Imperial College London

MATH97043 MATH97152

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2021

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Number Theory: Elliptic Curves

Date: Monday, 24 May 2021

Time: 09:00 to 11:30

Time Allowed: 2.5 hours

Upload Time Allowed: 30 minutes

This paper has 5 Questions.

Candidates should start their solutions to each question on a new sheet of paper.

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD INCLUDING A COMPLETED COVERSHEET WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

You may use any results from the lectures, provided that you state them clearly.

1. Consider the projective plane conic:

$$5X^2 - 7Y^2 + 9Z^2 = 0.$$

Determine whether it has a point over the following completions:

(a) $\mathbb{Q}_5$ (5 marks)

(b) $\mathbb{Q}_3$ (5 marks)

(c) $\mathbb{Q}_7$. (5 marks)

(d) Are there other completions of $\mathbb{Q}$ for which the conic has no points? (5 marks)

(Total: 20 marks)

2. (a) Let P_1, P_2, P_3, P_4, P_5 be distinct points in $\mathbb{P}^2(\mathbb{C})$ and such that no three of the five points are collinear. Show that there is a unique conic passing through those points (up to rescaling the equation of the conic by a scalar in $\mathbb{C}^\times$).

(5 marks)

(b) Let

$$P_1 = (1, 1), \quad P_2 = (1, -1), \quad P_3 = (-1, -1), \quad P_4 = (-1, 1) \in \mathbb{A}^2(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}).$$

Find a basis of the space of conics through these points given by singular conics (work projectively).

(10 marks)

(c) Can you find a conic through $P_1, \ldots, P_4$ intersecting the line at infinity with multiplicity 2 at a non-singular point? (5 marks)

(Total: 20 marks)

3. Compute the torsion subgroup of $E(\mathbb{Q})$ for the following elliptic curves:

(a) $y^2 = x^3 - 8$ (10 marks)

(b) $y^2 = x^3 - 2x + 1.$ (10 marks)

(Total: 20 marks)

4. Show that the group $E(\mathbb{Q})$ of rational points of the elliptic curve $y^2 = x^3 - 9x$ is finite.

(20 marks)

(Total: 20 marks)

5. Let p be a prime. Let E be an elliptic curve over $\mathbb{Q}_p$ defined by the Weierstrass equation $y^2 - g(x) \in \mathbb{Z}_p[x,y]$ where $g(x)$ is a monic cubic polynomial. Denote $\overline{E}$ the (not necessarily non-singular) cubic defined by reducing the coefficients of the polynomial $y^2 - g(x)$ modulo p.

Let $\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$ be the set of non-singular points of $\overline{E}$ over $\mathbb{F}_p$. Let $E(\mathbb{Q}_p)^{(0)}$ be the subset of $E(\mathbb{Q}_p)$ given by points reducing to non-singular points modulo p.

(a) Let E be elliptic curve over $\mathbb{Q}_3$ defined by the polynomial $y^2 - x^3 - 24 \in \mathbb{Z}_3[x,y]$. Let

$$P = (25/4, -131/8) \quad \text{and} \quad Q = (1,5)$$

be points of $E(\mathbb{Q}_3)$. Does $3P + 2Q$ reduce to a singular point in $\overline{E}(\mathbb{F}_3)$? (5 marks)

(b) Applying Hensel's Lemma or otherwise, show that the reduction map $E(\mathbb{Q}_p)^{(0)} \to \overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$ is surjective.

(10 marks)

(c) Let E be the elliptic curve defined by $y^2 - x^3 + 7 \in \mathbb{Z}_7[x,y]$. Show that $E(\mathbb{Q}_7)^{(0)} = E(\mathbb{Q}_7)$.

(5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2021

This paper is also taken for the relevant examination for the Associateship.

MATH97043/ MATH97152

Number Theory: Elliptic Curves (Solutions)

Setter's signature	Checker's signature	Editor's signature
....	....	....

