Imperial College
London

MATH97043 MATH70064

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2022

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

Elliptic Curves

Date: 06 June 2022

Time: 09:00 – 11:30 (BST)

Time Allowed: 2:30 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 AS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD WITH COMPLETED COVERSHEETS WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

You may use any results from the lectures, as long as you refer to them clearly.

1. Let a and b be non-zero integers and consider the plane projective rational conic with equation

$$aX^2 + bY^2 - Z^2 = 0. \qquad (1)$$

(a) Let p be an odd prime not dividing ab. Show that Equation (1) has a non-zero solution over $\mathbb{Q}_p$. (6 marks)

(b) Let p be an odd prime, such that $p \nmid b$ and p divides a exactly (that is, $p \mid a$ and $p^2 \nmid a$). Show that Equation (1) has a non-zero solution over $\mathbb{Q}_p$ if and only if the image of b in $\mathbb{Z}/p\mathbb{Z}$ is a square. (6 marks)

(c) Show that if $a \equiv b \equiv 3 \pmod 4$, Equation (1) has no non-zero solutions over $\mathbb{Q}_2$.

(3 marks)

(d) Find integer values of a and b such that (1) has no non-zero solutions in $\mathbb{Q}_2$ and $\mathbb{Q}_{17}$, but it admits non-zero solutions over every other completion of $\mathbb{Q}$. (5 marks)

(Total: 20 marks)

2. Determine the structure of the torsion subgroup of $E(\mathbb{Q})$, up to isomorphism, for the following elliptic curves:

(a) $E : y^2 = x^3 - 11x + 14$

(10 marks)

(b) $E : y^2 = x^3 + 4$.

(10 marks)

(Total: 20 marks)

3. (a) Let $\mathcal{C}$ be the affine plane cubic defined by the equation

$$uv = (u-v)^3$$

in $\mathbb{A}^2(\mathbb{Q})$. Denote by $\tilde{\mathcal{C}}$ the projective plane cubic obtained by homogenising the equation of $\mathcal{C}$.

(i) Find the singular points of $\tilde{\mathcal{C}}$. (2 marks)

(ii) Show that $\tilde{\mathcal{C}}$ has a unique rational point at infinity. (2 marks)

(iii) Denote by $\mathcal{O}$ the unique rational point at infinity. Show that $\mathcal{O}$ is non-singular and is a point of inflection. (2 marks)

(b) Let $\tilde{\mathcal{C}}(\mathbb{Q})^{\mathrm{ns}}$ be the set of non-singular rational points of $\tilde{\mathcal{C}}$. Consider the map

$$\psi \colon \tilde{\mathcal{C}}(\mathbb{Q})^{\mathrm{ns}} \to \mathbb{Q} \setminus \{0\}$$

$$\psi(\mathcal{O}) = 1 \qquad \psi((u,v)) = u/v$$

where (u,v) is an affine rational point of the cubic. Show that ψ is well-defined and a bijection. (7 marks)

(c) Show that the map ψ is a group isomorphism, where the source is endowed with the group law on non-singular rational points with identity $\mathcal{O}$, and the target is viewed as a group under multiplication. *You may assume without proof that the cubic $\tilde{\mathcal{C}}$ is irreducible.* (7 marks)

(Total: 20 marks)

4. Let E be an elliptic curve over $\mathbb{Q}$ with equation $y^2 = x^3 + b$ where b is a non-zero integer, and b is not divisible by u^6, for any $u \in \mathbb{Z}_{>1}$.

(a) Show that $E(\mathbb{Q})$ has an element of order 2 if and only if b is a cube. (3 marks)

(b) Show that $E(\mathbb{Q})$ has an element of order 3 if and only if either b is a square or $b = -432$. (7 marks)

(c) Show that if p is a prime and $p \equiv 2 \pmod 3$, the set

$$\{(x,y) \in \mathbb{F}_p^2 \mid x^3 = y^2 - b\}$$

has cardinality p. (5 marks)

(d) Consider the elliptic curve E with Weierstrass equation

$$y^2 = x^3 + (5 \cdot 7 \cdot 11 \cdot 13 \cdot 17).$$

Show that the torsion subgroup of $E(\mathbb{Q})$ is trivial.

(5 marks)

(Total: 20 marks)

5. (a) Let p be an odd prime. Choose $a \in \mathbb{Z}_p$, such that $|a|_p = 1$ and that the reduction of a modulo p is not a square. Show that the set $\{1, p, a, pa\}$ is a set of coset representatives for $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

(5 marks)

(b) Let E be the elliptic curve over $\mathbb{Q}_{13}$ with equation

$$y^2 = x(x-13)(x-1).$$

Determine the order of $E(\mathbb{Q}_{13})/2E(\mathbb{Q}_{13})$.

