Assignment 4. Implementation and Cryptanalysis of NTRU

The deadline is Tuesday, November 15 midnight. You have to hand in a short description of the algorithms you implemented, the implementation code as a collection of subroutines (functions), and computational results.

NTRU public key generation, encryption and decryption. Let $(N, p, q) = (11, 3, 32)$ and $L_f = L(4, 3), L_g = L(3, 3), L_\phi = L(3, 3)$ be NTRU public parameters. The polynomials

$$f = -1 + X - X^2 + X^4 + X^6 + X^8 - X^{10}, \quad g = -1 + X + X^4 + X^5 - X^8 - X^{10}$$

is an NTRU private key.

1. Compute the inversions of f modulo $x^N - 1, p$ and modulo $x^N - 1, q$. Compute the NTRU public key. Let $m = -1 - X^3 + X^4 + X^8 + X^9 - X^{10}$ represent a message block and $\phi = 1 + X^2 - X^3 + X^4 - X^6 - X^7$. Compute the NTRU cipher-text c.
2. Let

   $$c = 26X^{10} + X^9 + 10X^8 + 28X^7 + 25X^6 + 24X^5 + 3X^4 + 20X^3 + 18X^2 + 28X + 9$$

   be an NTRU cipher-text. Compute the plain-text.

Multiple encryption of the same message. Let the parameters of NTRU (including the private key) be as above and the same message block m was encrypted with different $\phi_1, \phi_2, \phi_3, \phi_4$. The cipher-texts are

$$10X^{10} + 29X^9 + 20X^8 + 28X^7 + 5X^6 + 24X^5 + 5X^4 + 30X^3 + 24X + 15$$
$$29X^{10} + 2X^9 + 28X^8 + 23X^7 + 3X^6 + 3X^5 + 19X^4 + 27X^3 + 12X^2 + 24X + 20$$
$$29X^{10} + 19X^9 + 4X^8 + 7X^7 + 15X^6 + 30X^5 + 30X^4 + 4X^2 + 20X$$
$$X^{10} + 28X^9 + 6X^8 + 9X^7 + 29X^6 + 29X^5 + 11X^4 + 3X^3 + 20X^2 + 8X + 14$$

Find m without using regular decryption algorithm. Give details on how you did that.