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]

Solution: (Similar examples seen)
To compute $2P = P \oplus P$, the first step is to compute $P * P$. The tangent line to E at P has slope

$$\frac{dy}{dx}(P) = \frac{3x^2 - 2x}{2y}(P)$$
$$= 0$$

so its equation is $y = \frac{1}{2}$.
Substituting this into the equation of E we get

$$\left(\frac{1}{2}\right)^2 = x^3 - x^2 + \frac{1}{4}$$

which simplifies to

$$x^3 - x^2 = 0.$$

This has a double root at $x = 0$ since the line is tangent to the curve E at P. The x-coordinate of $P * P$ is given by the third root $x = 1$: so we have

$$P * P = \left(1, \frac{1}{2}\right)$$

hence

$$2P = \left(1, -\frac{1}{2}\right).$$

Next we compute $3P = 2P \oplus P$; again we start by computing $2P * P$. The line joining P to $2P$ has slope

$$\frac{-\frac{1}{2} - \frac{1}{2}}{1 - 0} = -1$$

so its equation is $y = -x + \frac{1}{2}$. Substituting this into the equation of E we get

$$\left(-x + \frac{1}{2}\right)^2 = x^3 - x^2 + \frac{1}{4}$$

which simplifies to

$$x^3 - 2x^2 + x = 0$$

This has a root at $x = 0$ corresponding to P, and a double root at $x = 1$ corresponding to $2P$. This shows that $P * 2P = 2P$, and hence

$$\begin{aligned} 3P &= -(P * 2P) = -2P \\ &= \left(1, \frac{1}{2}\right). \end{aligned}$$

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

Solution: (Similar examples seen) We have seen in the previous part that $3P = -2P$ and hence $5P = O$. This shows that the order of P divides 5. Since $P \neq O$, the order cannot be 1, so it must equal 5.

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

$$\begin{aligned} E_1 &: \ y^2 = x^3 - x \\ E_2 &: \ y^2 = x^3 - 2x. \end{aligned}$$

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

Solution: (Similar examples seen)
One solution is to compute the j-invariants of the 2 curves: we have

$$\begin{aligned} j(E_1) &= 1728\frac{4(-1)^3}{-4(-1)^3 - 27(0)^2} \\ &= -1728; \\ j(E_2) &= 1728\frac{4(-2)^3}{-4(-2)^3 - 27(0)^2} \\ &= -1728. \end{aligned}$$

From lectures we know that two curves with equal j-invariant are isomorphic over $\mathbb{C}$.

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

Solution: (Unseen) No. We can write the equation of E_1 as

$$y^2 = x(x-1)(x+1)$$

which shows that $E_1(\mathbb{Q})$ contains 3 points of order 2:

$$(-1, 0), (0, 0), (1, 0).$$

On the other hand, the equation of E_2 is

$$y^2 = x(x^2 - 2)$$

Since the cubic on the right has only 1 rational root, the group $E_2(\mathbb{Q})$ contains only 1 element of order 2, namely the point $(0, 0)$.

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

Solution: (Bookwork)

Integrality Theorem: Let E be an elliptic curve given by an equation

$$y^2 = x^3 + ax + b \quad \text{where } a, b \in \mathbb{Z}.$$

If $(x, y) \in E(\mathbb{Q})$ is a point of finite order, then $x, y \in \mathbb{Z}$.

Nagell–Lutz Theorem: Let E be an elliptic curve given by an equation

$$y^2 = x^3 + ax + b \quad \text{where } a, b \in \mathbb{Z}.$$

Let $\Delta = -4a^3 - 27b^2$ denote the discriminant of E. Let $(x, y) \in E(\mathbb{Q})$ be a point of finite order (so $x, y \in \mathbb{Z}$). Then either $y = 0$ or $y^2 \mid \Delta$.

(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]

Solution: (Similar examples seen)

We start by finding and factoring the discriminant. We have

$$\begin{aligned} \Delta &= -4 \cdot (-11)^3 - 27 \cdot 6^2 = 4352 \\ &= 2^8 \cdot 17. \end{aligned}$$

Nagell–Lutz tells us that if $(x, y) \in T$, then $y = 0$ or $y^2 \mid \Delta$. In the latter case the possibilities are

$$|y| = 1,\ 2,\ 4,\ 8,\ 16.$$

We look for candidate torsion points by computing an appropriate range of values of the cubic $f(x) = x^3 - 11x - 6$. Note that

$$\frac{df}{dx} = 3x^2 - 11$$

so for $|x| > \sqrt{11/3}$ the cubic is monotonic increasing.

