Loughborough University

ELLIPTIC CURVES
(20MAC260)

Summer 2021 | 2 hours

You may use any calculator (not just those on the University's approved list).
To obtain full marks you must justify your answers appropriately. It is not sufficient simply to state results.
Answer **ALL** questions.

---

1. (a) For the elliptic curve E defined by the equation

$$y^2 = x^3 - 3x^2 + 3x$$

calculate the order of the point $P = (3, 3)$ on E. [15]

(b) Consider the family of curves defined by

$$E_t: \quad y^2 = tx^3 - 3x + 2t$$

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

Find all values of t for which E_t is not an elliptic curve. [10]

2. Let E be the elliptic curve defined by the equation

$$y^2 = x^3 - 11x + 10.$$

(a) Use the Nagell-Lutz Theorem to compute the torsion subgroup $T \subset E(\mathbf{Q})$. [20]

(b) Is the group $E(\mathbb{Q})$ finite or infinite? You must justify your answer. [5]

3. Let E be the elliptic curve defined by the equation

$$y^2 = x^3 - 12x.$$

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

   (b) Using reduction modulo suitable primes, compute the torsion subgroup $T \subset E(\mathbb{Q})$. [20]

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

$$y^2 = x^3 + x - 1.$$

   (i) Find a point $P \in E(\mathbb{Q})$ such that

$$h_x(P) > 3$$

   where $h_x : E(\mathbb{Q}) \to \mathbb{R}$ denotes the height function. [10]

   (ii) Does there exist a natural number M such that

$$h_x(Q) \leq M$$

   for all points $Q \in E(\mathbb{Q})$? You must justify your answer. [5]

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

$$\omega_1 = \sqrt{2}\,i$$
$$\omega_2 = -\frac{1}{2} + \left(\frac{1}{2} - \sqrt{2}\right) i$$

   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]