(15 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2022

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

MATH70064/97043/97152

Number Theory: Elliptic Curves (Solutions)

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

seen ⇓

6, B

1. (a) We first consider the equation $Z^2 = aX^2 + bY^2$ over $\mathbb{F}_p$. As x varies over $\mathbb{F}_p$, the term $ax^2 + b$ takes $(p+1)/2$-values, as many as the squares in $\mathbb{F}_p$ (because $a \neq 0 \mod p$), so at least one of them is a square by the pigeonhole principle. Thus, there exists integers x, z such that

$$z^2 \equiv ax^2 + b \pmod{p}$$

Suppose that $p \nmid z$. The polynomial $f(T) = T^2 - (ax^2 + b) \in \mathbb{Z}_p[T]$ has derivative $f'(T) = 2T$, so

$$|f(z)|_p < |f'(z)|_p^2 = 1.$$

Then, by Hensel's Lemma, f has a root $z' \in \mathbb{Z}_p$ congruent to z modulo p. Then $[x : 1 : z']$ is a solution of the equation in $\mathbb{P}^2(\mathbb{Q}_p)$. On the other hand, if $p \mid z$, then $p \nmid x$, because $p \nmid b$. Then $g(T) = aT^2 + b - z^2$ satisfies

$$|g(x)|_p < |g'(x)|_p^2 = 1.$$

So again, by Hensel's Lemma, it admits a zero $x' \in \mathbb{Z}_p$, and $[x' : 1 : z]$ is a point of the conic in $\mathbb{P}^2(\mathbb{Q}_p)$.

seen ⇓

6, B

(b) Suppose that $p \mid\mid a$, $p \nmid b$ and that $Z^2 = aX^2 + bY^2$ has a solution $[x : y : z] \in \mathbb{P}^2(\mathbb{Q}_p)$. Without loss of generality, we can assume $\max(|x|_p, |y|_p, |z|_p) = 1$. If $|z|_p < 1$, then $|by^2|_p = |z^2 - ax^2|_p < 1$, so we would conclude that $|y|_p < 1$, but this implies that $p^2 \mid ax^2$, so $p \mid x$, contradicting the fact that the maximum of the norms is equal to 1. Reducing x, y, z mod p, we get a solution to

$$z^2 \equiv by^2 \pmod{p}$$

with z (hence y) non-zero. It follows that $(z/y)^2 = b \pmod{p}$, so b is a quadratic residue mod p.

Conversely, if b mod p is a quadratic residue, there exists an $z \in \mathbb{Z}$, $p \nmid z$, such that $z^2 = b \pmod{p}$. If we consider the polynomial $h(T) = T^2 - b$, we can again find a solution in $\mathbb{Z}_p$ by Hensel's Lemma; denote it by z'. Then $[0 : 1 : z']$ is a point of the conic in $\mathbb{P}^2(\mathbb{Q}_p)$.

seen ⇓

3, A

(c) Let $[x : y : z]$ be a solution of the equation of $Z^2 = aX^2 + bY^2$ with $a \equiv b \equiv 3 \pmod{4}$. As before, we can assume that the maximum of the 2-adic norms of x, y, z is equal to 1. Then the equation

$$0 \equiv z^2 - ax^2 - by^2 \equiv z^2 + x^2 + y^2 \pmod{4}$$

has a non-zero solution. Since squares are congruent to either 0 or 1 mod 4, this is a contradiction.

(d) We can proceed by trial and error, using the conditions we showed for the existence of solutions for an equation of the form $Z^2 = aX^2 + bY^2$. In order to have a non-zero real solution, either a or b must be positive, and if we choose $a \equiv b \equiv 3 \pmod 4$, we can assure that the equation will have no solutions over $\mathbb{Q}_2$. By Part (a), we deduce that 17 must divide ab. In addition, since we always have solutions for primes not dividing $2ab$, it is better to choose the equation so that ab has as few divisors as possible. So we can try $a = -17$, which is congruent to 3 mod 4, and want to choose a positive b such that $b = 3 \pmod 4$ so that b is not a quadratic residue mod 17. The value $b = 3$ works. It remains to check that the resulting conic has points over $\mathbb{Q}_3$; by (b) it suffices to check that -17 is a quadratic residue mod 3, which is true.