1. (a) There are no solutions over $\mathbb{Q}_5$. Suppose there is a solution $[x : y : z] \in \mathbb{P}^2(\mathbb{Q}_5)$. We can assume that the maximum of the norms of x, y, z is equal to 1. If $|y|_5 < 1$, then $|z|_5 < 1$, because otherwise $|7y^2 - 9z^2|_5 = |z^2|_5 = 1 > |5x^2|_5$. But then we would have $|7y^2 - 9z^2|_5 \leq 5^{-2}$, forcing $|x|_5 < 1$, which contradicts the fact that the maximum of the norms is 1. So $|y|_5 = 1$. But then reducing modulo 5, the equation

$$-7y^2 + 9z^2 = 0 \mod 5$$

admits a non-zero solution. Since y is non-zero modulo 5, we can assume $y = 1$ and get a solution to $z^2 = 3 \mod 5$, but 3 is not a quadratic residue mod 5. Contradiction.

$\boxed{\text{sim. seen} \Downarrow}$ $\boxed{5, \text{A}}$

(b) There is a solution over $\mathbb{Q}_3$. This would follow from noticing that we can rescale the variable Z for the conic and solve $5X^2 - 7Y^2 + Z^2$, which admits a solution over $\mathbb{Q}_p$ for all primes p not dividing $2 \cdot 5 \cdot 7$. However, we can easily do this directly. By Hensel's Lemma applied to the polynomial $f(T) = T^2 - 7 \in \mathbb{Z}_3[T]$, for the value $t_0 = 1$ satisfying $|f(1)|_3 = |-6|_3 < 1 = |f'(1)|_3^2$, we can find a squareroot of 7 in $\mathbb{Z}_3$ congruent to 1 modulo 3. Call it α. Then $[0 : 1 : \alpha/3]$ works.

$\boxed{\text{sim. seen} \Downarrow}$ $\boxed{5, \text{B}}$

(c) There is a solution in $\mathbb{Q}_7$. Modulo 7, there is a non-zero solution to

$$5x^2 + 9z^2 = 0 \pmod 7.$$

For instance, we can take one such that $x = 1$ and $z = 1$. Then we can take the polynomial $g(T) = 5T^2 + 9 \in \mathbb{Z}_7[T]$, and apply Hensel's Lemma to the value $t_0 = 1$ to get a squareroot of $-9/5$ in $\mathbb{Z}_7$. Call it β. Then $[\beta : 0 : 1]$ works.

$\boxed{\text{sim. seen} \Downarrow}$ $\boxed{5, \text{A}}$

(d) There are no solutions over $\mathbb{Q}_2$. Suppose $[x : y : z]$ is a solution. We can again assume that the maximum of the norms is 1. Notice that $5 = -7 = 9 = 1 \pmod 4$. Then reducing modulo 4 we get a non-zero solution to

$$x^2 + y^2 + z^2 = 0 \pmod 4.$$

But since squares are congruent to either zero or 1 modulo 4, this is impossible.

$\boxed{\text{sim. seen} \Downarrow}$ $\boxed{5, \text{A}}$

2. (a) Every conic in $\mathbb{P}^2(\mathbb{C})$ can be written as

sim. seen ⇓

5, B

$$aX^2 + bY^2 + cXY + dXZ + eYZ + fZ^2 = 0.$$

for $a, b, c, d, e, f \in \mathbb{C}$. Imposing that the conic passes through the points $P_1, P_2, \ldots, P_5$ gives 5 linear conditions on the six coefficients, so the space of solutions has dimension at least 1. Suppose that C_1, C_2 are two conics through the 5 points. Then by Bezout's Theorem, they must have a common factor. Either that factor is irreducible of degree 2 or it has degree 1. In the first case, the conics are the same up to rescaling. In the second case, they have a line in common. Then C_1 must factor as $C_1 = L_1 \cdot L_2$, where L_1, L_2 are linear factors, and at least 3 of the 5 points must lie on the graph of either L_1 or L_2.

unseen ⇓

10, D

(b) This can be solved either by pure thought or by calculation. We are given 4 points, and no 3 are collinear. Passing through 4 points gives 4 linear conditions on the coefficients of the conics; so there is at least a 2-dimensional space of solutions. If we choose a 5-th point such that it does not lie on any of the lines through 2 of the 4 points (which can certainly do over $\mathbb{C}$), then we determine a unique conic by Part (a). So the space of conics through the 4 points must have dimension exactly 2. To find singular conics through those points we can choose two points and draw a line through them; and then draw the line through the remaining two points.

