(1) Use the Baby Step, Giant Step method to compute \( L_3(11) \) for \( p = 401 \). Show your work.

(2) Use the Pohlig-Hellman algorithm to compute \( L_2(28) \) for \( p = 37 \). Show your work.

(3) (Page 216, problem 12) Consider the following Baby Step, Giant Step attack on RSA, with public modulus \( n \). Eve knows a plaintext \( m \) and a ciphertext \( c \). She chooses \( N^2 \geq n \) and makes two lists: The first list is \( c^j \pmod{n} \) for \( 0 \leq j < N \). The second list is \( mc^{-Nk} \pmod{n} \) for \( 0 \leq k < N \).

(a) Why is there always a match between the two lists, and how does a match allow Eve to find the decryption exponent \( d \)?

(b) Your answer to the first part may be partly false. What Eve has really found is an exponent \( d \) such that \( c^d \equiv m \pmod{n} \). Give an example of a plaintext-ciphertext pair where the \( d \) you find is not the decryption exponent. (Usually \( d \) is very close to being the correct decryption exponent.)

(c) Why is this not a useful attack on RSA? (Hint: How long are the lists? Compare to trial division.)