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]

Solution: (Bookwork) The order of P on E is the smallest natural number n such that $nP = O$, where O denotes the identity, if such an n exists; if no such n exists, P is said to have infinite order.

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

$$\begin{aligned} E \,:\, y^2 &= x^3 + x^2 + 7x \\ P &= (1, 3) \\ Q &= (7, 21). \end{aligned}$$

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

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

Solution: (Similar examples seen) We follow the procedure defined in lectures. First we consider $2P$. The point $P{*}P$ is defined as the third point of intersection of the curve C with the line L_P, the tangent line to C at P. The slope of L_P is given by

$$\begin{aligned} \left(\frac{dy}{dx}\right)_{|P} &= \left(\frac{3x^2 + 2x + 7}{2y}\right)_{|P} \\ &= \frac{3 \cdot 1^2 + 2 \cdot 1 + 7}{2 \cdot 3} \\ &= \frac{12}{6} = 2. \end{aligned}$$

So the tangent line L_P has equation of the form $y = 2x + c$, and substituting the coordinates of P, we see that $c = 1$. So the line L_P is $y = 2x + 1$. To find the x-coordinate of $P * P$ we substitute this into the equation of E: this gives

$$\begin{aligned} (2x + 1)^2 = x^3 + x^2 + 7x \quad &\Leftrightarrow \\ x^3 - 3x^2 - 3x - 1 = 0. & \end{aligned}$$

This equation has a double root at $x = 1$, corresponding to P; the third root corresponds to $P * P$. We can find this either by inspection or by long division: in any case we find that the third root is also $x = 1$. Since $P * P$ lies on the line $y = 2x + 1$ and has the same x-coordinate as P, we get $P * P = P$. Therefore we get

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

Next we consider $2Q$. The same procedure shows that the tangent line $L_Q$at

Q has slope

$$\begin{aligned}\left(\frac{dy}{dx}\right)_{|Q} &= \left(\frac{3x^2+2x+7}{2y}\right)_{|Q}\\ &= \frac{3\cdot 7^2+2\cdot 7+7}{2\cdot 21}\\ &= 4.\end{aligned}$$

and substituting the coordinates of Q we get that the equation of L_Q is $y = 4x-7$. To find $Q*Q$ we substitute this into the equation of E to get

$$\begin{aligned}(4x-7)^2 = x^3+x^2+7x \quad &\Leftrightarrow\\ x^3-15x^2+63x-49 &= 0.\end{aligned}$$

This has a double root at $x=7$; long division by $(x-7)^2$ shows that the third root is at $x=1$. Using the equation of the line L_Q we get $Q*Q=(1,-3)=P$ and hence

$$\begin{aligned}2Q &= P\\ &= (1,3).\end{aligned}$$

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

Solution: (Similar examples seen) In the previous part we found that $2P=-P$, so $3P=O$. Therefore the order of P divides 3; since P is not the identity, this shows that P has order 3.
We also found that $2Q=P$, so $6Q=O$. This shows that the order of Q divides 6. Since $2Q\neq O$ the order is not 2; we also know that $3Q=P+Q$, which is nonzero since $Q\neq -P$. Therefore Q has order 6.

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

Solution: (Bookwork)

Mordell's Theorem: let E be an elliptic curve defined over the rational numbers $\mathbb{Q}$. Then

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

where $r\geq 0$ is a natural number and T is a finite group.

(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]

Solution: (Similar examples seen) Nagell–Lutz says that if $P = (x, y)$ is a point of finite order on E, then y is an integer and $y = 0$ or $y^2 \mid \Delta$. We compute

$$\begin{aligned}\Delta &= -4 \cdot (-6)^3 - 27 \cdot (6)^2 \\ &= -108 \\ &= 2^2 \cdot 3^3.\end{aligned}$$

So the possibilities are

$$|y| = 0, 1, 2, 3, 6.$$

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

$$\frac{df}{dx} = 3x^2 - 6$$

so for $|x| > \sqrt{2}$ the cubic is monotonic increasing.