We compute that $f(-3) = 0$; since $|-3| > \sqrt{11/3}$ the monotonic property above says that $f(x) < 0$ for $x \leq -4$, and so no x-value in this range can give us a point on the curve. Also we compute $f(7) = 260 > 16^2$, so again the monotonic propery says that $f(x) > 256$ for $x \geq 7$, and so for x in this range we do not get any point on our curve with one of the y-values listed above.

So we can restrict to computing values of $f(x)$ for integers x in the range $-3 \leq x \leq 6$. We get

$$0,\ 8,\ 4,\ -6,\ -16,\ -20,\ -12,\ 14,\ 64,\ 144.$$

Among these, the values which are squares of y-values listed above are the following:

$$\begin{aligned} f(-3) &= 0 = 0^2 \\ f(-1) &= 4 = (\pm 2)^2 \\ f(5) &= 64 = (\pm 8)^2. \end{aligned}$$

So, along with the identity O, we have candidate torsion points

$$(-3, 0),\ (-1, \pm 2), (5, \pm 8).$$

The point $P_1 = (-3, 0)$ has y-coordinate equal to 0 and so it is a point of order 2. We must show the other points are not actually torsion points.

For the point $P_2 = (-1, 2)$ we compute that

$$\pm 2P_2 = (6, \pm 12)$$

Since 12^2 does not divide Δ Nagell–Lutz says that $2P_2$ is not a torsion point, hence P_2 is not a torsion point and neither is $-P_2 = (-1, -2)$.

For the point $P_3 = (5, 8)$ we compute that

$$2P_3 = (6, -12)$$

and so again $\pm P_3$ are not torsion points.

We have shown that the only actual torsion points are the identity O and the point $(-3, 0)$, of order 2. Hence

$$T = \{O, (-3, 0)\} \cong \mathbb{Z}_2.$$

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]

Solution: (Similar examples seen)

Computing using the formulas for addition in Weierstrass form, we find

$$\begin{aligned} x(2P) &= \left(\frac{3x^2}{2y}\right)^2_{|P} - 2x(P) \\ &= 0 \end{aligned}$$

So $2P = \pm P$, but since $P \neq O$ we cannot have $2P = P$. Therefore we conclude that $2P = -P$, hence $3P = 0$. So the order of P must divide 3; since P is not the identity, it does not have order 1, so it must have order 3.

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

Solution: (Similar examples seen)

We compute

$$\begin{aligned} \Delta &= -27 \cdot 16^2 \\ &= -2^8 \cdot 3^3. \end{aligned}$$

So the only odd prime p for which $\overline{E}$ is not an elliptic curve is $p = 3$.

(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]

Solution: (Similar examples seen)

By Part (b), we know that the reduction $\overline{E}$ of E modulo p is an elliptic curve for any odd prime $p \neq 3$. The Torsion Embedding Theorem then says in particular that $|T|$ divides $|\overline{E}(\mathbb{F}_p)|$.

- First we reduce mod 5. We get the elliptic curve $\overline{E}$ given by the equation

$$\overline{E} : \ y^2 = x^3 + 1.$$

Tabulating the $\mathbb{F}_5$-points on this curve we get

x	0	1	2	3	4
x^3+1	1	2	4	3	0
y	± 1	$-$	± 2	$-$	0

Here we use the list of squares in $\mathbb{F}_5$:

$$0^2 = 0,\ 1^2 = 4^2 = 1,\ 2^2 = 3^2 = 4.$$

So

$$\overline{E}(\mathbb{F}_5) = \{O, (0, \pm 1), (2, \pm 2), (4, 0)\}\,.$$

Therefore $|\overline{E}(\mathbb{F}_5)| = 6$, so by the Torsion Embedding Theorem we have $|T| \mid 6$.

- Next we reduce E mod 7. This gives the curve $\overline{E}$ defined by the equation

$$\overline{E}\ :\ y^2 = x^3 + 2.$$

Tabulating the $\mathbb{F}_7$-points on this curve we get

x	0	1	2	3	4	5	6
x^3+2	2	3	3	1	3	1	1
y	± 3	$-$	$-$	± 1	$-$	± 1	± 1

Here we use the list of squares in $\mathbb{F}_7$:

$$0^2 = 0,\ 1^2 = 6^2 = 1,\ 2^2 = 5^2 = 4,\ 3^2 = 4^2 = 2.$$

So

$$\overline{E}(\mathbb{F}_7) = \{O, (0, \pm 3), (3, \pm 1), (5, \pm 1), (6, \pm 1)\}\,.$$

Therefore $|\overline{E}(\mathbb{F}_5)| = 9$, so by the Torsion Embedding Theorem we have $|T| \mid 9$.

