Imperial College
London

MATH70064

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2023

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

Elliptic Curves

Date: 30 May 2023

Time: 14:00 – 16:30 (BST)

Time Allowed: 2.5hrs

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

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

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

- **You may use any results from the lectures, or other references, provided that you state them clearly or refer to them precisely.**
- **Any unjustified answer, regardless of it being correct or not, will be given zero mark.**

1. (a) Consider the polynomial $P(x) = x^3 + x + 1$ with coefficients in $\mathbb{Q}_3$.

   (i) Prove that any root of P in $\mathbb{Q}_3$ is a 3-adic unit *i.e.* belongs to $\mathbb{Z}_3^\times$. (2 marks)

   (ii) Determine the number of roots (counted with multiplicities) of P in $\mathbb{Q}_3$. (4 marks)

   (iii) Does P have rational roots *i.e.* belonging to $\mathbb{Q}$? Justify your answer. (2 marks)

   (b) Let p be a prime number. Find all $x \in \mathbb{Q}_p$ such that $\sum_{n\geq 1} \frac{x^n}{n^n}$ converges in $\mathbb{Q}_p$. (6 marks)

   (c) Let p be a prime number. Prove that $\mathbb{Z}_p$ is uncountable as a set.
   Hint: show it contains a set in bijection with the uncountable set:

$$\{0,1\}^{\mathbb{Z}_{\geq 0}} = \{(a_n)_{n\in\mathbb{Z}_{\geq 0}} \mid a_n \in \{0,1\}\}.$$

(6 marks)

(Total: 20 marks)

2. Consider the projective plane conic:

$$X^2 - 11Y^2 + 5Z^2 = 0.$$

   (a) Determine whether it has a point over the following completions:

   (i) $\mathbb{Q}_5$ (4 marks)

   (ii) $\mathbb{Q}_{11}$ (4 marks)

   (iii) $\mathbb{Q}_2$ (4 marks)

   (iv) all other completions of $\mathbb{Q}$ (4 marks)

   (b) Determine whether the conic has a rational solution. (4 marks)

(Total: 20 marks)

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

(a) $E : y^2 = x^3 + x + 1$ (10 marks)

(b) $E : y^2 = x^3 + 2023^{2022}x + 2022^{2023}$
Prime factorisation help: $2022 = 2 \cdot 3 \cdot 337$ *and* $2023 = 7 \cdot 17^2$ (10 marks)

(Total: 20 marks)

4. Let $a \in \mathbb{Z}_{\geq 0}$. Consider the cubic $E_a : y^2 = x^3 - x^2 - a^2x + a^2$ over $\mathbb{Q}$.

(a) Show that E_a is an elliptic curve if and only if $a \geq 2$. (2 marks)

(b) Assume $a \geq 2$.

(i) Find at least 6 points of $E_a(\mathbb{Q})$. (3 marks)

(ii) Let $P = (x_0, y_0) \in E_a(\mathbb{Q})$. If $y_0 \neq 0$, prove that $2 \cdot P = (x_{2P}, y_{2P})$ satisfies the formula:

$$x_{2P} = 1 - 2x_0 + \alpha^2 \text{ with } \alpha = \frac{3x_0^2 - 2x_0 - a^2}{2y_0}.$$

Computation help:

$$x^3 - x^2 - a^2x + a^2 = (x - x_0)^3 + (3x_0 - 1)(x - x_0)^2 + \dots.$$

(2 marks)

(c) Assume $a \geq 2$. Set $A_a = -27 \cdot (3a^2 + 1)$, $B_a = 27 \cdot (18a^2 - 2)$ and $\Delta_a = 4A_a^3 + 27B_a^2$.

