欧几里得算法

李奕萱 151160030

Lemma 2.13 : If j, k, q are positive integers such that

$k = qj + r$, then

$$\gcd(j, k) = \gcd(r, j)$$

```
gcd( j , k)            //Assume that j<k and that j and k are positive integers

(1) if ( k == j )

(2)         return j as gcd ,1 as x , 0 as y

(3) else

(4)         i = 0 ; k [ i ] = k ; j [ i ] = j;

(5) do              //find the value of the gcd

(6)         q [ i ] = k [ i ] / j [ i ]

(7)         r [ i ] = k [ i ] mod j [ i ]

(8)         k [ i + 1 ] = j [ i ]

(9)         j [ i + 1 ] = r [ i ]

(10)        i = i + 1

(11) while ( r [ i-1 ] == 0)

(12) gcd = j [ i -1]
```

invariance 1 : gcd (k [i-1] , j [i-1]) = gcd (k , j)

0<r[i]<j[i]<k[i]

invariance 1 :

奠基 :

第一次进入循环前, $i=1$, $k[i-1] = k[0] = k$, $j[i-1] = j[0] = j$, $r[i-1]=r[0]$有$gcd(k[i-1],j[i-1]) = gcd(k,j)$, 且$0<r[0]<j[0]<k[0]$满足条件。

保持:

假设第m次进入循环前:

$gcd(k[m-1],j[m-1]) = gcd(j[m-1],r[m-1]) = gcd(k,j)$ (1)

$k[m]=j[m-1], j[m]=r[m-1]$ (2)

$0<r[m-1]<j[m-1]<k[m-1]$ (3)

那么第m+1次进入循环前:

$gcd(k[m+1-1],j[m+1-1])=gcd(j[m-1],r[m-1])=gcd(k,j)$ (4)

$0<r[m]<j[m]=r[m-1]<j[m-1]=k[m]$ (5)

终止:

假设可以跳出循环，此时$r[i-1]=0$，则$k[i-1]=q[i-1]j[i-1]$, 易得到$gcd[k,j]=gcd(k[i-1],j[i-1])=j[i-1]$, 得证

```
//compute the x and y
(13) i=i-1
(14) y [ i ] = 0 , x [ i ] = 1
(15) while ( i > 0 )
(16)        i=i-1
(17)        y [ i ] = x [ i + 1 ]
(18)        x [ i ] = y [ i + 1 ] - q [ i ] * x [ i + 1 ]
(19) return gcd , x [0] as x, y [0] as y
```

invariance 2 : gcd (k , j) = y [i-m+1] k [i-m+1] + x [i-m+1] j[i-m+1]

invariance 2 :

奠基：

第一次进入循环前，m=1，y[i-1+1]=y[i]=0, x[i-1+1]=x[i]=1, 由之前的证明知，gcd=j[i]=x[i]j[i]+y[i]k[i]，满足。

保持：

假设第m次进入循环前，有

gcd=x[i-m+1]j[i-m+1]+y[i-m+1]k[i-m+1] (1)

那么第m+1次进入循环前，有

k[i-m]=q[i-m]*j[i-m]+r[i-m]

(2)

r[i-m]=j[i-m+1]

(3)

j[i-m]=k[i-m+1]

(4)

j[i-m+1]=k[i-m]-q[i-m]*j[i-m]

(5)

gcd=x[i-m+1]k[i-m]+(y[i-m+1]-q[i-m]*x[i-m])j[i-m] (6)

终止：

若可以跳出循环则以计算好了x[0]和y[0]的值，因此有x[0]k+y[0]j=gcd，得证

完全性证明

- 第一个循环：因为r[m]=j[m+1]>r[m+1]>0,所以随着循环次数的增加r[m]一直在减小且r[m]一直为非负整数，因此总会达到0跳出循环，终止。
- 第二个循环：因为i为有限正整数，故循环次数为有限次，因此一定会跳出循环，终止。

Thank you !