Loughborough University

ELLIPTIC CURVES
(22MAC260)

Semester 2 22/23 In-Person Exam Paper

This examination is to take place in-person at a central University venue under exam conditions. The standard length of time for this paper is **2 hours**.

You will not be able to leave the exam hall for the first 30 or final 15 minutes of your exam. Your invigilator will collect your exam paper when you have finished.

Help during the exam

Invigilators are not able to answer queries about the content of your exam paper. Instead, please make a note of your query in your answer script to be considered during the marking process.

If you feel unwell, please raise your hand so that an invigilator can assist you.

You may use a calculator for this exam. It must comply with the University's Calculator Policy for In-Person exams, in particular that it must not be able to transmit or receive information (e.g. mobile devices and smart watches are not allowed).

To obtain full marks you must justify your answers appropriately. It is not sufficient simply to state results.

Answer **ALL** questions.

A formula sheet is provided on the final page of this exam paper.

---

1. (a) Define the **order** of a point P on an elliptic curve E. [5]

   (b) Consider the elliptic curve E and the two points P and Q on E defined by

$$E : y^2 = x^3 + x^2 + 7x$$
$$P = (1, 3)$$
$$Q = (7, 21).$$

   (Note that E is **not** in Weierstrass form.)

   (i) Compute the points $2P$ and $2Q$. [15]

   (ii) Using the previous part, find the order of P and the order of Q. [5]

2. (a) State Mordell's Theorem. [5]

   (b) For the elliptic curve E curve defined by

$$E : y^2 = x^3 - 6x + 6$$

   use the Nagell–Lutz Theorem to compute the torsion subgroup $T \subset E(\mathbb{Q})$. [15]

   (c) For a natural number n, let E_n be the elliptic curve defined by

$$E_n : y^2 = x^3 - nx + n.$$

   Show that if n is even, the group of rational points $E_n(\mathbb{Q})$ is infinite. [5]

3. (a) Let E be the elliptic curve defined by

$$E : y^2 = x^3 - 8x - 3.$$

   (i) Find all odd primes p for which the curve $\overline{E}$ obtained by reducing E modulo p is **not** an elliptic curve. [5]

   (ii) By reducing modulo appropriate primes, compute the torsion subgroup $T \subset E(\mathbb{Q})$. [15]

   (b) Let p a prime number of the form $5k + 2$ where k is a natural number. Let E be the elliptic curve defined by

$$E : y^2 = x^3 + p.$$

   Show that the torsion subgroup $T \subset E(\mathbb{Q})$ has order $|T| \leq 3$. [5]

4. (a) For a lattice L in the complex plane and a natural number $k \geq 3$, define the **Eisenstein series of weight** k associated to L. [5]

   (b) Let L be the lattice spanned by the two complex numbers

$$\omega_1 = -\frac{8}{5} - \frac{6}{5}\,i$$
$$\omega_2 = 1 + i$$

   Find a complex number τ in the region

$$\mathcal{F} := \left\{ z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0,\ |\,\mathrm{Re}(z)| \leq \frac{1}{2},\ |z| \geq 1 \right\}$$

   such that L is similar to the lattice

$$\mathbb{Z} \oplus \mathbb{Z} \cdot \tau.$$ [10]

   (c) Consider the family of elliptic curves defined by

$$E_t \ : \ y^2 = x^3 - 3x^2 + (3+t)x - 3.$$

   where $t \in \mathbb{C}$ is a complex number.

   (i) Transform E_t to Weierstrass form, and hence compute the j-invariant $j(E_t)$. [5]

   (ii) If E_L is the elliptic curve associated to the lattice L in part (b) above, find a value of $t \in \mathbb{C}$ for which E_t is an elliptic curve such that $E_t \simeq E_L$. (You may use without proof any results from the module, provided you state them clearly.) [5]

Formula Sheet

- Weierstrass form of an elliptic curve:

$$E : \ y^2 = x^3 + ax + b$$

- Discriminant of a curve E in Weierstrass form:

$$\Delta = -4a^3 - 27b^2$$

- j-invariant of a curve E in Weierstrass form:

$$j(E) = 1728 \cdot \frac{4a^3}{\Delta}$$

- Point addition formulae: given a curve E in Weierstrass form,
  - given points P, Q on E with coordinates

$$P = (x_0, y_0)$$
$$Q = (x_0, -y_0)$$

    then $P \oplus Q = O$.
  - given points P, Q on E with coordinates

$$P = (x_0, y_0)$$
$$Q = (x_1, y_1) \quad \text{where } x_0 \neq x_1$$

    let

$$m = \frac{y_1 - y_0}{x_1 - x_0}$$
$$x_2 = m^2 - x_0 - x_1$$
$$y_2 = y_0 + m(x_2 - x_0);$$

    then $P \oplus Q = (x_2, -y_2)$.
  - given a point P on E with coordinates

$$P = (x_0, y_0) \quad \text{where } y_0 \neq 0;$$

    let

$$m' = \frac{3x_0^2 + a}{2y_0}$$
$$x_1 = (m')^2 - 2x_0$$
$$y_1 = y_0 + m'(x_1 - x_0);$$

    then $2P = P \oplus P = (x_1, -y_1)$.