$\boxed{\text{unseen} \Downarrow}$

$\boxed{5, \text{D}}$

2. For these questions, multiple solutions are possible, either applying the Nagell-Lutz Theorem, or computing the group of points of the elliptic curves mod p for a prime p of good reduction.

meth seen ⇓

5, A

(a) Let E be the elliptic curve with equation $y^2 = x^3 - 11x + 14$. The discriminant is $\Delta = 4(-11)^3 + 27 \cdot 14^2 = 32 = 2^5$. For a prime p, let $\overline{E}_p$ be the cubic over $\mathbb{F}_p$ obtained by reducing the coefficients of the equation of E modulo p. For $p \nmid 2\Delta$, $\overline{E}_p$ is non-singular, and the restriction to the torsion subgroup of $E(\mathbb{Q})$ of the reduction map $\mathrm{red}_p \colon E(\mathbb{Q}) \to \overline{E}_p(\mathbb{F}_p)$ is injective. For $p = 3$, direct inspection shows that

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

Since the points of order 2 are precisely those whose y-coordinate vanishes, $\overline{E}_3(\mathbb{F}_3)$ is an abelian group of order 4 with only one element of order 2, so it must be cyclic.

5, A

On the other hand, we can observe that $P = (1,2)$ is a rational point of E. It follows that either P is 4-torsion, and then necessarily of order 4, because its y-coordinate is non-zero, or it has infinite order. The tangent line at P has equation is of the form $y = mx + c$, where $m = \frac{3x_P^2 - 11}{2y_P} = \frac{3 \cdot 1 - 11}{4} = -2$, so by the doubling formula,

$$x_{2P} = m^2 - 2x_P = 4 - 2 = 2.$$

By substituting the value of x_{2P} into the equation of E, we see that $y_{2P} = 0$. So we deduce that that $2P$ has order 2, that is, P has order 4. In particular, $E(\mathbb{Q})_{\mathrm{tors}}$ has a subgroup isomorphic to C_4. Because it embeds into a group isomorphic to C_4, it must be isomorphic to C_4 itself.

meth seen ⇓

5, A

(b) The discriminant of $E : y^2 = x^3 + 4$ is $\Delta = 27 \cdot 4^2 = 3^3 \cdot 2^4$. By the Nagell-Lutz Theorem, the torsion points must have integers coordinates (x, y) with $y = 0$ or $y^2 \mid \Delta$, that is $y \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6 \pm 12\}$. We first check for what values of y as above we get that the equation of E has an integral solution in x, that is $y^2 - 4$ is a cube. We see that the only possibilities are $(0, \pm 2)$. Thus, either $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial or it is cyclic of order 3.

5, A

The torsion subgroup is cyclic of order 3 if and only if the point $P = (0,2)$ is of inflection. The line $y = 2$ meets the cubic at P with multiplicity 3, so P has order 3, and $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to C_3. (Alternatively, one can compute the apply the doubling formula, and determine that $2P = -P$).

3. (a) The projective curve $\tilde{\mathcal{C}}$ is the zero-set of the homogeneous polynomial $F(U,V,W) = (U-V)^3 - UVW$. Taking partial derivatives

seen/sim.seen ⇓

6, A

$$\frac{\partial F}{\partial U} = 3(U-V)^2 - VW, \qquad \frac{\partial F}{\partial V} = -3(U-V)^2 - UW, \qquad \frac{\partial F}{\partial W} = UV,$$

we see that a singular point must satisfy $U = V = 0$, so $[0:0:1]$ is the unique singular point. Intersecting the cubic $\tilde{\mathcal{C}}$ with the line at infinity (of equation $W = 0$), we obtain the rational solution $\mathcal{O} = [1:1:0]$ with multiplicity 3, so $\mathcal{O}$ is a point of inflection.

seen/sim.seen ⇓

7, B

(b) If $P = (u,v) \in \tilde{\mathcal{C}}(\mathbb{Q})$ with $v = 0$, then $u = 0$, so the map is well-defined. Consider a projective line through the singular point. By Bézout's Theorem, it will meet the cubic at 3 points, counted with multiplicity and the intersection multiplicity at the singular point will be at least 2. A line through the singular point can be written as either $U = \lambda V$ for some $\lambda \in \mathbb{Q}$ or as $V = 0$; but in the latter case, the only point of intersection with the cubic is the singular point, so we can discard this case.