(i) Show that $E'_a : y^2 = x^3 + A_ax + B_a$ can be deduced from E_a by a change of variables via a rational map you will make explicit. (3 marks)

(ii) Prove this rational map induces a group isomorphism $E_a(\mathbb{Q}) \simeq E'_a(\mathbb{Q})$. (4 marks)

(iii) Prove that $5 \mid \Delta_a$ if and only if a is a square mod 5. (3 marks)

(iv) Deduce that $E_a(\mathbb{Q})_{\text{tors}}$ has order 4 or 8 when a is not a square mod 5. (3 marks)

(Total: 20 marks)

5. Consider the elliptic curve $E : y^2 = x^3 - 351x + 1890$ whose discriminant is $\Delta = -2^8 \cdot 3^{14}$ and whose 2-torsion points are:

$$E[2] = \{\mathcal{O}, (24, 0), (6, 0), (-30, 0)\}.$$

Assuming $E(\mathbb{Q})_{\text{tors}} = E[2]$ and $(-3, \pm 81) \in E(\mathbb{Q})$, compute the rank of E. (20 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2023

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

MATH70064

Elliptic Curves (Solutions)

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

1. (a) (i) Let $\alpha \in \mathbb{Q}_3$ be a root of $P(x) = x^3 + x + 1$. Then $\alpha^3 + \alpha + 1 = 0$ so $\alpha(1 + \alpha^2) = -1$. Taking the 3-adic norm we obtain $|\alpha|_3 \times |1 + \alpha^2|_3 = 1$. Recall that $|x + y|_3 = |x|_3$ if $|x|_3 > |y|_3$. If $\alpha \in 3\mathbb{Z}_3$ then $|\alpha|_3 < 1$ and $|1 + \alpha^2|_3 = 1$. If $\alpha \notin \mathbb{Z}_3$, then $|\alpha|_3 > 1$ and it implies $|1 + \alpha^2|_3 = |\alpha^2|_3 > 1$. As a result $|\alpha|_3 \times |1 + \alpha^2|_3 = 1$ holds only if $|\alpha|_3 = 1$ *i.e.* $\alpha \in \mathbb{Z}_3^\times$.

seen ⇓

2, A

(ii) We will apply the strong version of Hensel's lemma we have seen during the lecture. First of all, if α is a root of P it reduces to a non-zero root modulo 3 as $\alpha \in \mathbb{Z}_3^\times$. So the number of roots of P modulo 3 is greater or equal to the number of roots of P in $\mathbb{Z}_3$. Consider $\bar{P}(x) = x^3 + x + 1$ over $\mathbb{F}_3$. It factors as $(x - 1)(x^2 + x - 1)$ where $x^2 + x - 1$ has no roots in $\mathbb{F}_3$ so it is irreducible in $\mathbb{F}_3[x]$. As a result of this factorisation, we already know that P has at most one root (coutend with multiplicities) in $\mathbb{Z}_3$. Applying Hensel's lemma with $\bar{P}(1) = 0$ and $\bar{P}'(1) = 3 \cdot 0^2 + 1 = 1 \neq 0$, we know that there exists a unique $t \in 1 + 3\mathbb{Z}_3$ such that $P(t) = 0$. Therefore P has a unique root in $\mathbb{Q}_3$ and it is multiplicity one.

seen ⇓

4, A

(iii) Assume that P has a rational root t and write it in reduced form $t = \frac{a}{b}$ where a and b are coprime integers. Then $(\frac{a}{b})^3 + \frac{a}{b} + 1 = 0$ implies that $a^3 + ab^2 + b^3 = 0$ *i.e.* $a^3 = -b^2(a + b)$ and by coprimality we must have $b = \pm 1$. Similarly $a = \pm 1$. But 1 and -1 are not roots of P, so it does not admit any rational root.

seen ⇓

2, A

(b) We have seen during the lecture that a series $\sum_n a_n$ for $a_n \in \mathbb{Q}_p$ is converging if and only if $a_n \to 0$. Here we need to check for which $x \in \mathbb{Q}_p$ we have $a_n = \frac{x^n}{n^n}$ converges to 0 *i.e.* $|a_n|_p \to 0$. Assume $x \neq 0$, then there exists $k \in \mathbb{Z}_{\geq 0}$ and u a p-adic unit such that $x = p^k u$. We are going to prove that a_n does not converge to 0. Indeed for $m \in \mathbb{Z}_{\geq 0}$ we have

$$|a_{p^m}|_p = \left| \frac{(p^k)^{p^m} u^{p^m}}{(p^m)^{p^m}} \right|_p = p^{(-k+m)p^m}.$$

