密码学作业001 学号 20131910023 姓名 金洋

（以Word文档提交,提交文档时在文件名和文档内部都写上学号和姓名,此后的各次作业按照此法处理）：

1. 用伪码表示非递归版本的欧几里得算法。

答：Algorithm GCD:

Input: 正整数a,b (a>b)

Output: gcd(a,b)

while (b != 0) {

r= a % b;

a = b;

b = r;

}

return a;

1. 用伪码表示递归版本的欧几里得算法。

答：Algorithm GCD:

Input: 正整数a,b (a>b)

Output: gcd(a,b)

If (b>0) then return GCD(b,a % b)

Else return a;

1. 用伪码表示非递归版本的扩展欧几里得算法。

答：Algorithm EXGCD:

Input 正整数a,b (a>b)

Output u, v, gcd(a,b)(满足au+bv=gcd(a,b))

u0=1; v0=0;

u1=0; v1=1;

u=0; v=1;

r=a%b;

q=(a-r)/b;

while(r)

{

u=u0-q\*u1; v=v0-q\*v1;

u0=u1; v0=v1;

u1=u; v1=v;

a=b; b=r; r=a%b;

q=(a-r)/b;

}

return u, v, b;

1. 用伪码表示递归版本的扩展欧几里得算法。

答：Algorithm EXGCD:

Input 正整数a,b (a>b)

Output u, v, gcd(a,b)(满足au+bv=gcd(a,b))

if (b==0) {

u=1;

v=0;

return a;

}

r= EXGCD(b,a%b);

t=u;

u=v;

v=t-a/b\*v;

return r;

1. 扩展欧几里得算法有何用途？

（1）求解不定方程pa+qb=c ①；

若c%gcd(a,b)=0,则有解，否则无解。

通过扩展欧几里得算法求得pa+qb=gcd(a,b)的解为，，

则①的一组解为，

则①的所有解

1. 求解模逆

当(a,b)=1时，则有au+bv=1

那么au=1 mod b，

u=a-1 mod b.

1. 欧几里得算法的时间复杂度是对数量级还是线性量级？

答：线性量级。

欧几里得算法复杂度是的常数倍，表示的是b的输入规模，故时间复杂度是线性量级。

1. 直接的幂算法或模幂算法的时间复杂度是什么量级？

答：假如计算的是，则直接计算需要进行A次，而A=，log2A是输入规模，故为指数量级。

1. 设a与b都为正整数，集合 {xa+yb|x,y都是整数}中的最小正整数记为d，证明：gcd(a,b)=d

证明：设gcd(a,b)=D，则D|a，D|b，故D|d①；

由欧几里得算法可知②

设；

令,则；

r也是a,b的线性组合，且r≥0

又d是集合中最小的正整数，故r=0，

从而d|a.同理可证d|b，

由②可得d|D

结合①得gcd(a,b)=d.

1. 若a,b,q,r皆为整数， a=bq+r, 证明gcd(a,b)= gcd(b,r)

证明：设d是a,b的公约数，则d|a,d|bq,∴d|a-bq，即d|r；

设e是b，r的公约数,则e|bq，e|r，∴e|bq+r，即e|a；

即a,b的公约数同时也是b,r的公约数，

b,r 的公约数同时也是a,b的公约数.

即a,b的公约数集合和b,r的公约数集合相等。

故gcd(a,b)= gcd(b,r)。