By substituting into the equation of $\tilde{\mathcal{C}}$ we get

$$(\lambda-1)^3V^3 - \lambda V^2W = V^2((\lambda-1)^3V - \lambda W) = 0$$

For $\lambda \notin \{0,1\}$, the solutions are given by the singular point with multiplicity 2, plus the affine point $(\frac{\lambda^2}{(\lambda-1)^3}, \frac{\lambda}{(\lambda-1)^3})$ with multiplicity 1. For $\lambda = 1$, we obtain the singular point with multiplicity 2, together with $\mathcal{O}$. Every $\lambda \in \mathbb{Q} \setminus 0$ is the image of a unique non-singular point under ψ; so ψ is a bijection.

seen/sim.seen ⇓

7, D

(c) First note that ψ preserves the identity element. Since $\mathcal{O}$ is a point of inflection, the group law on $\tilde{\mathcal{C}}(\mathbb{Q})^{\mathrm{ns}}$ satisfies the property that 3 points sum to zero if and only if there is a line intersecting the cubic precisely at those points (counted with multiplicity).

A line that does not pass through the singular point can be written in the form

$$W = aU + bV$$

for some $a, b \in \mathbb{Q}$. Substituting in the equation of the cubic we get

$$(U-V)^3 - UV(aU+bV) = 0$$

Since any non-singular point has non-zero V-coordinate, we can set $t = U/V$ and get

$$(t-1)^3 - t(at+b) = 0.$$

This is a monic polynomial with constant coefficient equal to -1, so the product of its roots is equal to 1. This is enough to show that ψ is a group homomorphism.

4. (a) A rational point of $E(\mathbb{Q})$ has order 2 if and only if its y-coordinate vanishes. So there is a point of order 2 if and only if $0 = x^3 + b$ has a rational solution, that is if $-b$, or equivalently b, is a cube.

seen/sim.seen ⇓

3, A

(b) Note that a point $P = (x_P, y_P)$ satisfies $3P = 0$ if and only if the tangent line at P meets the curve with multiplicity 3. The tangent line has the form $y = mx + c$, where $m = 3x_P^2/2y_P$. We can assume $y_P \neq 0$. Using the doubling formula, we can see that this gives

seen/sim.seen ⇓

7, C

$$3x_P = m^2 = 9x_P^4/4y_P^2 = 9x_P^4/4(x_P^3 + b),$$

which gives the pair of conditions

$$x_P(x_P^3 + 4b) = 0 \qquad \text{and} \qquad y_P^2 = x_P^3 + b$$

So we have either $x_P = 0$ or $x_P^3 = -4b$. In the former case, we get a solution for the second equation if and only if b is a square. In the latter case, $-4b$ is a cube, which means that $b = 2c^3$ for some integer c. Then the fact that $x_P^3 + b = -4b + b = -6c^3$ is a square implies that $c = -6d^2$, so that $b = -2^4 \cdot 3^3 d^6$. Since we are assuming that b is sixth-power-free, we get that $b = -2^4 \cdot 3^3 = -432$.

seen/sim.seen ⇓

5, C

(c) Note that if p is a prime and $p \equiv 2 \pmod 3$, the map $x \mapsto x^3$ is a bijection from $\mathbb{F}_p$ to itself. Indeed, the multiplicative group $\mathbb{F}_p^\times$ is cyclic of order $(p-1)$, so if $3 \nmid (p-1)$ the map $x \mapsto x^3$ is a group automorphism of $\mathbb{F}_p^\times$ and gives a bijection of sets on all of $\mathbb{F}_p$. So for each value in $y \in \mathbb{F}_p$, there is precisely one value of x such that $x^3 = y^2 - b$. Thus, the cardinality of the set is p.

seen/sim.seen ⇓

1, B

(d) The discriminant of E is $\Delta = 27b^2$, where $b = 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$. The torsion subgroup maps injectively into the group of $\mathbb{F}_p$-points of the reduction of E for every p of good reduction, that is $p \nmid 2\Delta$; thus, for $p \notin \{2, 3, 5, 7, 11, 13, 17\}$.

4, D

If we take a prime $p > 17$ and $p \equiv 2 \pmod 3$, the elliptic curve E will have good reduction at p, and its group of points over $\mathbb{F}_p$ will have order $(p+1)$ (from part (c), also accounting for the point at infinity). Applying this result to the primes 23 and 29, we obtain that the order of the torsion subgroup of $E(\mathbb{Q})$ must divide $(24, 30) = 6$. But from part (a) and (b), $E(\mathbb{Q})$ has no points of order 2 or 3, so the torsion subgroup must be trivial.

