信息学

基础数论二-同余与EXgcd

西南大学附属中学校

信息奥赛教练组

前情提要

西南大学附属中学 High School Affiliated to Southwest University

前面我们已经学习了质数、约数的相关概念和知识
数论里，同余这一概念也非常重要

同余

设m是给定的一个正整数，a、b是整数，若满足m|(a-b)，则称a与b对模m同余，记为a≡b(mod m)

简单来说，如果x%p=y%p，x,y对于p的余数相同，称为同余

同余

同余式的性质

1. 自反性：$a \equiv a(mod\ m)$
2. 对称性：若$a \equiv b(mod\ m)$, 则$b \equiv a(mod\ m)$
3. 传递性：若$a \equiv b(mod\ m)$,$b \equiv c(mod\ m)$，则 $a \equiv c(mod\ m)$
4. 消去律：$ac \equiv bc(\%p) \rightarrow a \equiv b(\%\frac{p}{gcd(c,p)})$
5. $a \equiv b(\%cd) \rightarrow a \equiv b(\%d)$
6. $(a \equiv b(\%d), a \equiv b(\%c)) \rightarrow a \equiv b(\%lcm(c,d))$
7. 若$a \equiv b(\%p)$,则对任意c有，$(a+c) \equiv (b+c)(\%p)$
8. 若$a \equiv b(\%p)$,则对任意c有，$(a \times c) \equiv (b \times c)(\%p)$
9. 若$a \equiv b(\%p)$,则对任意c有，$(a^c) \equiv (b^c)(\%p)$
10. 若$a \equiv b(\%p)$, $c \equiv d(\%p)$则，$(a+c) \equiv (b+d)(\%p)$
    $(a-c) \equiv (b-d)(\%p)$
    $(a*c) \equiv (b*d)(\%p)$

自己下来慢慢看

值得注意的地方：
同余满足加、减、乘，但没有除

问题：如果要求除法怎么办?

a/c(%p)　　b/c(%p)

$a*c^{-1} \equiv b*c^{-1}\ (\%p)$

c^{-1}称为a的乘法逆元
逆元也称为数论倒数

回顾：欧拉函数

对于一个正整数n，小于n且和n互质的正整数（包括1）的个数，记作φ(n)。

$\varphi(n)=n*(1-1/p_1)(1-1/p_2)(1-1/p_3)*(1-1/p_4)\ldots\ldots(1-1/p_n)$

其中p_1, p_2……p_n为n的所有质因数，n是不为0的整数。φ(1)=1（唯一和1互质的数就是1本身）

对于任何两个互质 的正整数a,n(n>2)有:$a^{\varphi(n)} \equiv 1 \bmod n$，即 **欧拉定理**

当n=p 且 a与素数p互质(即:gcd(a,p)=1)则上式有: $a^{(p-1)} \equiv 1 \bmod n$，即 **费马小定理**

未学习数论第一课的同学可以找我拿：基础数论一课件

费马小定理

假如a是一个整数，p是一个质数

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

证明略

乘法逆元

如果ax≡1(mod p)，且a与p互质（gcd(a,p)=1），则称a关于模p的乘法逆元为x，x=inv[a]

逆元的作用题目中要求对答案取模，但我们又不得不使用一般的除法的时候，就需要用逆元的乘法来代替除法

听了前面PPT介绍的东西，你觉得逆元可以怎么求?

乘法逆元的求法

四种方法：

- 欧拉定理求逆元
- 费马小定理求逆元
- 递推求逆元
- 扩展欧几里得求逆元

求解乘法逆元

费马小定理求解逆元

p为质数

费马小定理：若p为素数/质数，则有 $a^{p-1} \equiv 1 \pmod{p}$

推理：$a^{p-2} \times a \equiv 1 \pmod{p}$，即 a^{p-2} 就是 a 在模 p 意义下的逆元。

欧拉定理求解逆元

a,p为互质

欧拉定理：若 a, p 互素，则有 $a^{\varphi(p)} \equiv 1 \pmod{p}$，(费马小定理的一般形式)

推理：$a^{\varphi(p)-1} \times a \equiv 1 \pmod{p}$，即 $a^{\varphi(p)-1}$ 就是 a 在模 p 意义下的逆元。

```
LL qpow(LL a,LL p,LL mod){  //快速幂
        LL t=1,x=a%mod;
        while(p)
        {
                if(p&1) t=t*x%mod;
                x=x*x%mod;
                p>>=1;
        }
        return t;
}
LL getinv(LL a,LL mod)
{
        return qpow(a,mod-2,mod);
}
```

递推求解逆元

p 是模， a 是待求逆元，则 a^{-1} 是 a 在模 p 意义下的逆元。

$p = k \times a + r$ ，令 $r < a$ ，则 $k = \left[\frac{p}{a}\right]$ ， $r = p\%a$

$k \times a + r \equiv 0 \pmod{p}$ ，两边都除以 ar ，

$k \times r^{-1} + a^{-1} \equiv 0 \pmod{p}$

$a^{-1} \equiv -k \times r^{-1} \pmod{p}$

$inv(a) \equiv -[p/a] \times inv(p\%a) \pmod{p}$

然后以 $inv(1) = 1$ 作为边界

```
void getinv(LL mod)
{
        inv[1]=1;
        for(int i=2;i<mod;i++)
                inv[i]=(mod-mod/i)*inv[mod%i]%mod;
}
```