Therefore $|a_{p^m}|_p \to +\infty$ when $m \to +\infty$. As a result $\sum_{n \geq 1} \frac{x^n}{n^n}$ does not converege when $x \neq 0$. Of course, it does converge when $x = 0$ as it is simply 0.

sim. seen ⇓

6, B

(c) We are going to use the p-adic expansion. As we have seen during the lectures, there is a correspondence between p-adic expansions and p-adic integers, resulting in a bijection:

$$(a_n)_{n \in \mathbb{Z}_{\geq 0}} \in \{0, \ldots, p-1\}^{\mathbb{Z}_{\geq 0}} \mapsto \sum_{n \geq 0} a_n p^n \in \mathbb{Z}_p.$$

So it is sufficient to prove that sequences in $\{0, \ldots, p-1\}$ is an uncountable set. We can use a method similar to Cantor's diagonal argument or simply remark that it contains the uncountable set $\{0, 1\}^{\mathbb{Z}_{\geq 0}} \subset \{0, \ldots, p-1\}^{\mathbb{Z}_{\geq 0}}$. The latter set is indeed uncountable as this is the power set of the integers $\mathcal{P}(\mathbb{Z}_{\geq 0}) = \{0, 1\}^{\mathbb{Z}_{\geq 0}}$.

unseen ⇓

6, D

2. The projective plane conic $X^2 - 11Y^2 + 5Z^2 = 0$.

sim. seen ⇓

4, A

(a) (i) There is a solution in $\mathbb{P}^2(\mathbb{Q}_5)$. Indeed consider the polynomial $f(x) = x^2 - 11$ in $\mathbb{Q}_5[x]$. We have over $\mathbb{F}_5$ that $\bar{f}(1) = 1^2 - 1 = 0$ and $\bar{f}'(1) = 2 \cdot 1 = 2 \neq 0$, so the strong version of Hensel's lemma applies: there exists (a unique) $t \in 1 + 5\mathbb{Z}_5$ such that $f(t) = 0$. Therefore $[t : 1 : 0]$ is a $\mathbb{Q}_5$-point of the conic.

sim. seen ⇓

4, A

(ii) There is no solution in $\mathbb{Q}_{11}$. Indeed, if there was one in $\mathbb{P}^2(\mathbb{Q}_{11})$, we can assume it can be written as $[a : b : c]$ where a, b and c are 11-adic integers and at least one of them is a 11-adic unit. If a and c are not 11-adic units, then y must be. However, this implies $|a^2 - 11b^2 + 5c^2|_{11} = |11b^2|_{11} = 11^{-1} \neq 0$ which is a contradiction. So at least one of a or c is a unit. But applying a similar argument on norms we see that actually both a and c must be units. In particular they reduce to a non-zero solution $[a_0 : b_0 : c_0] \in \mathbb{P}^2(\mathbb{F}_{11})$ with $a_0 \neq 0$ and $c_0 \neq 0$ of $X^2 + 5Z^2 = 0$. In particular $a_0 c_0^{-1}$ must be a root of $x^2 + 5 = x^2 - 6$. But $\mathbb{F}_{11}^{\times 2} = \{1, 3, 4, 5, 9\}$ so 6 is not a square in $\mathbb{F}_{11}$ and $a_0 c_0^{-1}$ can be a root of 6. Therefore there is no solution $[a : b : c]$ in $\mathbb{P}^2(\mathbb{Q}_{11})$ to $X^2 - 11Y^2 + 5Z^2 = 0$.