Alternatively, we can do a computation. Imposing the condition that the conics pass through the chosen points gives the system of equations:

$$\begin{cases} a+b+c+d+e+f=0 \\ a+b-c+d-e+f=0 \\ a+b+c-d-e+f=0 \\ a+b-c-d+e+f=0. \end{cases}$$

This gives $c = d = e = 0$ and $f = -(a+b)$. So we get the 2-parameter family:

$$F_{a,b}(X,Y,Z) = aX^2 + bY^2 - (a+b)Z^2 = 0$$

Taking partial derivatives, we get

$$\frac{\partial F}{\partial X} = 2aX, \quad \frac{\partial F}{\partial Y} = 2bY, \quad \frac{\partial F}{\partial Z} = -2(a+b)Z.$$

So there are no singular points unless either $a = 0$ or $b = 0$ or $a + b = 0$. For $a = 0$, up to scalars, we get the singular conic $Y^2 - Z^2 = 0$. For $b = 0$, we get $X^2 - Z^2 = 0$. For $a + b = 0$, we get $X^2 - Y^2 = (X+Y)(X-Y)$. Taking any two out of these three gives a basis of the conics through the 4 points.

5, C

unseen ⇓

(c) In this case, we can assume $ab \neq 0$, otherwise there is a unique point at infinity, but it is singular. But then the intersection of the conic $F_{a,b}(X,Y) = aX^2 + bY^2 - (a+b)Z^2$ with the line $Z = 0$ always gives two distinct points.

3. (a) The elliptic curve is $y^2 = x^3 - 8$. For this question there could potentially be different approaches, relying on either Nagell-Lutz or reduction modulo primes. We start looking for points of order 2: by imposing $y = 0$, we get the solution $(2, 0)$. The discriminant is $\Delta = 27 \cdot 8^2$, so if we want to apply the Lutz-Nagell Theorem we have to check the existence of solutions for $y^2 \mid 27 \cdot 8^2$, that is $y \mid 3 \cdot 8$. This is a bit tedious, so we try reducing modulo a prime not dividing 2Δ. Over $\mathbb{F}_5$, we get that $\overline{E}(\mathbb{F}_5)$ has 6 points, namely, $\boxed{\text{meth seen} \Downarrow}$ $\boxed{5, \text{A}}$

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

in addition to the point at infinity. So we get a group of order 6. Since the reduction map $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$ for $p \nmid 2\Delta$ is injective on torsion points, we must have either that either the torsion subgroup of $E(\mathbb{Q})$ has order 2 or order 6. To rule out the second possibility, we can look at the reduction modulo 7. Here we get only get 3 points of order 2

$$(1, 0), (2, 0), (4, 0)$$

so the group of points $E(\mathbb{F}_7)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This rules out the possibility that the torsion subgroup would be cyclic of order 6, so it is cyclic of order 2. $\boxed{5, \text{B}}$

(b) The elliptic curve is $y^2 = x^3 - 2x + 1$. We can spot the points with integer coordinates $(1, 0)$ and $(0, \pm 1)$. We check that these are all the possible points by Nagell-Lutz. The discriminant is $\Delta = 4(-2)^3 + 27 = -32 + 27 = -5$. So we look at the solutions for $y = \pm 1$. In this case, we get $\boxed{\text{meth seen} \Downarrow}$

$$1 = x^3 - 2x + 1,$$

giving the solution $x = 0$, so we recover the points $(0, \pm 1)$.

So either the torsion subgroup is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$. $\boxed{5, \text{A}}$

We can compute the tangent line through $P = (0, 1) = (x_P, y_P)$ (or use the doubling formula directly):

$$2y_P y - (3x_P^2 - 2)x + c = 0$$

which gives $y + x = 1$ and get $(-x + 1)^2 = x^3 - 2x + 1$, giving

$$1 = 2x_P + x_{2P}$$

So $x_{2P} = 1$ and $y_{2P} = -1 + x_{2P} = 0$. So the torsion subgroup is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. $\boxed{5, \text{B}}$

seen ⇓

4. Let $y^2 = x\,(x-3)\,(x+3)$ be E. We denote $e_1 = 0$, $e_2 = -3$ and $e_3 = 3$. The points of order 2 are rational and of the form $T_i = (e_i, 0)$. We let S be the set of primes dividing $(e_1 - e_2)(e_2 - e_3)(e_3 - e_1) = (0+3)(-3-3)(3) = -54$; we get $S = \{2, 3\}$. In the lectures, we have showed that there is a group homomorphism

$$\delta \colon E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

with kernel $2E(\mathbb{Q})$ and such that

$$\delta(x,y) = (x - e_1, x - e_2, x - e_3) = (x, x+3, x-3),$$

if (x,y) is not 2-torsion and

$$\delta(\mathcal{O}) = (1,1,1), \quad \delta(T_1) = (-1, 3, -3), \quad \delta(T_2) = (-3, 2, -6), \quad \delta(T_3) = (3, 6, -2).$$