求解乘法逆元

求逆元详解参见博客：
https://www.cnblogs.com/daybreaking/p/9342060.html
https://blog.csdn.net/qq_37630072/article/details/98471030
https://blog.csdn.net/xiaoming_p/article/details/79644386

裴蜀定理

又称贝祖定理（Bézout's lemma）。是一个关于最大公约数的定理。

说明了对任何整数 a、b和它们的最大公约数 d ，有ax+by=m，当且仅当m是d的倍数时有解

ax+by=gcd(a,b)，关于未知数x和y的线性丢番图方程
裴蜀等式有解时必然有无穷多个整数解，每组解x、y都称为裴蜀数

a,b互质的充分必要条件是存在整数x,y使ax+by=1

证明略，自行百度

有了裴蜀定理，可以把同余式ax ≡ c (mod b)转换为ax+by=c这样的形式

小知识：充要条件

简单的高一数学知识，搬运自百度百科

A是条件，B是结论

A能推出B，条件能推出结论，满足充分性，A是B的充分不必要条件
B能推出A，结论能反推条件，满足必要性，A是B的必要不充分条件
A能推出B，B能推出A，则满足充分必要性，A、B互为充要条件

1. A="三角形等边"；B="三角形等角"。
2. A="某人触犯了法律"；B="应当依照刑法对他处以刑罚"。
3. A="付了足够的钱"；B="能买到商店里的东西"。

例1中A是B的充分必要条件;
例2中A是B的必要不充分条件;
（A触犯法律包含各种法，有刑法有民法；B已经确定是刑法。B属于A，所以A是B的必要不充分条件)
例3中A是B的必要不充分条件;
（A付够了钱 可以买的是车、房子等；但是B能买到商店里的东西一定是要付够钱)

扩展欧几里得算法

扩展欧几里得算法用于解决这样一个问题：
给定正整数a,b，求ax+by=gcd(a,b)的一组整数解

假如得到了一组解x0,y0，方程的通解可得：

x = x0 + (b/gcd)*t
y = y0 – (a/gcd)*t

通解推导过程：
ax + by = gcd(a,b) ①
ax0 + by0 = gcd(a,b) ②
① - ②:a(x-x0)+b(y-y0)=0
将两边同除以gcd(a,b),得 a/gcd(a,b)与b/gcd(a,b)互质,
记 A= a/gcd(a,b), B= b/gcd(a,b), 且A、B互质
肯定有A*(t*B)=B*(t*A)
A (x-x0) =B (y0-y)
所以
x-x0=b/gcd(a,b)*t;
y0-y=a/gcd(a,b)*t
所以
x=x0+b/gcd(a,b)*t
y=y0-a/gcd(a,b)*t

证明：https://www.cnblogs.com/caibingxu/p/10850664.html

扩展欧几里得算法

扩展欧几里得算法用于解决这样一个问题：
给定正整数a,b，求ax+by=gcd(a,b)的一组整数解

假如得到了一组解x0,y0，方程的通解可得：

x = x0 + (b/gcd)*t
y = y0 – (a/gcd)*t

$\xrightarrow{\text{A=a/gcd,B=b/gcd}}$

x = x0 +B*t
y = y0 – A*t

ax+by=c的整数解，只需将ax+by=gcd(a,b)的每个解乘上 c/gcd(a, b) 即可

我们不可能需要全部的解，一般题目会这么问： 求ax+by=c的最小整数解x0

```
x=x*c/gcd(a,b)
B=b/gcd(a,b)
x0=x%B
```

例题：青蛙的约会

扩展欧几里得算法—程序实现

ax+by=gcd(a,b)=bx’+a%b*y’

$$= bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor * b\right)y'$$

$$= ay' + b\left(x' - \left\lfloor \frac{a}{b} \right\rfloor * y'\right)$$

引用&

```
int exgcd(int a,int b,int &x,int &y)
{   if(b==0)
    {   x=1,y=0;
        return a;
    }
    int g=exgcd(b,a%b,y,x);
    y-=a/b*x;
    return g;
}
```

于是得到：
x=y’
y=x’-a/b*y’
x,y在同时缩小
当y=0时，a*1+b*0=a（**边界条件**）
这样就可以递归求解了

例题：同余方程

扩展欧几里得算法的应用

扩展欧几里得算法在求解不定方程解的时候，顺带也能把gcd求出来

（1）求解不定方程；
（2）求解模线性方程（线性同余方程）；
（3）求解模的逆元；

扩展欧几里得求逆元

根据裴蜀定理，ax ≡1(mod p)可以表示为

$$ax+py = 1$$

x是我们要求的逆元，那么使用exgcd求解即可

```
int getinv(int a, int p){  //exgcd求逆元
    int x,y,gcd;
    gcd = exgcd(a,p,x,y);
    if(gcd==1){
        x=(x%p+p)%p;//保证x为正数;
        return x;
    }
   else{
        cout<<"a,p不互质";
        return 0;
    }
}
```

Thanks

For Your Watching

FZOI

西大附中信息学竞赛

High School Affilinted to Southwest University