Putting these results together, we get $|T| \mid \gcd(6, 9) = 3$. On the other hand, in Part (a) we saw that the point $P = (0, 4)$ has order 3, hence we have $|T| > 1$. Therefore $|T| = 3$ and

$$T = \langle P \rangle = \{O, P, -P\} \cong \mathbb{Z}_3.$$

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

Solution: (Bookwork) The Weierstrass $\wp$-function associated to the lattice L is defined as

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\omega \in L,\ \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

continued. . .

(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

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

Solution: (Similar examples seen) First we have that L is similar to the lattice $\mathbb{Z} \oplus \mathbb{Z}\omega$ where

$$\begin{aligned}\omega &= \frac{\omega_2}{\omega_1} \\ &= \frac{1}{2}(1-i)\left(\frac{\sqrt{3}-1}{6} + \frac{\sqrt{3}+1}{6}\, i\right) \\ &= \frac{\sqrt{3}}{6} + \frac{1}{6}\, i \\ &= \frac{1}{3}\exp(\pi\, i/6).\end{aligned}$$

Since $|\omega| = 1/3$ we apply the transformation

$$S\colon \tau \mapsto -\frac{1}{\tau}$$

to get

$$\begin{aligned}S\omega &= -3\exp(-\pi\, i/6) \\ &= -3\cos(\pi\, i/6) + 3\sin(\pi\, i/6) \\ &= \frac{-3\sqrt{3}}{2} + \frac{3}{2}\, i.\end{aligned}$$

The real part of this number is $\mathrm{Re}(S\omega) = \frac{-3\sqrt{3}}{2} \approx -2.598$, so we must apply the map

$$T\colon \tau \mapsto \tau + 1$$

3 times: this gives

$$T^3 S\omega = 3 - \frac{3\sqrt{3}}{2} + \frac{3}{2}\, i.$$

continued. . .

Now the absolute value of the real part is $|\operatorname{Re}(S\omega)| \approx 0.401$, and the absolute value of the number is

$$\begin{aligned}\left|T^3 S\omega\right| &= \sqrt{\left(3 - \frac{3\sqrt{3}}{2}\right)^2 + \left(\frac{3}{2}\right)^2} \\ &> \frac{3}{2} > 1\end{aligned}$$

so $T^3 S\omega \in \mathcal{F}$.

So the required number τ is

$$\begin{aligned}\tau &= T^3 S\omega \\ &= 3 - \frac{3\sqrt{3}}{2} + \frac{3}{2}\,i.\end{aligned}$$

(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]

Solution: (Unseen)

There are two cases to consider: $E(\mathbb{Q})$ infinite, and $E(\mathbb{Q})$ finite.

- First suppose that $E(\mathbb{Q})$ is infinite. From lectures, we know that for any constant N, the set of points $P \in E(\mathbb{Q})$ such that $h_x(P) \leq N$ is finite. In particular, this is true for $N = N(c)$ as defined in the question. Therefore only finitely many points in $E(\mathbb{Q})$ satisfy $h_x(P) \leq N(c)$. Since we assume there are infinitely many points altogether, it follows that infinitely many of them must satisfy $h_x(P) > N(c)$.
- Now suppose that $E(\mathbb{Q})$ is finite. Then every $P \in E(\mathbb{Q})$ has finite order. We want to show that every point $P \in E(\mathbb{Q})$ satisfies $h_x(P) \leq N(c)$.

  First, if $P = O$, then $h_x(P) = 0$ by definition, so the required inequality holds.

continued. . .

If $P \neq O$, then $P = (x, y)$. Since E is defined by an integral equation, and P has finite order, the Integrality Theorem and Nagell–Lutz say that $x, y \in \mathbb{Z}$ and $y = 0$ or $y^2 \mid \Delta = -27c^2$.

If $y = 0$ then $x^3 = -c$. In this case

$$\begin{aligned} h_x(P) &= \ln(|x|) \\ &= \frac{1}{3}\ln(c) < N(c) \end{aligned}$$

as required.

If $y \neq 0$, then $y^2 \mid -27c^2$. Since $x^3 = y^2 - c$, we get

$$\begin{aligned} |x^3| &= |y^2 - c| \\ &< |27c^2|. \end{aligned}$$

Taking natural logs on both sides, and dividing by 3, this gives

$$\begin{aligned} h_x(P) = \ln(|x|) &\leq \frac{1}{3}\left(3\ln(3) + 2\ln(c)\right) \\ &= \ln(3) + \frac{2}{3}\ln(c) \\ &= N(c) \end{aligned}$$

as required.

continued. . .

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