sim. seen ⇓

4, B

(iii) There are no solutions in $\mathbb{Q}_2$. Indeed if $[a : b : c] \in \mathbb{P}^2(\mathbb{Q}_2)$ is a solution with a, b and c being 2-adic integers and at least one is a unit, then we should get a non-zero solution $[a_0 : b_0 : c_0]$ with coefficients in $\mathbb{Z}/4\mathbb{Z}$ to the projective conic $X^2 - 11Y^2 + 5Z^2 = X^2 + Y^2 + Z^2$. But for all $x \in \mathbb{Z}/4\mathbb{Z}$, we have $x^2 = 0$ or $x^2 = 1$. Therefore there does not exist a_0, b_0 and c_0 in $\mathbb{Z}/4\mathbb{Z}$ not all zero such that $a_0^2 + b_0^2 + c_0^2 = 0$. So there is no solution to $X^2 - 11Y^2 + 5Z^2$ in $\mathbb{Q}_2$.

sim. seen ⇓

4, B

(iv) There exist obvious solutions in $\mathbb{P}^2(\mathbb{R})$, for instance $[\sqrt{11} : 1 : 0]$ will be a real point of the conic. There remains to check other completions of $\mathbb{Q}$, that is for p-adic fields $\mathbb{Q}_p$ when p does not divide $2 \cdot 5 \cdot 11$.

The polynomial $11y^2 - 5$ in $\mathbb{F}_p[y]$ takes $\frac{p+1}{2} = \frac{p-1}{2} + 1$ different values because $11b^2 - 5 = 11(b')^2 - 5$ if and only if $b = \pm b'$. The same is true for x^2 in $\mathbb{F}_p[x]$ which also takes $\frac{p+1}{2} = \frac{p-1}{2} + 1$ different values. By the pigeonhole principle we see that the set $\{11b^2 - 5 \mid b \in \mathbb{F}_p\}$ must meet $\{a^2 \mid a \in \mathbb{F}_p\}$ as they both contain $\frac{p+1}{2}$ elements and $|\mathbb{F}_p| = p$. Set $11b_0^2 - 5 = b_1^2$ for this element where $b_0, b_1 \in \mathbb{F}_p$. Note that either $b_0 \neq 0$ or $b_1 \neq 0$ as $5 \neq 0$ in $\mathbb{F}_p$. Lift them arbitrarily to $\mathbb{Z}_p$ as b_0' and b_1'.

If $b_1 \neq 0$, then Hensel's lemma applies to $P(T) = T^2 - (11(b_0')^2 - 5)$ in $\mathbb{Z}_p[T]$ because $P(b_1) = 0$ and $P'(b_1) = 2b_1 \neq 0$ in $\mathbb{F}_p$. So there exists $t \in \mathbb{Z}_p$ such that $P(t) = 0$ and $[t : b_1' : 1]$ is a solution in $\mathbb{P}^2(\mathbb{Q}_p)$.

If $b_0 \neq 0$, then apply Hensel's lemma to $Q(T) = 11T^2 - (5 + (b_1')^2)$ to get a root $t \in \mathbb{Z}_p$ of Q such that $[b_1' : t : 1]$ is as solution in $\mathbb{P}^2(\mathbb{Q}_p)$.

meth seen ⇓

4, A

(b) By Hasse principle for conics, there is a rational solution if and only if there are solutions for all completions of $\mathbb{Q}$. But there is no solution for the completions $\mathbb{Q}_{11}$ and $\mathbb{Q}_2$, so there is no rational solution of the conic.

3. (a) The discriminant of $y^2 = x^3 + x + 1$ is $\Delta = 4 \cdot 1^3 + 27 \cdot 1^2 = 31$ and this is a prime number. Applying Nagell-Lutz theorem, we know that any torsion point different from the point at infinity $\mathcal{O}$ is of the form $(x, y) \in E(\mathbb{Q})$ with x, y integers and either $y = 0$ or $y^2 \mid \Delta$. As a result of Δ being prime, the only possibilities are $y \in \{0, \pm 1\}$. When $y = 0$, we must consider the roots of the polynomial $P(x) = x^3 + x + 1$, which has no integer roots because the funciton $x \mapsto P(x)$ is strictly increasing and we have $P(-1) = -1$ and $P(0) = 1$. When $y = 1$ (the case $y = -1$ is symmetric) we are left to solve $x^3 + x = x(x^2 + 1) = 0$ which has roots 0 and $\pm i$ in $\mathbb{C}$. Hence $P = (0, 1) \in E(\mathbb{Q})$ as well as $-P = (0, -1)$ are the only cadidates for non-trivial torsion points. By the doubling formula we have $2 \cdot P = (1/4, -9/8)$. So $2 \cdot P$ is not a point torsion by the contraposed of Nagell-Lutz and this implies that P itself is not torsion. Also $-P$ is torsion if and only if P is, so both are not torsion points. Therefore the torsion subgroup is the trivial group.