We know that $\operatorname{Im}(\delta) = \{(\delta_1, \delta_2, \delta_3) \mid \delta_1\delta_2\delta_3 = 1\}$. The image is contained in the subgroup whose entries are $\{\pm1, \pm2, \pm3, \pm6\}$. Since $\delta_3 = (\delta_1\delta_2)^{-1} = \delta_1\delta_2$, we will ignore the third coordinate.

In order to compute the rank it remains to compute the image of δ. Since $E(\mathbb{Q})$ is a finitely generated abelian group, the rank is 0 if and only if $E(\mathbb{Q})$ is finite. For this, we determine for which $b_1, b_2 \in \{\pm1, \pm2, \pm3, \pm6\}$ the equations

$$x = b_1 u^2, \quad x + 3 = b_2 v^2 \quad x - 3 = b_1 b_2 w^2.$$

have a rational solution. We can eliminate x and solve

$$\begin{cases} b_2 v^2 - b_1 u^2 = 3 & (1) \\ b_1 u^2 - b_1 b_2 w^2 = 3. & (2) \end{cases}$$

5, A

First we observe that if $b_2 < 0$, there are no rational solutions (otherwise either (1) or (2) would have no solution depending on the sign of b_1). So we can represent the pairs (b_1, b_2) in a table

	1	2	3	6	-1	-2	-3	-6
1	✓							
2							✓	
3					✓			
6			✓					
-1	×	×	×	×	×	×	×	×
-2	×	×	×	×	×	×	×	×
-3	×	×	×	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

meth seen ⇓

in which the columns correspond to values of b_1 and the rows correspond to values of b_2, where we marked ✓ the pairs (b_1, b_2) such that a solution exists and × those for which a solution does not exist. We want to fill the rest of the table. Because the order of the image is at least 4, the rank is 0 if and only if it is exacly 4, i.e. the size of the rational 2-torsion. We need to show that for every other pair (b_1, b_2) there are no solutions. Note that since we have a solution of the form (b_1, b_2) with $b_1 < 0$, it suffices to show that there are no more solutions in the top left quadrant.

1. $(b_1, b_2) \in \{(1,2), (1,6)\}$: In both cases, Equation (1) has no rational solution, because it has no solutions over $\mathbb{Q}_3$.

2. $(b_1, b_2) = (1, 3)$: We get no solution for Equation (2) over $\mathbb{Q}_3$.
3. $b_1 \in \{\pm 2, \pm 6\}$ and b_2 odd: we can write $u = U/Z$, $v = V/Z$, $w = W/Z$, and try to solve

$$\begin{cases} b_2 V^2 - b_1 U^2 = 3Z^2 & (3) \\ b_1 U^2 - b_1 b_2 W^2 = 3Z^2. & (4) \end{cases}$$

for $U, V, W, Z \in \mathbb{Z}$ not all 0 and without common factors. Then by (4), we have $2 \mid Z$ and then by (3) we get $2 \mid V$, so $4 \mid b_1 U^2$, so $2 \mid U$ because $4 \nmid b_1$. Then $2 \mid W$, so $2 \mid U, V, W, Z$. Contradiction.

We can update the table:

	1	2	3	6
1	✓	×		×
2	×			
3	×	×		×
6	×		✓	

Now, since $(3, 6)$ is in the image of δ, if a pair (b_1, b_2) is not in the image of δ, then $(3, 6) \cdot (b_1, b_2)$ is also not in the image of δ.

