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 \( 2P = O \).

Solution If \( P = (-3, 9) \) and \( Q = (-2, 8) \) then \( \lambda = (9 - 8)/(-3 - (-2)) = -1 \), so \( x_3 = (-1)^2 - (-3) - (-2) = 6 \) and hence \( y_3 = 9 + (-1)(6 - (-3)) = 0 \). Thus \( R = (6, 0) \) and hence \( P + Q = (6, 0) \).

To find \( 2P \), the tangent at \( P \) has gradient \( \lambda = (3(-3)^2 - 36) / 2.9 = -1/2 \), so \( x_3 = (-1/2)^2 - 2.(-3) = 25/4 \) and \( y_3 = 9 + (-1/2)(25/4 - (-3)) = 35/8 \), giving \( 2P = (25/4, -35/8) \).

(Check: \((-35/8)^2 = (25/4)^3 - 36.(25/4)\), so this point is on the elliptic curve.)

In any elliptic curve \( y^2 = f(x) \), the points \( P \) with \( 2P = O \) are \( P = O \) and those \( P = (x, y) \) with \( y = 0 \). Putting \( y = 0 \) here gives \( x^3 - 36x = 0 \), with roots \( x = 0, \pm 6 \), so the points \( P \) with \( 2P = O \) are \( P = O = (\infty, \infty), (0, 0), (6, 0) \) and \((-6, 0)\).

Exercise 2: Find the quadratic residues in \( \mathbb{Z}_7 \) and \( \mathbb{Z}_{11} \), together with their square roots.

Solution In \( \mathbb{Z}_7 \) the quadratic residues are 1, 2 and 4, with square roots \( \pm 1, \pm 3 \) and \( \pm 2 \) respectively. In \( \mathbb{Z}_{11} \) the quadratic residues are 1, 3, 4, 5 and 9, with square roots \( \pm 1, \pm 5, \pm 2, \pm 4 \) and \( \pm 3 \) respectively.

Exercise 3 Let \( F = \mathbb{Z}_5 \). Find the orders of the elliptic curves \( y^2 = x^3 - 1 \) and \( y^2 = x^3 + x + 1 \).

Solution For \( x = 0, 1, 2, 3, 4 \) the values of \( x^3 - 1 \) in \( \mathbb{Z}_5 \) are 4, 0, 2, 1 and 3, with 2, 1, 0, 2 and 0 square roots \( y \), giving \( 2 + 1 + 0 + 2 + 0 + 1 = 6 \) points on the elliptic curve \( y^2 = x^3 - 1 \) (including \( O \)).

The corresponding values of \( x^3 + x + 1 \) in \( \mathbb{Z}_5 \) are 1, 3, 1, 1 and 4, with 2, 0, 2, 2 and 2 square
roots \( y \), giving \( 2 + 0 + 2 + 2 + 2 + 1 = 9 \) points on the elliptic curve \( y^2 = x^3 + x + 1 \).

**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 \( F = \mathbb{Z}_5 \). Show that both have order 8. Show that \( E_1 \) is not cyclic. Is \( E_2 \) cyclic?

**Solution** For \( x = 0, 1, 2, 3, 4 \) the values of \( x^3 - x \) in \( \mathbb{Z}_5 \) are 0, 0, 1, 4 and 0, with 1, 1, 2, 2 and 1 square roots \( y \), giving \( |E_1| = 1 + 1 + 2 + 2 + 1 + 1 = 8 \). There are three points \( P = (x, 0) \) of order 2 (with \( x = 0, 1, 4 \)), so according to the last theorem (with \( p = 2 \)) implies that \( E_1 \) is not cyclic.

For \( x = 0, 1, 2, 3, 4 \) the values of \( x^3 - x + 1 \) in \( \mathbb{Z}_5 \) are 1, 1, 2, 0 and 1, with 2, 2, 0, 1 and 2 square roots \( y \), giving \( |E_2| = 2 + 2 + 0 + 1 + 2 + 1 = 8 \). The only prime dividing \( |E_2| \) is \( p = 2 \), and there is exactly one point \( P = (x, 0) \) of order 2 in \( E_2 \) (namely \( (3, 0) \)), so Theorem 5 implies that \( E_2 \) is cyclic.

**Exercise 5** Let \( E \) be the elliptic curve \( y^2 = x^3 + x + 6 \) over \( F = \mathbb{Z}_{11} \). Show that \( |E| = 13 \).

Taking \( P = (2, 7) \) as a generator, find an integer \( i \) such that \( iP = (8, 8) \) in \( E \).

**Solution** The quadratic residues in \( \mathbb{Z}_{11} \) are 1, 3, 4, 5, 9. For \( x = 0, 1, \ldots, 10 \) the values of \( x^3 + x + 6 \) in \( \mathbb{Z}_{11} \) are 6, 8, 5, 3, 8, 4, 8, 4, 9, 7, 4, with 0, 0, 2, 2, 0, 2, 0, 2, 2, 0, 2 square roots \( y \), giving \( 0 + 0 + 2 + 2 + 0 + 2 + 0 + 2 + 0 + 2 + 1 = 13 \) points on \( E \) (including \( O \)).

By computing \( 2P = (5, 2) \), \( 3P = (8, 3) \), \ldots in turn, one would eventually find that \( 10P = (8, 8) \).

**References**

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