**Cryptography Assignment - 12**

**Pramod Aravind Byakod**

**Exercise 7.30**

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

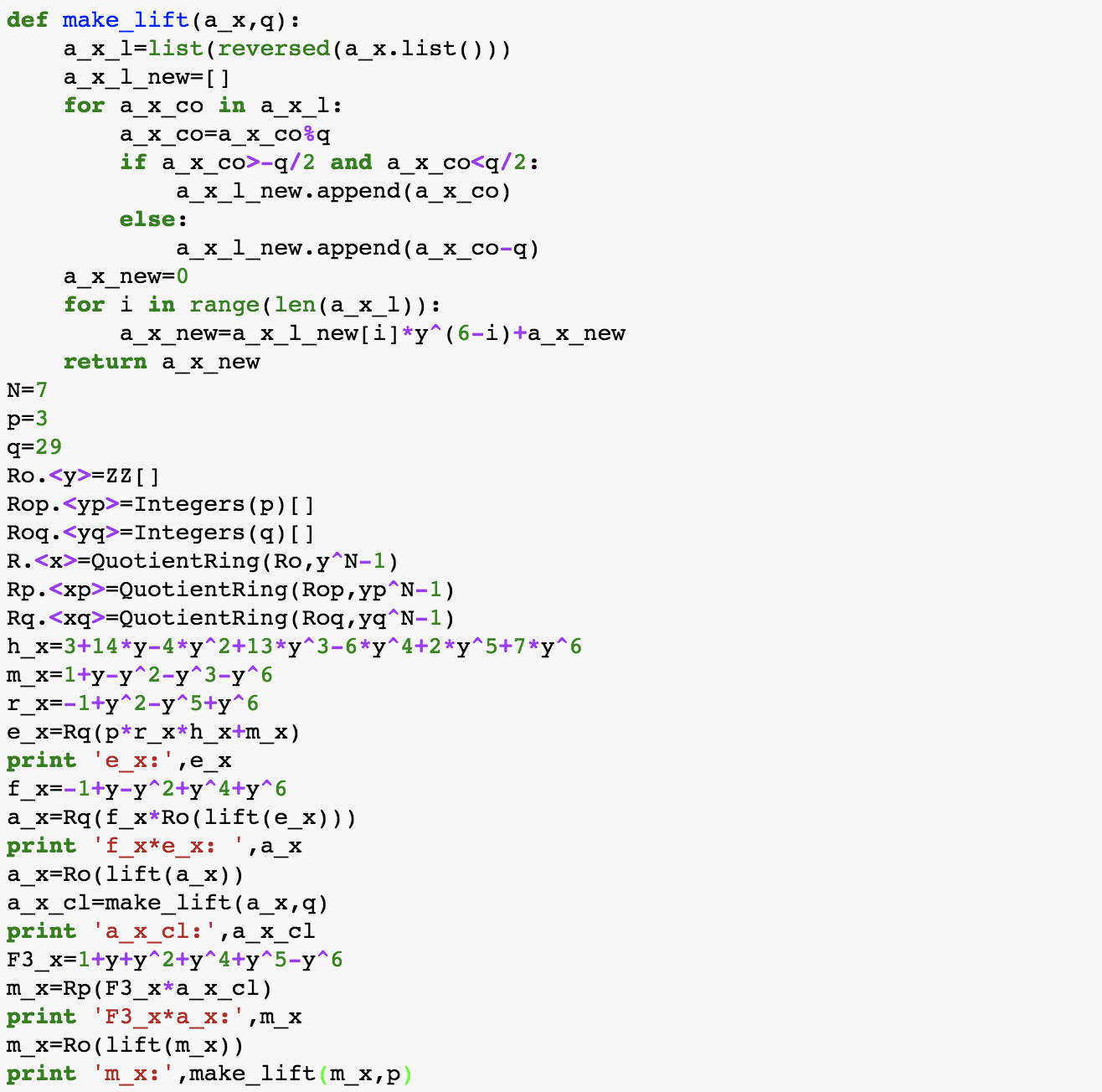
**h(x) = 3 + 14X − 4X^2 + 13X^3 − 6X^4 + 2X^5 + 7X^6.**

**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.**

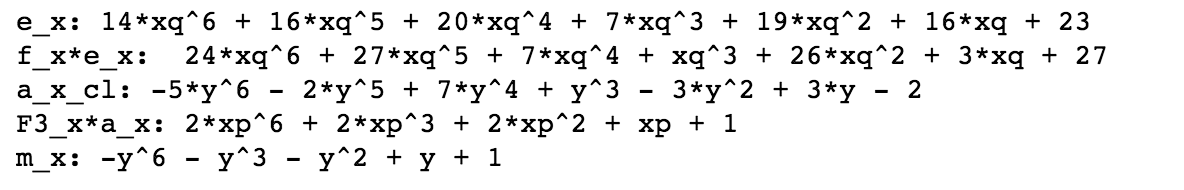
**(a) What ciphertext does Bob send to Alice?**

**(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.**

Solution:



Output:



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

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

**Exercise 7.45**

**Apply Gauss’s lattice reduction algorithm (Proposition 6.63) to solve SVP for**

**the following two-dimensional lattices having the indicated basis vectors. How many**

**steps do the algorithm take?**

**(a) v1 = (120670, 110521) and v2 = (323572, 296358).**

**(b) v1 = (174748650, 45604569) and v2 = (35462559, 9254748).**

**(c) v1 = (725734520, 613807887) and v2 = (3433061338, 2903596381).**

Solution:

Program:



Output:

(a)

Vector 1: (14, -47)

Vector 2: (-362, -131)

Number of steps taken: 6

(b)

Vector 1: (147, 330)

Vector 2: (690, -207)

Number of steps taken: 7

(c)

Vector 1: (4690, 126)

Vector 2: (2086, 4235)

Number of steps taken: 11