实验项目名称：扩展Euclid 算法 实验学时： 2

同组学生姓名： 无 实验地点： 4号科技楼1204

实验日期： 2023.9.13 实验成绩：

批改教师： 黄丹丹 批改时间： 2023.9.16

实验2 扩展Euclid 算法

一、基于OBE模式的实验目的和要求

1、掌握扩展欧几里德算法基本原理；

2、熟悉求解两数的最大公因子；

3、掌握求解模空间中的乘法逆元。

二、实验仪器和设备

Visual C/C++

三、实验过程

1、设计实现算法程序，Euclid 算法求a, b的最大公因子gcd (a, b)。

EUCLID (a, b)

1. X  a; Y  b；

2. if Y= 0 then return X= (a, b)；

3. if Y=1 then return Y= (a, b)；

4. R=X mod Y；

5. X=Y；

6. Y=R；

7. goto 2.

测试示例：当 a=3737, b=2701时，求出相应的gcd (a, b) = 37。

2、设计实现算法程序，Extended Euclid算法求b在mod a 下的乘法逆元，若逆元不存在程序需正确响应。

EXTENDED EUCLID (a, b)

1. (1, 0, a); (0, 1, b);

2. if , then return ；no inverse;

3. if , then return； ;

4.  ;

5. ;

6. ;

7.  ;

8. goto 2.

测试示例：

当n = 3337 = 47\*71，*ϕ*(*n*) = 46\*70 **=** 3220，e = 79时，求出*ϕ*(*n*) = 1019。

3、程序代码：

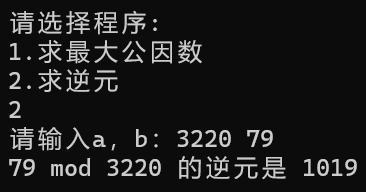
#include<stdio.h>void Euclid(){    int a,b;    printf("请输入a，b：");    scanf("%d %d",&a,&b);    int X,Y,R;    X=a,Y=b;    while(1){        if(Y==0){            printf("gcd( %d , %d ) = %d",a,b,X);            return;        }else if(Y==1){            printf("gcd( %d , %d ) = %d",a,b,Y);            return;        }        R=X%Y;        X=Y;        Y=R;        }}void ExtendedEuclid(){    int a,b;    printf("请输入a，b：");    scanf("%d %d",&a,&b);    int x1,x2,x3,y1,y2,y3;    int t1,t2,t3;    x1=1,x2=0,x3=a,y1=0,y2=1,y3=b;    while(1){        if(y3==0){            printf("%d mod %d 没有逆元",a,b);            return;        }else if(y3==1){            printf("%d mod %d 的逆元是 %d",b,a,y2);            return;        }        int q=x3/y3;        t1=x1-q\*y1,t2=x2-q\*y2,t3=x3-q\*y3;        x1=y1,x2=y2,x3=y3;        y1=t1,y2=t2,y3=t3;    }}int main(){    printf("请选择程序:\n1.求最大公因数\n2.求逆元\n");    int flag;    scanf("%d",&flag);    if(flag==1){        Euclid();    }else{        ExtendedEuclid();    }    return 0;}

四、实验结果与分析

测试结果截图与分析如下：

文本

描述已自动生成



五、基于OBE模式的学生自我评价与体会

本次实验主要学习了欧几里得算法，并在了解掌握之后通过C语言编程实现算法。先是辗转相除法求最大公因数。原理很简单，就是几个数换位取余直至为1或者为0。然后是欧几里得拓展算法求逆元。总体思路也是大差不差，是三个数换位取余，只不过会出现一种没有逆元的情况。通过本次实验我对欧几里得算法有了深刻的理解，并能进行运用。