 (mod 8) = 1 (3 is the modular inverse of 3 mod 8)

To be noted that, modular inverse of a mod m depends on both value a and b, and they must be co-prime. Try for case a = 3, m = 7 (result : 5) and a = 3, m = 6 (no result exists!)

Fermat's Little Theorem:

If p is prime, and a and p is co-prime (gcd(a, p) = 1), then

```
a ^ (p-1) ≡ 1 (mod p)                               (Can be written as a ^ p ≡ a
(mod p))
```

From this theorem, it can be stated that: * a ^ (p-1) - 1 is divisable by p * (a ^ p) - a is divisable by p

Calculating Modular inverse from Fermat Theorem:

If a and m is co-prime and m is prime (this conditions are stated in fermat theorem), then

```
a ^ (m-1) ≡ 1 (mod m)
or, 1 ≡ ( a ^ (m - 1) (mod m) )                         (Side Changing, as a % m ≡ b
% m, is same as: b % m ≡ a % m)
or, a ^ (-1) ≡ ( a ^ (m-1) * a ^ (-1) (mod m) )        (Multiplicating a ^ (-1) both
sides)
Finally, a ^ (-1) ≡ ( a ^ (m-2) ) (mod m)
```

So we can calculate modular inverse (a^(-1)) by finding (a ^ (m-2)) (mod m)

We can also prove how modular arithmatic on exponents work, go through this link