	1	2	3	6
1	✓	×	×	×
2	×	×	×	×
3	×	×	×	×
6	×	×	✓	×

So we conclude that the image of δ has order $4 = |E(\mathbb{Q})[2]|$, which implies that the rank is 0, so $E(\mathbb{Q})$ is finite. $\boxed{15, \text{C}}$

5. (a) We reduce the equation mod 3 and get

unseen ⇓

$$y^2 = x^3$$

so the only singular point is $(0, 0)$. There is a reduction map

$$\mathrm{red}\colon E(\mathbb{Q}_3) \to \overline{E}(\mathbb{F}_3)$$

and the reduction of a point with coordinates (x, y) is singular if and only if $|x|_3, |y|_3 < 1$. The coordinates of the points P and Q are units in $\mathbb{Z}_3$, so $P, Q \in E(\mathbb{Q}_3)^{(0)}$. We have showed in the lectures that $E(\mathbb{Q}_3)^{(0)}$ is a group, so $3P+2Q \in E(\mathbb{Q}_3)^{(0)}$ as well, and thus it does not reduce to a singular point. (Note that trying to compute $3P + 2Q$ by hand is not feasible in this case, coordinates are huge!).

unseen ⇓

(b) The point at infinity of $\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$ is the image of the point at infinity of $E(\mathbb{Q}_p)$, so we can assume the point is affine. Denote $f(x, y) = y^2 - g(x) \in \mathbb{Z}_p[x, y]$ and denote $\overline{f}$ its image in $\mathbb{F}_p[x, y]$. Let $(x_0, y_0) \in \mathbb{A}^2(\mathbb{F}_p)$ be a non-singular point of the cubic $\overline{f} = 0$. Then either

$$\frac{\partial \overline{f}}{\partial x}(x_0, y_0) \neq 0 \quad \text{or} \quad \frac{\partial \overline{f}}{\partial y}(x_0, y_0) \neq 0.$$

Let us assume we are in the second case. Let $\tilde{x}_0, \tilde{y}_0$ be lifts of x_0, y_0 in $\mathbb{Z}_p$. Consider the polynomial $\alpha(T) = f(\tilde{x}_0, T) \in \mathbb{Z}_p[T]$. Then

$$\alpha(\tilde{y}_0) = 0 \pmod{p} \quad \text{and} \quad \alpha'(\tilde{y}_0) = \frac{\partial f}{\partial y}(\tilde{x}_0, \tilde{y}_0) \neq 0 \pmod{p}$$

by the assumptions that $\overline{f}(x_0, y_0) = 0$ and $\frac{\partial \overline{f}}{\partial y}(x_0, y_0) \neq 0$ respectively. It follows from Hensel's Lemma that the polynomial α has a zero congruent to $\tilde{y}_0$ modulo p. Call it $\breve{y}_0$. Then $(\tilde{x}_0, \breve{y}_0)$ is a point of $E(\mathbb{Q}_p)^{(0)}$ reducing to (x_0, y_0) in $\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$. Similarly for the case $\frac{\partial \overline{f}}{\partial x}(x_0, y_0) \neq 0$.

unseen ⇓

(c) The equation defining $\overline{E}$ is $y^2 = x^3 \in \mathbb{F}_7[x, y]$. The only singular point is $(0, 0)$. A point of $E(\mathbb{Q}_7)$ reducing to $(0, 0)$ would have coordinates $x, y \in \mathbb{Q}_7$ with $|x|_7, |y|_7 < 1$. So 7 would divide x and $y \in \mathbb{Z}_7$ and thus $7^2 \mid (y^2 - x^3) = -7$; contradiction.

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.

Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a sperate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
MATH97043MATH97152	1	This question went ok. Most students determined the existence of points correctly, but few justified their answers well.
MATH97043MATH97152	2	This question was often skipped at least in part. Many attempted 2a), setting up the question correctly, but did not show the uniqueness of the conic. 2b) was generally fine. In 2c) few students argued correctly that there are no conics iin the given family such that the line at infinity is tangent.
MATH97043MATH97152	3	This went almost universally well.
MATH97043MATH97152	4	This was a bit worse than I anticipated, given that the question was predictable. Almost everyone knew how to proceed, but not many could argue well that solutions would not exist in the various cases.
MATH97043MATH97152	5	This went fine, given that it was meant to be more challenging. Many stumbled on 5a), failing to use the fact that E(Q_p)^{(0)} is a subgroup. Those who attempted 5b) mostly had the correct ideas, but the arguments were a bit sloppy, with some confusion about what partial derivatives should be assumed to be non-zero. It was often unclear whether polynomials were taken with coefficient in Z or Z_p or F_p. Part c) was mostly fine.