Homework 3

Name: Weicheng Zhang JHID: wzhang81

A1

function [result]=Euclid(a,b)

d=gcd(a,b);

aj\_2=max(a,b);

aj\_1=min(a,b);

aj=mod(aj\_2,aj\_1);

qj\_1=floor(max(a,b)/min(a,b));

xj\_2=1; xj\_1=0;

yj\_2=0; yj\_1=1;

count=2;

while aj~=0

xj=xj\_2+qj\_1\*xj\_1;

yj=yj\_2+qj\_1\*yj\_1;

qj=floor(aj\_1/aj);

aj\_2=aj\_1;

aj\_1=aj;

aj=mod(aj\_2,aj\_1);

xj\_2=xj\_1; xj\_1=xj;

yj\_2=yj\_1; yj\_1=yj;

qj\_1=qj;

count=count+1;

end

xj\_1=power(-1,count-1)\*xj\_1;

yj\_1=power(-1,count)\*yj\_1;

result=[d,xj\_1,yj\_1];

end

Diary:

invmodn(2501,1002)

ans =

125

Euclid(105,5)

ans =

5 0 1

Euclid(543,47)

ans =

1 -9 104

Euclid(302,7)

ans =

1 1 -43

diary

A2

function q2(a,n)

if gcd(a,n)~=1

disp('No inverse of a')

end

result=Euclid(max(a,n),min(a,n))

q=-result(1,2)

x=mod(result(1,3),min(a,n))

end

q2(3,20)

result =

1 -1 7

q =

1

x =

1

invmodn(3,20)

ans =

7

q2(789,2574)

No inverse of a

q2(79,2574)

result =

1 -12 391

q =

12

x =

75

invmodn(79,2574)

ans =

391

mod(ans,79)

ans =

75

q2(43,257)

result =

1 -1 6

q =

1

x =

6

invmodn(43,257)

ans =

6

diary

A6

(a,b)

Diary

q6a

result =

Columns 1 through 18

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Columns 19 through 36

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Columns 37 through 54

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Columns 55 through 62

1 1 1 1 1 1 1 1

diary

q6b

result =

Columns 1 through 18

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Columns 19 through 20

1 1

diary

Code:

(a)

function q6a

result=[];

for x=0:61

product=abs(p(x));

result=[result,isprime(product)];

end

result

end

function res=p(x)

res=8\*x\*x-488\*x+7243;

end

(b)

function q6b

result=[];

for x=0:19

product=abs(p2(x));

result=[result,isprime(product)];

end

result

end

function res=p2(x)

res=power(x,4)+29\*power(x,2)+101;

end