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

$\boxed{10, \text{A}}$

(b) The discriminant $\Delta = 4 \cdot A^3 + 27 \cdot B^2$ of $y^2 = x^3 + Ax + B$ with $A = 2023^{2022}$ and $B = 2022^{2023}$ is too big to be computed by hand. However, one can see that some small primes do not divide Δ *e.g.* we have:

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

$\boxed{10, \text{C}}$

- $A \equiv 1 \mod 3$ and $B \equiv 0 \mod 3$
  so $\Delta \equiv 1 \mod 3$
- $A \equiv 3^{2022} \equiv (-1)^{1011} \equiv -1 \equiv 4 \mod 5$ and $B \equiv (-3)^{2023} \equiv 3 \mod 5$
  so $\Delta \equiv 4 \mod 5$

Now, we can use the following result that was proved during the lectures: if p does not divide 2Δ, we have an injective group morphism $E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_p)$.

On the one hand apply it for $p = 3$. The equation becomes $y^2 = x^3 + x$ over $\mathbb{F}_3$.

x	0	1	2
$x^3 + x$	0	2	1
$\#y$	1	0	2

Adding the point at infinity we have $E(\mathbb{F}_3) = 4$.

On the other hand when $p = 5$ the equation becomes $y^2 = x^3 + 4x + 3$ over $\mathbb{F}_5$.

x	0	1	2	3	4
$x^3 + 4x + 3$	3	3	4	2	3
$\#y$	0	0	2	0	0

Adding the point at infinity we have $|E(\mathbb{F}_5)| = 3$.

As $E(\mathbb{Q})_{\text{tors}}$ is a subgroup of both $E(\mathbb{F}_3)$ and $E(\mathbb{F}_5)$, its order divides $\gcd(4, 3) = 1$. Therefore $|E(\mathbb{Q})_{\text{tors}}| = 1$ and $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$ is the trivial group.

seen ⇓

2, A

4. (a) For $g(x) \in \mathbb{Q}[x]$, the cubic curve $y^2 = g(x)$ is an elliptic if and only if the cubic is non-singular, which is equivalent over $\mathbb{Q}$ (according to the lecture notes) to the fact that $g(x)$ has no repeated roots. Here $x^3 - x^2 - a^2x + a^2 = (x-1)(x-a)(x+a)$, so the roots 1, a and $-a$ are all distinct if $a \geq 2$. In other cases the polynomial above has repeated roots. Indeed, when $a = 0$ the root 0 has multiplicity 2 and when $a = 1$ the root 1 has multiplicity 2.

sim. seen ⇓

3, B

(b) (i) There are obvious affine points $\{(1,0),(a,0),(-a,0),(0,a),(0,-a)\}$ on the elliptic curve. They are all different because $a \geq 2$. To find a 6-th point point one can add to these five the point at infinity $\mathcal{O} = [0:1:0]$.

meth seen ⇓

2, C

(ii) The equation of the tangent at $P = (x_0, y_0)$ is:

$$2y_0(y - y_0) = 3x_0^2(x - x_0) - 2x_0(x - x_0) - a^2(x - x_0).$$

It gives $y = \alpha(x - x_0) + y_0$ where $\alpha = \frac{3x_0^2 - 2x_0 - a^2}{2y_0}$ since $y_0 \neq 0$. Now replacing in the equation of the curve, we are having:

$$(\alpha(x - x_0) + y_0)^2 = x^3 - x^2 - a^2x + a^2$$

and simplifying the equation the term $x - x_0$ will appear with multiplicity at least 2 and the remaining root in the degree 1 factor defines x_{2P} (possibly it can be x_0 itself if P is an inflexion point). According to the computational help, we can ignore the term in $x - x_0$ of degree striclty less than 2 therefore we have the equation:

$$\alpha^2(x - x_0) = (x - x_0)^3 + (3x_0 - 1)(x - x_0)^2.$$

We eventually find that $\alpha^2 = x_{2P} - x_0 + 3x_0 - 1$ *i.e.* $x_{2P} = 1 - 2x_0 + \alpha^2$.

