# 逆元与ax+by不定方程

2021年8月21日 0:32

- [x] CodeForces - 327C Magic Five

等比数列求和公式
分母是2^n-1时，利用费马小定理求逆元
a^(p-1) -=- 1mod(m)，当m为质数时
a*a^(p-2) = 1mod(p)
即a^(p-2)为a的逆元，减少复杂度

7C - Line

拓展欧几里得模板题

```
int exgcd(int a, int b, int &x, int &y){
//返回gcd(a,b) 并求出解(引用带回)
   if(b==0){
      x = 1, y = 0;
      return a;
   }
   int x1,y1,gcd;
   gcd = exgcd(b, a%b, x1, y1);
   x = y1, y = x1 - a/b*y1;
   return gcd;
}
```

什么是逆元?

如果b与m互质

★ 当n为质数的时候，快速幂求逆元

a / b ≡ a * x (mod n)
b * x ≡ 1 (mod n)
费马小定理：n为质数的时候
b ^ (n-1) ≡ 1 (mod n)
也就是 b * b ^ (n - 2) ≡ 1 (mod n)
1/b等价于b^(n-2)

★ 当n不是质数的时候，用拓展欧几里得求逆元

a有逆元的充要条件：a与p互质，有gcd(a,p) = 1

设a的逆元x，有a * x ≡ 1 (mod p)

即求解 ax + py = 1 的解 x

对右边的推广：gcd(a,m) == 1则只有唯一解

拓展欧几里得算法：(逆元求解线性同余方程)

给定a，b求一组x，y使得不定方程(丢番图方程)

ax+by = gcd(a,b)

特别的，当a与b互质的时候求出的x，y只要满足

x就是a的逆元

推理：

b = 0时，ax + by = a; 解得x = 1;

b !=0时，ax+by = gcd(a,b);

gcd(a,b) = gcd(b,a%b);

$$bx' + (a\%b)y' = gcd(b, a\%b)$$

$$bx' + (a - \lfloor a/b \rfloor * b)y' = gcd(b, a\%b)$$

$$ay' + b(x' - \lfloor a/b \rfloor * y') = gcd(b, a\%b) = gcd(a, b)$$

因此只要递归求出下一层的x，y代回式子就行

$$x = y', \quad y = x' - \lfloor a/b \rfloor * y'$$

实际代码中，将x',y'调换了位置也就是by' +(a%b)x' = d

此时 x = x',y = y'-(a/b)x'递归回原来位置

应用：

1.求解不定方程

2.求线性同余方程

3.求解模的逆元

拓展：

ax+by=c一般方程则有解表示c是d = gcd(a,b)的倍数

解决方法：用拓展欧几里得求出ax+by = d的解

然后将解乘以c/d，这是特解x，y

通解 = 特解+齐次解

ax+by = 0是齐次解（为什么用b/gcd(a,b)）

通：x' = x+k*b/d（这样可以保证b/d与a/d互质）

y' = y+k*a/d（这样的数字比较多）

应用：求解线性同余方程 ax ≡ b(mod m)

等价于求ax +my = b;

当b = 1，a与m互质时，x就是a的逆元