#include<iostream>

#include<algorithm>

#include<math.h>

#define N 50

using namespace std;

int gcd(int a, int b)

{

if (a == 0 || b == 0)

return 0;

if (a == b)

return a;

if (a > b)

return gcd(a-b, b);

return gcd(a, b-a);

}

int main(void)

{

int p=0;

int q=0;

int i=0;

int k=0;

int inp=0;

int m=0;

int r=0;

int arr[N]={0};

int fn=0;

int n1=0;

int n2=0;

int t1=0;

int t2=0;

int t=0;

int n=0;

int c=0;

cout<<"\n enter the value of p :";

cin>>p;

cout<<"\n enter the value of q :";

cin>>q;

cout<<"\n enter the value of m:";

cin>>m;

n=p\*q;

fn=(p-1)\*(q-1);

for(i=2;i<fn;i++)

{

if(gcd(fn,i)==1)

{

arr[k]=i;

++k;

}

}

for(i=0;i<k;i++)

{

cout<<"\t"<<arr[i];

}

cout<<"\nselect the value of e :";

cin>>inp;

n1=fn;

n2=inp;

t1=0;

t2=1;

while(n1!=1 && n2!=0)

{

q=n1/n2;

r=n1%n2;

t=t1-(q\*t2);

cout<<"\n"<<q<<"\t"<<n1<<"\t"<n2<<"\t"<<r<<"\t"<<t1<<"\t"<<<<"\t"<<t;

n1=n2;

n2=r;

t1=t2;

t2=t;

}

cout<<"\nvalue of t1 :"<<t1;

cout<<"\nvalue of t2 :"<<t2;

cout<<"\nPrivate key is:"<<"["<<inp<<","<<n<<"]";

cout<<"\nPublic key is:"<<"["<<t1<<","<<n<<"]";

cout<<"\nthe value of C is :"<<fmod(pow(m,inp),n);

cout<<"\nThe value of M is :"<<fmod(pow(c,t1),n);

cout<<"\n"<<c;

cout<<"\n"<<n;

return 0;

}

OUTPUT

enter the value of p :7

 enter the value of q :13

 enter the value of m:10

        5       7       11      13      17      19      23      25      29      31      35      37      41      43      47      49  53       55      59      61      65      67      71

select the value of e :5

14      72      5       2       0       1       -14

2       5       2       1       1       -14     29

2       2       1       0       -14     29      -72

value of t1 :29

value of t2 :-72

Private key is:[5,91]

Public key is:[29,91]

the value of C is :82

The value of M is :10