Loughborough University

ELLIPTIC CURVES
(20MAC260)

Semester 2 2021 — 23 hours

This is a (1a) online examination, meaning you have 23 hours in which to complete and submit this paper. How you manage your time within the 23-hour window is up to you, but we expect you should only need to spend approximately 2 hours working on it. If you have extra time or rest breaks as part of a Reasonable Adjustment, you will need to add this to the amount of time you are expected to spend on the paper.

It is your responsibility to submit your work by the deadline for this examination. You must make sure you leave yourself enough time to do so.

It is also your responsibility to check that you have submitted the correct file(s).

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]

Solution: (Similar examples seen)

We start by computing the point $2P = P \oplus P$. The first step is to compute $P * P$.

The tangent line to E at the point P has slope

$$\frac{dy}{dx}(P) = \frac{3x^2 - 6x + 3}{2y}(P)$$
$$= 2$$

so its equation is

$$y = 2x - 3$$

Substituting this into the equation of E we get

$$(2x-3)^2 = x^3 - 3x^2 + 3x$$

which simplifies to

$$x^3 - 7x^2 + 15x - 9 = 0$$

Since the line is tangent to the curve at P, we know this cubic has $x = 3$ as a double root; divding we get

$$x^3 - 7x^2 + 15x - 9 = (x-3)^2(x-1)$$

So the point $P * P$ has $x = 1$; since it is on the line $y = 2x - 3$ we get

$$P * P = (1, -1) \text{ and so}$$
$$2P = P \oplus P = (1, 1).$$

Next we compute $3P = 2P \oplus P$: again we start by computing $2P * P$. The line joining $2P$ to P has slope $\frac{3-1}{3-1} = 1$ so the equation is $y = x$. Substituting this in the equation of E we get

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

which simplifies to

$$x(x-1)(x-3) = 0$$

The roots $x = 3$ and $x = 1$ correspond to P and $2P$ respectively, so $P * P$ has $x = 0$ and $y = 0$. Therefore

$$2P * P = (0, 0) \text{ and so}$$
$$3P = (0, 0).$$

Since $3P$ has y-coordinate equal to 0, it is a point of order 2. Therefore

$$6P = 2(3P)$$
$$= O.$$

Since we have seen that $2P$, $3P \neq O$ and $4P = -2P \neq O$ and $5P = -P \neq O$ this shows that P has order 6.

(b) Consider the family of curves defined by

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

continued. . .

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

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

Solution: (Similar examples seen)

First, for $t = 0$ the right-hand side is not a cubic, so E_0 does not give an elliptic curve.

For $t \neq 0$, we put the given curve in Weierstrass form by setting

$$x' = x/t,\ y' = y/t$$

and clearing denominators; this transforms the given equation to

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

(where the variables have been renamed to x and y).

The discriminant of this curve is

$$\begin{aligned}\Delta &= -4a^3 - 27b^2 \\ &= -4(-3t)^3 - 27(2t^3)^2 \\ &= -108t^3(t^3 - 1).\end{aligned}$$

For $t \neq 0$ we get $\Delta = 0$ when $t^3 - 1$, that is

$$t = 1,\ \omega,\ \omega^2$$

where $\omega = \exp(2\pi i/3)$.

So E_t is not an elliptic curve for $t = 0,\ 1, \omega,\ \omega^2$.

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 $T \subset E(\mathbb{Q})$. [20]

Solution: (Similar examples seen) The discriminant of the curve is

$$\begin{aligned}\Delta &= -4a^3 - 27b^2 \\ &= -4(-11)^3 - 27(10)^2 \\ &= 2624 \\ &= 2^6 \cdot 41\end{aligned}$$

continued. . .

Nagell-Lutz says that if (x, y) is a point of T, then $y = 0$ or $y^2 \mid \Delta$, in other words $y = 0$ or $|y| = 1, 2, 4, 8$. We now analyse these possibilities.

As usual we can tabulate the possibilities to check if there are any corresponding x-values for each value of $|y|$:

$\lvert y\rvert$	0	1	2	4	8
y^2	0	1	4	16	64
x					

To fill in the bottom row, we argue as follows. We note that if $f = x^3 - 11x + 10$ then $\frac{df}{dx} = 3x^2 - 11$. So f is monotonic increasing for $|x| \geq \sqrt{11/3}$, in particular for $x \leq -2$ or $x \geq 2$.

We can check that $f(-4) < 0$, so $f(x) < 0$ for $x \leq -4$, and $f(5) = 80$, so $f(x) > 64$ for $x \geq 6$. For $-3 \leq x \leq 4$ the values of $f(x)$ can be calculated as follows:

$$16,\ 24,\ 20,\ 10,\ 0,\ -4,\ 4,\ 30$$

Comparing with the above table, we see that our candidate torsion points are

$$(-3, \pm 4),\ (3, \pm 2)\ (1, 0).$$

The latter point has $y = 0$ and therefore has order 2.

For $P = (-3, \pm 4)$ we use the formula from Week 3 to compute that the x-coordinate of $2P$ is

$$\begin{aligned} x(2P) &= \left(\frac{3x(P)^2 - 11}{2y(P)}\right)^2 - 2x(P) \\ &= \left(\frac{16}{8}\right)^2 - 2 \cdot (-3) \\ &= 10 \end{aligned}$$

Doubling again we find that

$$\begin{aligned} x(4P) &= \left(\frac{3x(2P)^2 - 11}{2y(2P)}\right)^2 - 2x(2P) \\ &= \frac{11521}{3600} \end{aligned}$$

Since this is not an integer, the point $4P$ is not torsion, hence neither is P. So the points (-3 ± 4) are not torsion.

continued. . .