5. (a) Let $z \in \mathbb{Q}_p^\times$; then z can be written uniquely as $z = p^n u$ for some $u \in \mathbb{Z}_p^\times$. So a square is of the form $p^n u = p^{2m} v^2$ for $v \in \mathbb{Z}_p^\times$, which implies that its norm is an even power of p and the image of u in $\mathbb{F}_p^\times$ is a quadratic residue. The converse also holds: it suffices to check that every element of $u \in \mathbb{Z}_p^\times$ whose image in $\mathbb{F}_p^\times$ is a quadratic residue is a square in $\mathbb{Z}_p$, but this follows from Hensel's Lemma applied to the polynomial $f(T) = T^2 - u$. As a consequence, $z = p^n u$ and $z = p^m v$ with $u, v \in \mathbb{Z}_p^\times$ define the same class modulo squares if and only if n and m have the same parity and $\left(\frac{u}{p}\right) = \left(\frac{v}{p}\right)$, so $\{1, p, a, pa\}$ is a complete set of coset representatives.

$\boxed{\text{seen/sim.seen} \Downarrow}$

$\boxed{5, \text{M}}$

(b) By part (a), we can choose a set of coset representatives of $\mathbb{Q}_{13}^\times/(\mathbb{Q}_{13}^\times)^2$ as $\{1, 2, 13, 26\}$ since $\left(\frac{2}{13}\right) = -1$. Consider the map

$\boxed{\text{seen} \Downarrow}$

$\boxed{3, \text{M}}$

$$\delta\colon E(\mathbb{Q}_{13}) \to \left(\mathbb{Q}_{13}^\times/(\mathbb{Q}_{13}^\times)^2\right)^3$$

sending

$$\delta(x, y) = (x, x - 13, x - 1).$$

for an affine point (x, y) with $y \neq 0$. The points of order 2 of $E(\mathbb{Q}_{13})$ are $(0, 0)$, $(13, 0)$, $(1, 0)$. For points of order 2, only two of the coordinates $(x, x - 13, x - 1)$ give a well-defined value in $\mathbb{Q}_{13}^\times/(\mathbb{Q}_{13}^\times)^2$, but we can fill in the third entry by imposing that the product of the three is a square. So we let

$$\delta(0,0) = (13, 13, 1), \quad \delta(13, 0) = (13, 13, 1), \qquad \delta(1, 0) = (1, 1, 1), \quad \delta(\mathcal{O}) = (1, 1, 1).$$

The 2-descent method establishes that δ is a group homomorphism, with kernel $2E(\mathbb{Q}_p)$, and the image of δ is contained in the subgroup of triples $(b_1, b_2, b_3) \in \left(\mathbb{Q}_{13}^\times/(\mathbb{Q}_{13}^\times)^2\right)^3$ such that $b_1 b_2 b_3 = 1$. To determine the order of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ it suffices to compute the image of δ. Since the coordinate b_3 is determined by b_1 and b_2, it suffices to consider $4^2 = 16$ possibilities as (b_1, b_2) ranges in $\left(\mathbb{Q}_{13}^\times/(\mathbb{Q}_{13}^\times)^2\right)^2$. A triple (b_1, b_2, b_3) is the image of an affine point (x, y) under δ if and only if

$$\begin{cases} x = b_1 u^2 \\ x - 13 = b_2 v^2 \\ x - 1 = b_3 w^2 \end{cases}$$

for some $u, v, w \in \mathbb{Q}_{13}$. Eliminating x, we are left with determining for which (b_1, b_2, b_3), the system of equations

$$\begin{cases} b_1 u^2 - b_2 v^2 = 13 & (1) \\ b_1 u^2 - b_3 w^2 = 1 & (2) \end{cases}$$

has solutions in $\mathbb{Q}_{13}$. So we can represent the pairs (b_1, b_2) in a table, in which the columns correspond to b_1 and the rows to b_2

	1	2	13	26
1	✓			
2				
13			✓	
26				

where we write ✓ if the triple (b_1, b_2, b_3) is in the image of δ and × otherwise. We can complete the table in a few steps:

seen/sim.seen ⇓

4, M

(i) $13 \mid\mid b_1$ *and* $13 \nmid b_2$: we can set $u = U/Z$, $v = V/Z$ and $w = W/Z$ and consider the system of homogeneous equations

$$\begin{cases} b_1U^2 - b_2V^2 = 13Z^2 & (3) \\ b_1U^2 - b_3W^2 = Z^2. & (4) \end{cases}$$

Suppose that this has a solution $[U : V : W : Z] \in \mathbb{P}^3(\mathbb{Q}_{13})$; we can assume without loss of generality that the U, V, W, Z are in $\mathbb{Z}_{13}$ and at least one is a unit. Note that the assumptions imply that $13 \mid\mid b_3$. From (3), $13 \mid V$ and from (4), $13 \mid Z$. This then implies that $13^2 \mid b_1U$, so $13 \mid U$. Similarly, $13 \mid W$. Contradiction. So the pairs $(13, 1)$, $(13, 2)$, $(26, 1)$ and $(26, 2)$ are not in the image of δ.

