Elliptic Curve Cryptography
Exercises

Exercise 1: If \( P = (-3, 9) \) and \( Q = (-2, 8) \) on the elliptic curve \( y^2 = x^3 - 36x \), find \( P + Q \) and \( 2P \). Find all points \( P \) such that \( 2P = O \).

Exercise 2: Find the quadratic residues in \( Z_7 \) and \( Z_{11} \), together with their square roots.

Exercise 3 Let \( F = Z_5 \). Find the orders of the elliptic curves \( y^2 = x^3 - 1 \) and \( y^2 = x^2 + x + 1 \).

Exercise 4 Let \( E_1 \) and \( E_2 \) be the elliptic curves \( y^2 = x^3 - x \) and \( y^2 = x^3 - x + 1 \), with \( F = Z_5 \). Show that both have order 8. Show that \( E_1 \) is not cyclic. Is \( E_2 \) cyclic?

Exercise 5 Let \( E \) be the elliptic curve \( y^2 = x^3 + x + 6 \) over \( F = Z_{11} \). Show that \(|E| = 13\). Taking \( P = (2, 7) \) as a generator, find an integer \( i \) such that \( iP = (8, 8) \) in \( E \).

References

1. G. A. Jones and D. Singerman, Complex Functions, CUP.