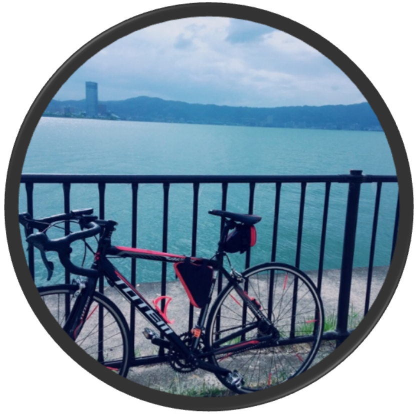
逆元の計算

xryuseix



HELLO!

Twitter : @ryusei_ishika

Username : xryuseix

Group : RiPPro (leader), RiST (sub-Leader)

お先に

$$A + B = (A\%P + B\%P)\%P$$

$$A - B = (A\%P + P - B\%P)\%P$$

$$A \times B = (A\%P \times B\%P)\%P$$

やりたいこと

A / B (mod P) を計算したい

A * X (mod P) なら計算できるので,
1/B=X (mod P)となるXが知りたい.

逆元とは

$$X^{-1} \equiv \frac{1}{X} \ (mod\ P)$$

逆元　　　分数

フェルマーの小定理とは

$$a^{P-1} \equiv 1\ (mod\ P)$$

- $1^6 = 1 \equiv 1 \pmod{7}$
- $2^6 = 64 \equiv 1 \pmod{7}$
- $3^6 = 729 \equiv 1 \pmod{7}$
- $4^6 \equiv (-3)^6 = 3^6 \equiv 1 \pmod{7}$
- $5^6 \equiv (-2)^6 = 2^6 \equiv 1 \pmod{7}$
- $6^6 \equiv (-1)^6 = 1^6 \equiv 1 \pmod{7}$

https://qiita.com/drken/items/6b4031ccbb2cab7436f3

逆元の計算

$$a^{P-1} \equiv 1 \ (mod\ P)$$

両辺をaで割る

$$a^{P-2} \equiv \frac{1}{a} \ (mod\ P)$$

逆元の計算

$$a^{P-2} \equiv \frac{1}{a} \pmod{P} \qquad X^{-1} \equiv \frac{1}{X} \pmod{P}$$

$$a^{P-2} \equiv a^{-1} \pmod{P}$$

逆元の計算

$$a^{P-2} \equiv a^{-1} \pmod P$$

aのP-2乗　aの逆元

Point !!

mod Pの世界で，aをP-2乗するとaの逆元となる

つまり，aで割るという操作はaのP-2乗をかけることと等しい

逆元の計算 ~実装~

```cpp
int pow(const int x, const int y, const int mod) {
    long long int res = 1;
    for(int i = 0; i < y; i++) {
        res *= x;
        res %= mod;
    }
    return res;
}

int main() {

    const int P = 1e9 + 7;
    int a = 8;
    int _a = pow(a, P-2, P);
    cout << "a: " << a << " a^{-1}: " << _a << endl;
}
```

このままだと計算量は

$O(P)$ (P=10^9+7)

繰り返し二乗法とは

$$\mathrm{X}^{22} = X^{2+4+16} = X^2 * X^4 * X^{16}$$
$$= X^{2^1} \times X^{2^2} \times X^{2^4}$$

また,

$$22 = 10110_{(2)} = 2^1 + 2^2 + 2^4$$

逆元の計算 ~繰り返し二乗法~

```cpp
int pow(long long int x, int y, const int mod) {
    long long int res = 1;
    while(y > 0) {
        if(y % 2) {
            res = res * x % mod;
        }
        x = x * x % mod;
        y /= 2;
    }
    return res;
}

int main() {

    const int P = 1e9 + 7;
    int a = 8;
    int _a = pow(a, P-2, P);
    cout << "a: " << a << " a^{-1}: " << _a << endl;
}
```

これで計算量は

$O(\log_2 P)$ (P=10^9+7)

逆元の計算 ~結論~

$$\frac{\mathrm{A}}{B} \equiv A \times \overset{\text{逆元}}{B^{-1}} \equiv A \times B^{P-2} \pmod{\mathrm{P}}$$

実際に計算する時

$$\frac{\mathrm{A}}{B}\%P \Rightarrow (A\%P \times (B^{P-2}\%P))\%P$$

逆元の計算 ~拡張ユークリッドの拡張~

$$ax \equiv 1 (mod\ P)$$

$$ax = 1 + Py$$

$$ax + (-Py) = 1$$

→ 一次不定方程式の解

演習課題

A.
整数が9個あり，それぞれの値は
[1, 1, 1, 2, 2, 2, 2, 3, 3]
です．並べ方は幾つでしょう？

B.
アルファベットが26*(26+1)/2
個あります.
Aが1個，Bが2個，…Zが26個です．並べ方は幾つでしょう？