(ii) $13 \mid\mid b_2$ *and* $13 \nmid b_1$: Since $(13, 13)$ is in the image of δ, and δ is a group homomorphism, we can conclude that the pairs of the form $(13b_1, 13b_2)$, with (b_1, b_2) as in (i), are not in the image of δ. We can fill in the table accordingly.

	1	2	13	26
1	✓		×	×
2			×	×
13	×	×	✓	
26	×	×		

seen/sim.seen ⇓

4, M

(iii) Let $b_1 = 2$ and $b_1 = 1$. As before, we can consider a system of homogeneous equations and look for solutions in $\mathbb{P}^3(\mathbb{Q}_{13})$. Equation (3) gives

$$2U^2 - V^2 = 13Z^2$$

which has no non-zero solutions over $\mathbb{Q}_{13}$, because 2 is not a quadratic residue mod 13. This implies that $U = V = Z = 0$; then it follows that $W = 0$, so there are no solutions in $\mathbb{P}^3(\mathbb{Q}_{13})$. So the triple $(2, 1, 2)$ is not in the image of δ. Since the image of δ is a group, neither is $(26, 13, 2)$. We can update the table.

	1	2	13	26
1	✓	×	×	×
2			×	×
13	×	×	✓	×
26	×	×		

unseen ⇓

4, M

(iv) $b_1 = b_2 = 2$. The system of equations becomes

$$\begin{cases} 2u^2 - 2v^2 = 13 & (5) \\ 2u^2 - w^2 = 1 & (6) \end{cases}$$

Choose $u = w = 1$, which solves (6). Then it suffices to find v solving (6), which is to say $v^2 = -11/2$, but $-11/2$ is in $1 + 13\mathbb{Z}_{13}$, so it is a square. It follows that $(2, 2, 1)$ is in the image of δ. Again, because the image of δ is a group, it follows that $(26, 26, 1)$ is also in the image of δ. Moreover, given that we have filled in all entries but two and that the order of the image must be a power of 2, we can conclude that no other triple is in the image and we can complete the table:

	1	2	13	26
1	✓	×	×	×
2	×	✓	×	×
13	×	×	✓	×
26	×	×	×	✓

Thus, the order of $E(\mathbb{Q}_{13})/2E(\mathbb{Q}_{13})$ is 4.

Review of mark distribution:

Total A marks: 32 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 12 of 12 marks
Total D marks: 16 of 16 marks
Total marks: 100 of 80 marks
Total Mastery marks: 20 of 20 marks

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 separate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
Elliptic Curves_MATH97043 MATH70064	1	This question was done very well on average. Some students struggled with part (d), which required to apply the criteria previously proved to find a conic with no points over some specific completions of the rationals. Some students did not choose the correct examples, or did not verify whether there actually were points over the other completions.
Elliptic Curves_MATH97043 MATH70064	2	This question was the most standard in the paper and was done almost universally correctly.
Elliptic Curves_MATH97043 MATH70064	3	Part (a) of this question was mostly done correctly. The students that attempted part (b) mostly did well. Few students realised that part (c) essentially required to check that if 3 points are collinear the product of their images under the map would be 1; even fewer manage to show it.
Elliptic Curves_MATH97043 MATH70064	4	Most students got partial marks on this question. Almost everyone got part (a) correctly, and most set up the correct calculation in part (b), but did not necessarily conclude the argument. Many students gave a more or less correct argument for part (c), though often more complicated than nessary. Most students understood that for part (d) one should use part (c) and the fact that the torsion subgroup would inject into the group of points over a finite field for a prime of good reduction, but many forgot to add the point at infinity when applying the previous part.
Elliptic Curves_MATH97043 MATH70064	5	This was by far the most difficult question. Many students did not attempt part (a) or did not give a correct argument. For part (b), many applied the 2-descent method over Q instead of over the given p-adic field. Only very few set up the question correctly, and even attempted to argue the existence of points in any of the possible cases.