逆元

定义

对于非零整数 a, m，如果存在 b 使得 $ab \equiv 1 \pmod{p}$，就称 b 是 a 在模 m 意义下的 **逆元**（inverse），记作 $b = a^{-1} \pmod{p}$。

> **特别注意**
>
> 如果 $a \equiv 1 \pmod{m}$，则称 a 在模 m 意义下 **不存在逆元**，因为 **任意数** 都是 a 在模 m 意义下的逆元。

背景

我们知道，对于除法操作来说取模操作不具有分配性，即：

$$\frac{a}{b} \bmod p \neq \frac{a \bmod p}{b \bmod p}$$

~~毕竟一般的取模操作只对整数有意义。~~

这时候需要引入逆元进行操作：

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

> **举个例子**
>
> $$\frac{10}{5} \pmod{3} \neq \frac{10 \bmod 3}{5 \bmod 3}$$
>
> 在模 3 意义下$5 \times 2 \equiv 1 \pmod{3} \Rightarrow$ 2是5在模3意义下的逆元
> 故：
>
> $$\frac{10}{5} \bmod 3 = (10 \times 2) \bmod 3 = 20 \bmod 3 = 2$$

由此也可以引申出有理数的取模运算：

给出一个有理数 $c = \frac{a}{b}$，则 $c \bmod p$ 的值被定义为 b 在模 p 意义下的逆元。

求解方法

费马小定理

> **费马小定理**
>
> 设 p 是素数，a 是不被 p 整除的整数，则有：
>
> $$a^{p-1} \equiv 1 \pmod{p}$$
>
> 由此可得：
>
> $$a^{p-2} \equiv a^{-1} \pmod{p}$$
>
> 即 a 在模 p 意义下的逆元为 $a^{p-2} \bmod p$。

使用快速幂求解即可。

```
int qpow(int a,int b){
    int ret = 1;
    for(;b;b>>=1,a*=a,a%=mod)if(b & 1)ret *= a,ret %= mod;
    return ret;
}
int inverse = qpow(b-1,mod-2)
```

扩展欧几里得算法

$ax \equiv 1 \pmod{p}$ 可转换成一个 丢番图方程 的形式：$ax - bp = 1$

通过线性同余方程求解。