

The University of Oxford

MSc (Mathematics and Foundations of Computer Science)

## Elliptic Curves

Michaelmas Term 2025

*The steps of (each) mini project are for your guidance; if you wish to take an alternative route to the desired goal, you are free to do so. But, if you follow the suggested route and find yourself unable to carry out any particular step, you may simply assume it so that you can continue with the mini project, but should make this assumption clear in your presentation.*

*The different parts of this miniproject are largely independent, and are likely to be of quite different lengths. Give clear and precise references to any results you use from the lecture notes, example sheets, books, on-line resources, or elsewhere, and justify all answers. Please include your own examples in addition to those gathered from other sources.*

*The following question parts test understanding of the course material without an open-ended component: 1(i),(ii); 3(i),(ii); 5(i).*

*Good answers to these parts will be sufficient to achieve a passing mark.*

### Question 1.

- (i) Find the torsion group over  $\mathbb{Q}$  of the elliptic curve

$$Y^2 = X(X + 1)(X - 3).$$

- (ii) Let  $\mathcal{E}$  be the elliptic curve  $Y^2 = X^3 + 9$ . Show that  $\mathcal{E}(\mathbb{Q})$  has a point of order 3 and a point of infinite order.
- (iii) Find other elliptic curves  $\mathcal{E}$  for which  $\mathcal{E}(\mathbb{Q})$  has a point of order  $N > 1$  and a point of infinite order.

**Question 2.** For any elliptic curve  $\mathcal{E}$  and any  $(s, t) \in \mathcal{E}(\mathbb{Q})$  with  $s, t \in \mathbb{Q}$  and  $s = \frac{c}{d}$ ,  $\gcd(c, d) = 1$ , let the height function  $h_x(s, t)$  be defined, as usual, by:

$$h_x((s, t)) = \log \max(|c|, |d|),$$

and define  $h_x(\mathbf{o}) = 0$ .

(i) Let:

$$\mathcal{E}_B : Y^2 = X^3 + B,$$

where  $B \in \mathbb{Z}$  and  $B \neq 0$ , be an elliptic curve. Find a constant  $C_1$ , which depends only on  $B \in \mathbb{Z}$  and  $Q \in \mathcal{E}_B(\mathbb{Q})$ , such that  $h_x(P + Q) \leq 2h_x(P) + C_1$  for all  $P \in \mathcal{E}_B(\mathbb{Q})$ . Find a constant  $C_2$ , which depends only on  $B \in \mathbb{Z}$ , such that  $h_x(2P) \geq 4h_x(P) - C_2$  for all  $P \in \mathcal{E}_B(\mathbb{Q})$ .

(ii) Find examples of elliptic curves of the form  $Y^2 = X^3 + B$  of rank  $> 0$ , where you are able to find generators for  $\mathcal{E}(\mathbb{Q})$ .

**Question 3.**

- (i) Find the rank of the elliptic curve  $Y^2 = X(X^2 + 3X + 7)$ .
- (ii) What can you say about the rank of the elliptic curve  $Y^2 = X(X^2 - p)$ , when  $p$  is prime and  $p \equiv 3 \pmod{8}$ ?
- (iii) Find infinite families of elliptic curves where you are able to determine the rank. Find other infinite families of elliptic curves where you are able to show the rank is at most 1.

**Question 4.**

- (i) Let  $\mathcal{C} : Y^2 = X(X + \lambda_1)(X + \lambda_2)$ , where  $\lambda_1, \lambda_2 \in \mathbb{Q}^*$  and  $\lambda_1 \neq \lambda_2$ . Determine  $\mu_1, \mu_2 \in \mathbb{Q}(\sqrt{\lambda_1}, \sqrt{\lambda_2})$  such that there is a 2-isogeny defined over  $\mathbb{Q}$  from  $\mathcal{C}$  to the curve  $\mathcal{D} : Y^2 = X(X - \mu_1)(X - \mu_2)$ . Suppose that  $(0, 0) \in 2\mathcal{C}(\mathbb{Q})$ ; show that  $\lambda_1, \lambda_2, \mu_1, \mu_2 \in (\mathbb{Q}^*)^2$ .
- (ii) Let  $\mathcal{E}$  be any elliptic curve, defined over  $\mathbb{Q}$ . Find the best bound you can on the possible number of  $\mathbb{Q}$ -rational points of order 4 on  $\mathcal{E}$ .

**Question 5.**

- (i) Construct several examples where the elliptic curve method is used to factorise 5-digit numbers, using small multiples of a point on an elliptic curve.
- (ii) Try to construct instances where the same 5-digit number can be factorised using different elliptic curves.