How to use modulo operation on competitive programming

Contents

※ mod indicates modulo operation (represented '%' on C++.)

1. Custom on competitive programming

- In many problems about combination, we answer the number **modulo 1000000007**
- Thus we prepare MOD as constant value:

```
#define MOD 1000000007
```

- since C++11, we also use constexpr:

```
constexpr long long MOD = 1000000007;
```

- Node that **1000000007 is a prime number**
- Sometimes 1000000009 or 998244353 are used (prime numbrs!)

2. How is mod used as +, -, and *

We have to take care of overfllow to use mod.

1. write usually
2. cover expression with ()=%
3. make function modXXX
   ex) modadd, modsub, modmul

2.1. Write usually

Note that a and b should be less than MOD.

```
a = (a + b) % MOD;
a = (a * b) % MOD;
// write not (a - b) but (MOD + (a - b)) for fear (a - b) < 0
a = (MOD + (a - b)) % MOD;
```

Another method

```
a += b;
a %= MOD;

a += MOD - b;
a %= MOD;

a *= b;
a %= MOD;
```

2.2. Covering with ()%=MOD

```
// apply modulo operation to a and b in advance
a %= MOD;
b %= MOD;

(a += b) %= MOD;
(a += MOD - b) %= MOD;
(a *= b) %= MOD;
```

2.3. make function modXXX

prepare as library:

```cpp
long long modadd(long long &a, long long b) {
  (a += b) %= MOD;
}

long long modsub(long long &a, long long b) {
  (a += MOD - b) %= MOD;
}

long long modmul(long long &a, long long b) {
  (a *= b) %= MOD;
}
```

how to use:

```
modadd(a, b);
modsub(a, b);
modmul(a, b);
```

3. How is mod used as division

In sammary, we can use this fact:

If p is a prime number, and a and b is less than p:

$$\frac{a}{b} \equiv ab^{p-2} \pmod{p}$$

- 1000000007 is a prime, so you can use that.
- b^{p-2} can calculate fast with exponentation by squaring.

```
long long moddiv(long long a, long long b) {
  return (a * modpow(b, MOD - 2)) % MOD;
}
```

Addition

- Some people make the class **modint** to use modulo operation easily.
- modint class is made using operator overloading.
- If you want to know this, please ask google.

Example:

```
class modint {
  ...
}

modint a, b;
modint n1, n2, n3, n4;
n1 = a + b;
n2 = a - b;
n3 = a * b;
n4 = a / b;
n5 = pow(a, b);
```

Appendix

Proof of a/b = a*b^(p - 2)

Bellow is a proof of this fact.

- You don't have to understand the proof if you only use it.

Outline of proof

1. Definition of congruence relation: $a \equiv b$
2. Definition of $\frac{a}{b}$
3. Proof of $a \equiv b \Rightarrow ka \equiv kb$
4. Inverse element: b^{-1}: $\frac{a}{b} \equiv ab^{-1}$
5. Fermat's little theorem $b^{-1} \equiv b^{p-2} \pmod p$ if p is a prime number

1. Definition of congruence relation

$$a \equiv b \pmod{m} \Leftrightarrow \ \exists k \in \mathbb{Z} \; s.t. \; a - b = mk$$

2. Definition of divition

When thinking of modulo m,
$\dfrac{a}{b}$ is defined as x such that $bx \equiv a \pmod{m}$

Example

About $\frac{4}{3}$ in modulo 7: x such that $3x \equiv 4 \pmod 7$

When $x \equiv 6$:

$$3x \equiv 3 \cdot 6 \equiv 18 \equiv 4 \pmod 7$$

thus $\frac{4}{3} \equiv 6 \quad (\text{mod } 7)$

3. Proof of characteristics of modulo arthmetics

$$a \equiv b \Rightarrow \forall k \in \mathbb{Z},\ ka \equiv kb \pmod{m}$$

Proof:

$$\begin{aligned} a \equiv b \pmod{m} &\Rightarrow a - b = m \cdot l \ (l \in \mathbb{Z}) \\ &\Rightarrow ka - kb = m \cdot kl \\ &\Rightarrow ka \equiv kb \pmod{m} \end{aligned}$$

※ Converse is not always true.

If you want to know details, please see this

4. Inverse element

- Inverse element of b is defined as x such that $bx \equiv 1 \pmod{m}$.
- It is represented as b^{-1} or $\dfrac{1}{b}$.

If we know b^{-1}, we can easily answer $\frac{a}{b}$:

$$\begin{aligned} bx \equiv a &\Rightarrow b^{-1}bx \equiv b^{-1}a \\ &\Rightarrow 1 \cdot x \equiv b^{-1}a \\ &\Rightarrow x \equiv ab^{-1} \end{aligned}$$

thus $\frac{a}{b} = ab^{-1}$.

- Inverse element in modular arthmetics does not always exist.

5. Fermat's little theorem:

If a is integer, p is a prime number, and $gcd(a, p) = 1$:

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

- There are various proofs of this theorem (this margin is too narrow to contain!)

If p is a prime number, you can know b^{-1}:

$$b^{p-1} \equiv 1 \pmod p \ ; \ \text{Fermat's Little Theorem}$$

$$\Rightarrow b\underline{b^{p-2}} \equiv 1 \pmod p$$

b^{-1} is x such that $b\underline{x} \equiv 1 \pmod p$.

$\Rightarrow \ b^{-1} \equiv b^{p-2} \pmod p$

In sammary,

$$\frac{a}{b} \equiv ab^{-1} \equiv ab^{p-2}$$