We compute that $f(-3) = -3 < 0$; since $|-3| > \sqrt{2}$ the monotonic property tells us that $f(x) < 0$ for $x \leq -3$, so no x-value in this range can give us a rational point on the curve. Also $f(4) = 46 > 6^2$, so again the monotonic property says that $f(x) > 6^2$ for $x \geq 4$, 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 in the range $-2 \leq x \leq 3$. We get

$$10, 11, 6, 1, 2, 16$$

Among these, the only value which is a square of a y-value listed above is $f(1) = 1 = 1^2$. So along with the identity O, we have candidate torsion points

$$P = (1, \pm 1).$$

We compute

$$x(2P) = \frac{17}{4} \notin \mathbb{Z}$$

so $\pm P$ are not torsion points.

We have shown that there are no torsion points other than the idenity O, and so $T = \{O\}$, the trivial group.

(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]

Solution: (Unseen) For every n, the curve E_n contains the point $P = (1,1)$. The formula for point doubling gives

$$\begin{aligned} x(2P) &= \left(\frac{3 \cdot 1^2 - n}{2 \cdot 1}\right)^2 - 2 \\ &= \left(\frac{3-n}{2}\right)^2 - 2 \end{aligned}$$

Since n is even, the numerator of this fraction is odd, so $x(2P)$ is not an integer. The Integrality Theorem therefore says that P has infinite order, and so $E(\mathbb{Q})$ is infinite.

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]

Solution: (Similar examples seen)
From lectures we know that, for an odd prime p, the reduction $\overline{E}$ is not an elliptic curve if and only if $p \mid \Delta$. We compute

$$\begin{aligned} \Delta &= -4 \cdot (-8)^3 - 27 \cdot (-3)^2 \\ &= 1805 \\ &= 5 \cdot 19^2. \end{aligned}$$

So $\overline{E}$ is not an elliptic curve for $p = 5$ or $p = 19$.

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

Solution: (Similar examples seen)
By Part (a), we know that the reduction $\overline{E}$ of E modulo p is an elliptic curve for any odd prime $p \neq 5$, 19. The Torsion Embedding Theorem then says in particular that $|T|$ divides $|\overline{E}(\mathbb{F}_p)|$.

- First we reduce mod 3. We get the elliptic curve $\overline{E}$ given by the equation

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

Tabulating the $\mathbb{F}_3$-points on this curve we get

x	0	1	2
x^3+x	0	2	1
y	± 0	$-$	± 1

Here we use the list of squares in $\mathbb{F}_3$:

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

So

$$\overline{E}(\mathbb{F}_3) = \{O, (0,0), (2, \pm 1)\}.$$

Therefore $|\overline{E}(\mathbb{F}_3)| = 4$, so by the Torsion Embedding Theorem we have $|T| \mid 4$.

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

$$\overline{E}\ :\ y^2 = x^3 + 6x + 4.$$

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

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

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

$$\overline{E}(\mathbb{F}_7) = \{O, (0,\pm 2), (1, \pm 2), (3,0), (4,\pm 1), (6, \pm 2)\}.$$

Therefore $|\overline{E}(\mathbb{F}_7)| = 10$, so by the Torsion Embedding Theorem we have $|T| \mid 10$.

Putting these results together we get $|T| \mid \gcd(4, 10) = 2$. So either T is the trivial group, or else $T = 2$ and T contains a point of order 2.
To decide if T contains an element of order 2, we note that any point of order 2 has y-coordinate equal to 0. So we are looking for an integer solution of $x^3 - 8x - 3 = 0$. By inspection such a solution is given by $x = 3$, so $(3, 0)$ is a point of order 2 in T.
Therefore

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

(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]

Solution: (Unseen) We have $\Delta = -27 \cdot p^2$ so in particular the curve $\overline{E}$ given by reduction of E mod 5 is an elliptic curve. It is given by the equation

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

Tabulating the $\mathbb{F}_5$-points on $\overline{E}$ we get

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

So

$$\overline{E}(\mathbb{F}_5) = \{O, (2,0), (3, \pm 2), (4, \pm 1)\}.$$

So the Torsion Embedding Theorem says that $|T| \mid 6$. However, if $|T| = 6$ then (as seen in lectures) $T \cong \mathbb{Z}_6$; in particular T contains a point of order 2. Any such point has coordinates $(x, 0)$ where $x \in \mathbb{Z}$ and $x^3 + p = 0$. Since p is a prime, this equation has no integer solution. Hence T has no element of order 2, and therefore $|T| \neq 6$. We conclude that $|T| \leq 3$.

