Loughborough University

ELLIPTIC CURVES
(21MAC260)

Semester 2 2022 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.

---

1. (a) Consider the elliptic curve E and the point $P \in E$ defined by

$$E : \ y^2 = x^3 - x^2 + \frac{1}{4}$$
$$P = \left(0, \frac{1}{2}\right).$$

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

(i) Compute the points $2P$ and $3P$. [10]

(ii) What is the order of P? You must justify your answer. [5]

(b) Consider the elliptic curves E_1 and E_2 defined by

$$E_1 : \ y^2 = x^3 - x$$
$$E_2 : \ y^2 = x^3 - 2x.$$

(i) Show that E_1 and E_2 are isomorphic over $\mathbb{C}$. [5]

(ii) Are the groups of rational points $E_1(\mathbb{Q})$ and $E_2(\mathbb{Q})$ isomorphic? You must justify your answer. [5]

2. (a) State the Integrality Theorem and the Nagell–Lutz Theorem. [5]

(b) For the elliptic curve E defined by

$$E : \ y^2 = x^3 - 11x - 6$$

use the Nagell-Lutz Theorem to show that the torsion subgroup $T \subset E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2$. [20]

continued. . .

3. Let E be the elliptic curve defined by

$$E \,:\, y^2 = x^3 + 16$$

(a) Find the order of the point $P = (0, 4)$ on E. [5]

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

(c) By reducing modulo one or more appropriate primes, and using the result of Part (a), compute the torsion subgroup $T \subset E(\mathbb{Q})$. [15]

4. (a) Define the **Weierstrass $\wp$-function** associated to a lattice $L \subset \mathbb{C}$. [5]

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

$$\omega_1 = 1 + i$$
$$\omega_2 = \frac{\sqrt{3}-1}{6} + \frac{\sqrt{3}+1}{6}\, i.$$

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) Let $c \in \mathbb{Z}_{>0}$ be a positive integer, and consider the elliptic curve E defined by

$$E \,:\, y^2 = x^3 + c.$$

If $N(c)$ is the positive real number defined by the formula

$$N(c) = \ln(3) + \frac{2}{3}\ln(c)$$

show that the set of points $P \in E(\mathbb{Q})$ whose height $h_x(P)$ satisfies the inequality

$$h_x(P) > N(c)$$

is either empty, or contains infinitely many elements. (You may use any properties of the function h_x given in lectures, provided you state them clearly.) [10]

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