unseen ⇓

3, D

(c) (i) First of all, we want to find a change of variables so that the elliptic curve has the form $y^2 = x^3 + Ax + B$ with A and B in $\mathbb{Q}$. Then by another change of variables (u^2x, u^3y) for $u \in \mathbb{Q}$, which preserves the latter type of equations, will give us coefficients in $\mathbb{Z}$.

In $x^3 - x^2 - a^2x + a^2$, we would like to get rid of the coefficients in x^2. Completing the cube, we obtain:

$$x^3 - x^2 - a^2x + a^2 = (x - \frac{1}{3})^3 - \frac{1}{3}x + \frac{1}{27} - a^2x + a^2.$$

Introducing $x - \frac{1}{3}$ above we get:

$$\begin{aligned} x^3 - x^2 - a^2x + a^2 &= (x - \frac{1}{3})^3 - \frac{1+3a^2}{3}(x - \frac{1}{3}) + a^2 + \frac{1}{27} - \frac{1+3a^2}{9} \\ &= (x - \frac{1}{3})^3 - \frac{1+3a^2}{3}(x - \frac{1}{3}) + \frac{18a^2 - 2}{27} \end{aligned}$$

Now a change of variables $(3^2x, 3^3y)$ will absorb the numerators. So the change of variables which transforms E_a in E'_a comes from the rational map $(x,y) \mapsto (3^2(x - \frac{1}{3}), 3^3y) = (9x - 3, 27y)$.

unseen ⇓

4, D

(ii) First of all the map $(x, y) \in E_a(\mathbb{Q}) \mapsto (9x - 3, 27y) \in E'_a(\mathbb{Q})$ is a bijection because its inverse is $(u, v) \mapsto (\frac{1}{9}(u + 3), \frac{1}{27}v)$ and the change of variables preserves the point at infinity (homogenising both equations and writing the map in projective coordinates we see it leaves $[0 : 1 : 0]$ unchanged). There remains to prove that this map is a group morphism. But the group law is characterised by the fact that $P + Q + R = \mathcal{O}$ when P, Q and R are aligned. But the change of variables is an affine transformation so it clearly preserves straight lines. Therefore the images of P, Q and R are again aligned and the map is a group morphism.

sim. seen ⇓

3, B

(iii) We have $\Delta_a = 4A_a^3 + 27B_a^2$. As both A_a and B_a can be divided by 27, which is prime to 5, it is equivalent to consider when 5 divides or not the integer $(3a^2 + 1)^3 + (18a^2 - 2)^2$. Leading the computation modulo 5 we have on the one hand:

$$(3a^2 + 1)^3 = 2a^6 + 2a^4 + 4a^2 + 1 = 2a^4 + a^2 + 1$$

because $a^5 = a$ in $\mathbb{F}_5$. On the other hand $(18a^2 - 2)^2 = 4a^4 + 3a^2 + 4$. Therefore:

$$(3a^2 + 1)^3 + (18a^2 - 2)^2 = 6a^4 + 4a^2 = a^4 - a^2 = a^2(a^2 - 1).$$

As a result $5 \mid \Delta_a$ if and only if $a^2(a^2 - 1) \equiv 0 \mod 5$. The latter condition is equivalent to a being congruent to one of the elements $\{0, 1, -1\}$, which are all the squares in $\mathbb{F}_5$.