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]

Solution: (Bookwork) The Eisenstein series of weight k associated to L is defined as

$$G_k(L) = \sum_{\omega \in L,\, \omega \neq 0} \frac{1}{\omega^k}.$$

(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]

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

$$\begin{aligned} \omega &= \frac{\omega_1}{\omega_2} \\ &= (1+i)^{-1}\left(-\frac{8}{5} - \frac{6}{5}i\right) \\ &= \frac{1}{2}(1-i)\left(-\frac{8}{5} - \frac{6}{5}i\right) \\ &= -\frac{7}{5} + \frac{1}{5}i. \end{aligned}$$

The real part of this number is $-\frac{7}{5} < -\frac{1}{2}$ so we apply the map

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

to get

$$T\omega = -\frac{2}{5} + \frac{1}{5}i.$$

Since $|T\omega| = \sqrt{1/5} < 1$ we apply the map

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

to get

$$\begin{aligned} ST\omega &= \left(\frac{2}{5} - \frac{1}{5}i\right)^{-1} \\ &= 5\left(\frac{1}{2-i} \cdot \frac{2+i}{2+i}\right) \\ &= 2+i. \end{aligned}$$

Finally we apply the map T^{-2} to get

$$T^{-2}ST\omega = i$$

Since this number has real part equal to 0 and absolute value equal to 1, we have $T^{-}2ST\omega \in \mathcal{F}$.

So the required number τ is

$$\begin{aligned} \tau &= T^{-2}ST\omega \\ &= i. \end{aligned}$$

(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]

Solution: (Similar examples seen) To transform E_t to Weierstrass form we make the substitution

$$x = x' + 1$$

which gives

$$\begin{aligned} y^2 &= (x\prime + 1)^3 - 3(x'+1)^2 + (3+t)(x'+1) - 3 \\ &= (x')^3 + t(x') + (t-2). \end{aligned}$$

Therefore

$$j(E_t) = 1728 \cdot \frac{4t^3}{-4t^3 - 27(t-2)^2}$$

(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]

Solution: (Unseen) Since L is similar to the lattice $\Lambda = \mathbb{Z} \oplus \mathbb{Z} \cdot i$, the elliptic curve E_L is isomorphic to the curve E_Λ. The Equivalence Theorem says that the curve E_Λ is defined by the equation

$$E_\Lambda \, : \; y^2 = 4x^3 - 60G_4x - 140G_6$$

where G_4 and G_6 are the Eisenstein series of weights 4 and 6 associated to Λ. An example seen in lectures shows we have $G_6(\Lambda) = 0$ so this equation is

$$E_\Lambda \, : \; y^2 = 4x^3 - 60G_4x$$

which in Weierstrass form becomes

$$E_\Lambda \, : \; y^2 = x^3 - 240G_4x.$$

This gives $j(E_\Lambda) = -1728$.
We want to find all t such that $E_t \simeq E_L$: for this, it is enough to find all t such that

$$j(E_t) = j(E_\Lambda).$$

By the above and the previous part, this becomes

$$1728 \cdot \frac{4t^3}{-4t^3 - 27(t-2)^2} = -1728$$

which reduces to

$$(t-2)^2 = 0$$

The only solution is therefore

$$t = 2.$$

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

$$\begin{aligned} P &= (x_0, y_0) \\ Q &= (x_0, -y_0) \end{aligned}$$

    then $P \oplus Q = O$.

  - given points P, Q on E with coordinates

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

    let

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

    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

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

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