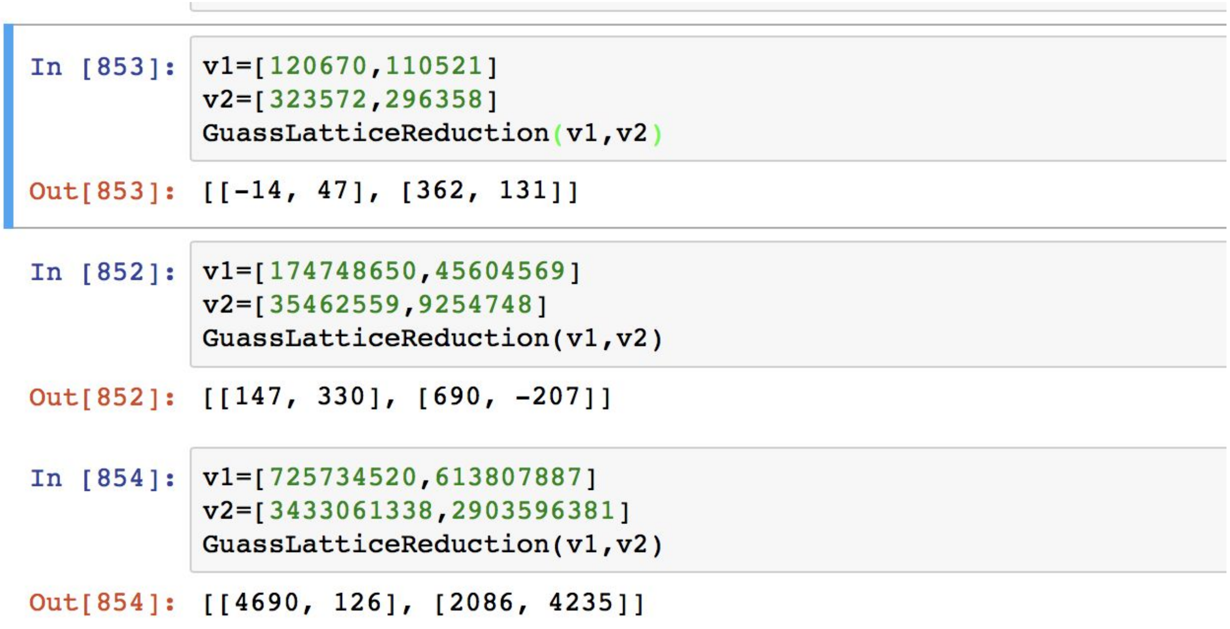
Cryptography HW 12
Yan Liang 112889478 2018/4/26

1.

```
def getLength(v):
    return v[0]*v[0]+v[1]*v[1]
def inner(u,v):
    return u[0]*v[0]+u[1]*v[1]
def switch(v1,v2):
    for i in range(0,len(v1)):
        temp=v2[i]
        v2[i]=v1[i]
        v1[i]=temp
def GuassLatticeReduction(v1,v2):
    m=1
    count=0
    while m!=0:
        count=count+1
        #print(count)
        len2=getLength(v2)
        len1=getLength(v1)
        #print(len2)
        #print(len1)
        if(len2<len1):
            switch(v1,v2);
        m=math.floor(inner(v1,v2)/getLength(v1));
        #print("m is "+str(m))
        v2[0]=v2[0]-m*v1[0]
        v2[1]=v2[1]-m*v1[1]
    return [v1,v2]
```



```
In [853]: v1=[120670,110521]
          v2=[323572,296358]
          GuassLatticeReduction(v1,v2)

Out[853]: [[-14, 47], [362, 131]]

In [852]: v1=[174748650,45604569]
          v2=[35462559,9254748]
          GuassLatticeReduction(v1,v2)

Out[852]: [[147, 330], [690, -207]]

In [854]: v1=[725734520,613807887]
          v2=[3433061338,2903596381]
          GuassLatticeReduction(v1,v2)

Out[854]: [[4690, 126], [2086, 4235]]
```

2.

```
sage: R29x.<x>=GF(29)[]
sage: r29a.<a>=QuotientRing(R29x,x^7-1)
sage: p=3
sage: q=29
sage: n=7
sage: r=-1+a^2-a^5+a^6
sage: h=3+14*a-4*a^2+13*a^3-6*a^4+2*a^5+7*a^6
sage: m=1+a-a^2-a^3-a^6
sage: c=p*h*r+m
sage: c
```

This is the cipherText

```
14*a^6 + 16*a^5 + 20*a^4 + 7*a^3 + 19*a^2 + 16*a + 23
```

Now we need to verify:

```
sage: a1=f*c
sage: a1
24*a^6 + 27*a^5 + 7*a^4 + a^3 + 26*a^2 + 3*a + 27
```

After center lift we got this:

```
def centerlift(q,l):
    for i in range(0,len(l)):
        if(l[i]<(-1*q/2)):
            l[i]=l[i]+q;
        elif(l[i]>(q/2)):
            l[i]=l[i]-q;
```

[-2, 3, -3, 1, 7, -2, -5]
So it should be:
So we need to verify in several steps, first we need to center lift f*c
Then we get this:
(-5)*a^6 + (-2)*a^5 + 7*a^4 + a^3 + (-3)*a^2 + 3*a + (-2)
the we need to consider this on a new ring which is R3b

```
R3x.<x>=GF(3)[]
sage: r3b.<b>=QuotientRing(R3x,x^7-1)
sage: liftresult=(-5)*b^6 + (-2)*b^5 + 7*b^4 + b^3 + (-3)*b^2 + 3*b + (-2)
sage: f3=1+b+b^2+b^4+b^5-b^6
sage: liftresult*f3
2*b^6 + 2*b^3 + 2*b^2 + b + 1
```

And center lift this for P then we get
-1*b^6-b^3-b^2+b+1
Which is the old message m.

(so basically two lift happened, when is when you do f*a you need to lift that with respect to q,
Then when you do f(q)*(f*a) you need to lift that result with respect to p.)