For $P = (3, \pm 2)$ we compute

$$\begin{aligned} x(2P) &= \left(\frac{3x(P)^2 - 11}{2y(P)}\right)^2 - 2x(P) \\ &= \left(\frac{16}{4}\right)^2 - 2 \cdot (3) \\ &= 10 \end{aligned}$$

and as above we see that the points $(3, \pm 2)$ are not torsion.

We conclude that the torsion subgroup is

$$\begin{aligned} T &= \{O, (-1, 0)\} \\ &\cong \mathbb{Z}_2. \end{aligned}$$

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

Solution: (Unseen) In the previous part we found points such as $P = (3, 2)$ which belong to $E(\mathbb{Q})$ but do not have finite order. So there are infinitely many points $\{nP \mid n \in \mathbb{Z}\}$, hence $E(\mathbb{Q})$ is infinite.

continued. . .

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]

Solution: (Similar examples seen) The discriminant is

$$\begin{aligned}\Delta &= -4 \cdot (-12)^3 \\ &= 2^8 3^3\end{aligned}$$

For an odd prime p, the reduction $\overline{E}$ modulo p is not an elliptic curve if and only if $p \mid \Delta$, so the only such prime is $p = 3$.

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

Solution: (Similar examples seen) By the previous part, the reduction of E mod p gives an elliptic curve for any odd prime p other than 3.

- First we reduce E mod 5 to get the curve $\overline{E}$ over $\mathbb{F}_5$ defined by

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

We tabulate the points on this curve over $\mathbb{F}_5$:

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

So we get

$$\overline{E}(\mathbb{F}_5) = \{O, (0,0), (1,\pm 2), (2,\pm 2), (3,\pm 1), (4 \pm 1)\} \quad \text{so}$$
$$\left|\overline{E}(\mathbb{F}_5)\right| = 10.$$

By the Torsion Embedding Theorem, for the torsion subgroup $T \subset E(\mathbb{Q})$ we must therefore have that $|T|$ divides 10.

- Next reduce mod 7 to get the curve $\overline{E}$ over $\mathbb{F}_7$ defined by

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

We tabulate the points on this curve over $\mathbb{F}_7$:

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

continued. . .

So we get

$$\overline{E}(\mathbb{F}_7) = \{O, (0,0), (4,\pm 3), (5,\pm 3), (6,\pm 2\} \quad \text{so}$$
$$\left|\overline{E}(\mathbb{F}_7)\right| = 8.$$

As before this implies $|T|$ divides 8.

Putting these two results together we get that $|T|$ divides $\gcd(8,10) = 2$.
Finally, we can see there is a nontrival torsion point on E, namely $P = (0,0)$ which has order 2 since the y-coordinate is 0. So we must have $|T| = 2$, and therefore $T \cong \mathbb{Z}_2$.

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]

Solution: (Similar examples seen) The curve E contains the evident point $Q = (1,1)$. This point has height $h_x(Q) = 0$ so it does not satisfy the condition.
Using the addition formula from Week 3 we compute

$$2Q = (2, -3)$$

This has height $h_x(2Q) = \ln(2) \approx 0.69$ so we continue.
Doubling again we find

$$4Q = \left(\frac{25}{36}, \frac{37}{216}\right)$$

This point has height

$$h_x(4Q) = \ln(36) \approx 3.58$$

so $P = 4Q$ is the required point.

(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]

Solution: (Unseen) For any given M there are only finitely many points $Q = (x, y)$ with $x, y \in \mathbb{Q}$ and $h_x(P) \leq M$. From the previous part for $Q = (1, 1)$ we have seen that $4Q$ has non-integer coordinates, so $Q = (1, 1)$ is not a point of finite order. Hence $E(\mathbb{Q})$ is infinite, so for any given M we have $h_x(Q) > M$ for all but finitely many $Q \in E(\mathbb{Q})$.

(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

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

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

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

We can now apply the transformations

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

and their inverses to move ω into the fundamental domain $\mathcal{F}$.

First we compute

$$\begin{aligned} T\omega &= \omega + 1 \\ &= \frac{1}{2\sqrt{2}} + \frac{1}{2\sqrt{2}}\, i \\ &= \frac{1}{2} \left(\exp(\pi i/4) \right) \end{aligned}$$

continued. . .

This has absolute value $|T\omega| = \frac{1}{2}$, so next we apply S to get

$$\begin{aligned} ST\omega &= -\frac{1}{T\omega} \\ &= -2\exp(-\pi i/4) \\ &= -2\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\,i\right) \\ &= -\sqrt{2} + \sqrt{2}\,i \end{aligned}$$

This number has absolute value $|ST\omega| = 2$. Its real part is $\mathrm{Re}(ST\omega) = -\sqrt{2} < -\frac{1}{2}$. So we apply T again to get

$$TST\omega = (-\sqrt{2} + 1) + \sqrt{2}\,i.$$

Now the absolute value of the real part is $|-\sqrt{2}+1| \approx 0.414 < \frac{1}{2}$ and the absolute value is

$$\sqrt{(-\sqrt{2}+1)^2 + (\sqrt{2})^2} > \sqrt{2} > 1$$

so $TST\omega \in \mathcal{F}$.

So the required number τ is

$$\begin{aligned} \tau &= TST\omega \\ &= (-\sqrt{2} + 1) + \sqrt{2}\,i. \end{aligned}$$