HW12

(Hoffstein book) 7.30 and 7.35

7.30. Alice and Bob decide to communicate using NTRUEncrypt with parameters (N, p, q) = (7, 3, 29). Alice’s public key is

h(x) = 3 + 14X − 4X^2 + 13X^3 − 6X^4 + 2X^5 + 7X^6.

Bob sends Alice the plaintext message m(x) = 1 + X – X^2 – X^3 – X^6 using the random element r(x) = −1 + X^2 – X^5 + X^6.

(a) What ciphertext does Bob send to Alice?

(b) Alice’s private key is f(x) = −1 + X – X^2 + X^4 + X^6 and F3(x) = 1 + X + X^2 + X^4 + X^5 – X^6. Check your answer in (a) by using f and F3 to decrypt the message.

(a)(b)

Code(Using Sagemath):

def center\_lifts(a\_x,q):

a\_x\_l=list(reversed(a\_x.list()))

a\_x\_l\_new=[]

for a\_x\_co in a\_x\_l:

a\_x\_co=a\_x\_co%q

if a\_x\_co>-q/2 and a\_x\_co<q/2:

a\_x\_l\_new.append(a\_x\_co)

else:

a\_x\_l\_new.append(a\_x\_co-q)

a\_x\_new=0

for i in range(len(a\_x\_l)):

a\_x\_new=a\_x\_l\_new[i]\*y^(6-i)+a\_x\_new

return a\_x\_new

N=7

p=3

q=29

Ro.<y>=ZZ[]

Rop.<yp>=Integers(p)[]

Roq.<yq>=Integers(q)[]

R.<x>=QuotientRing(Ro,y^N-1)

Rp.<xp>=QuotientRing(Rop,yp^N-1)

Rq.<xq>=QuotientRing(Roq,yq^N-1)

h\_x=3+14\*y-4\*y^2+13\*y^3-6\*y^4+2\*y^5+7\*y^6 #public key: in Rq

m\_x=1+y-y^2-y^3-y^6 #plaintext:in Rp

r\_x=-1+y^2-y^5+y^6 #random polynomial r

#Encryption

e\_x=Rq(p\*r\_x\*h\_x+m\_x) #ciphertext: mod q

print 'e\_x:',e\_x

#Decryption

f\_x=-1+y-y^2+y^4+y^6

a\_x=Rq(f\_x\*Ro(lift(e\_x))) #mod q

print 'f\_x\*e\_x: ',a\_x

a\_x=Ro(lift(a\_x))

a\_x\_cl=center\_lifts(a\_x,q) #center\_lifts modulo q

print 'a\_x\_cl:',a\_x\_cl #in R

F3\_x=1+y+y^2+y^4+y^5-y^6 #mod p

m\_x=Rp(F3\_x\*a\_x\_cl)

print 'F3\_x\*a\_x:',m\_x

m\_x=Ro(lift(m\_x))

print 'm\_x:',center\_lifts(m\_x,p)

print 'finished'

Result:

e\_x: 14\*xq^6 + 16\*xq^5 + 20\*xq^4 + 7\*xq^3 + 19\*xq^2 + 16\*xq + 23

f\_x\*e\_x: 24\*xq^6 + 27\*xq^5 + 7\*xq^4 + xq^3 + 26\*xq^2 + 3\*xq + 27

a\_x\_cl: -5\*y^6 - 2\*y^5 + 7\*y^4 + y^3 - 3\*y^2 + 3\*y - 2

F3\_x\*a\_x: 2\*xp^6 + 2\*xp^3 + 2\*xp^2 + xp + 1

m\_x: -y^6 - y^3 - y^2 + y + 1

finished

So the ciphertext is: 14\*x^6 + 16\*x^5 + 20\*x^4 + 7\*x^3 + 19\*x^2 + 16\*x + 23

And the message after decrypt is m\_x: -x^6 - x^3 - x^2 + x + 1, it is the same as the plaintext, so verified.

7.35. This exercise describes a variant of NTRUEncrypt that eliminates a step in the decryption algorithm at the cost of requiring slightly larger parameters. Suppose that the NTRUEncrypt private key polynomials f(x) and g(x) are chosen to satisfy f(x) = 1 + pf 0(x) ≡ 1 (mod p) and g(x) = pg0(x) ≡ 0 (mod p), and that NTRU encryption is changed to e(x) ≡ h(x) r(x) + m(x) (mod q). (The change is the omission of p before h(x).)

(a) Prove that if q is sufficiently large, then the following algorithm correctly decrypts the message:

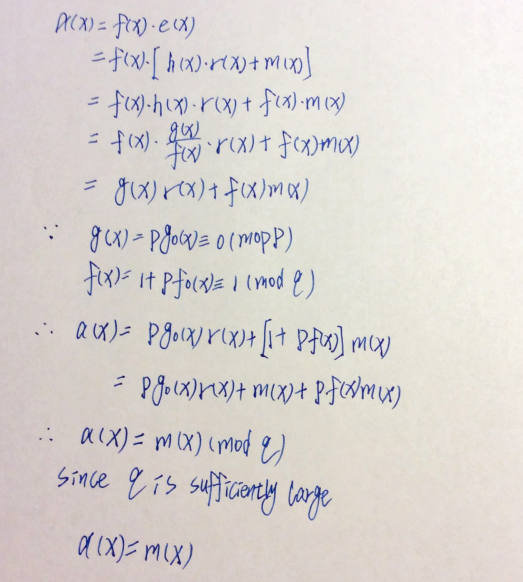
• Compute a(x) ≡ f(x) e(x) (mod q) and center-lift to an element of R.

• Compute a(x) (mod p). The result is m(x).

Note that this eliminates the necessity to multiply a(x) by f(x)−1 (mod p).

(a) Suppose that we choose f 0, g0 ∈ T (d, d), and that we also assume that m is ternary. Prove that decryption works provided q > 8dp + 2. (Hint. Mimic the proof of Proposition 7.48.)

（a）



(b)