part seen ⇓

3, D

(iv) When a is not a square modulo 5, we know by the previous question that 5 does not divide Δ_a. Therefore we can apply the result already mentioned in Question 3(b) above: as 5 does not divide $2\Delta_a$, we have an embedding of groups $E'_a(\mathbb{Q})_{\mathsf{tors}} \hookrightarrow E(\mathbb{F}_5)$. As a is not a square modulo 5, we have $a^2 \equiv -1 \mod 5$. So reducing the equation of E'_a modulo 5 gives $y^2 = x^3 + 4x$. We write $x^3 + 4x = x^3 - x$ for simplicity. Now:

x	0	1	2	3	4
$x^3 - x$	0	0	1	1	0 .
$\#y$	1	1	2	2	1

so $|E'_a(\mathbb{F}_5)| = 8$. We deduce that $|E'_a(\mathbb{Q})_{\mathsf{tors}}|$ divides 8. But the group isomorphism above tells us that $E'_a[2] = \{\mathcal{O}, (9a - 3), (6, 0), (-9a - 3, 0)\}$ so the 2-torsion of E'_a is rational. Therefore $4 \leq |E'_a(\mathbb{Q})_{\mathsf{tors}}|$ and we obtain that the torsion subgroup of $E'_a(\mathbb{Q})$ has either order 4 or 8. Group isomorphism preserves torsion subgroups, so the same holds for the torsion in $E_a(\mathbb{Q})$.

meth seen ⇓

8, M

5. By assumption, we know that the 2-torsion is rational because $|E[2]| = 4$. Consider:

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

defined by $\delta(x, y) = (x - e_1, x - e_2) = (x - 24, x - 6)$ if $y \neq 0$ and:

$$\delta(\mathcal{O}) = (1, 1)$$

$$\delta(24, 0) = (3, 2)$$

$$\delta(6, 0) = (-2, -2)$$

$$\delta(-30, 0) = (-6, -1)$$

The map δ is a group morphism. By assumption we have $(-3, 81) \in E(\mathbb{Q})$ and it must be a non torsion point because $E(\mathbb{Q})_{\text{tors}} = E[2]$. So the rank of $E(\mathbb{Q})$ is at least 1. Its image through δ is:

$$\delta(-3, 81) = (-3 - e_1, -3 - e_2) = (-27, -9) = (-3, -1).$$

Moreover we are given $\Delta = -2^8 \cdot 3^{14}$, so the image of δ is contained in the set of pairs $(a, b) \in \mathbb{Q}(S, 2)^2$ where $\mathbb{Q}(S, 2) = \{\pm1, \pm2, \pm3, \pm6\}$. We apply the descent method to determine the image of δ by ruling out some couples $(b_1, b_2) \in \mathbb{Q}(S, 2)^2$.

First we observe that $y^2 = (x - 24)(x - 6)(x + 30)$ and :

$$x - 24 = b_1u^2 < x - 6 = b_2v^2 < x + 30 = b_1b_2w^2.$$

In order for the product to be a square, we must have that b_1 and b_2 have same sign. We represent the pairs (b_1, b_2) in the table with ✓ the subgroup of order 8 generated by the images of δ above:

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

Now in order to rule out some couples, we try to prove that the intersection of quartics below has no rational points:

$$\begin{cases} b_2v^2 - b_1u^2 = -6 + 24 = 18 \\ b_1b_2w^2 - b_2v^2 = 30 - 6 = 36 \end{cases}$$

sim. seen ⇓

4, M

1. let $(b_1, b_2) = (1, 3)$, then homogenising the equation:

$$\begin{cases} 3V^2 - U^2 = 18Z^2 & (1) \\ 3W^2 - 3V^2 = 36Z^2 & (2) \end{cases}$$

and assuming U, V, W, Z are coprime integers, we have by (I) that $3 \mid U$. But then $9 \mid 3V^2$ so $3 \mid V$. By (2) it implies $3 \mid W$. Therefore $27 \mid 36Z^2$ so $3 \mid Z$. We get a contradiction, so this couple has to be ruled out. We have just been using the fact that $3 \mid b_2$ but not b_1, so more couples can be ruled out (see the $\times_1$ in the table below). We can also eliminate all couples obtained by multiplying by admissible couples ✓ (see the $\times_{1'}$ in the table).

	1	2	3	6	-1	-2	-3	-6
1	✓		$\times_1$	$\times_1$	$\times$	$\times$	$\times$	$\times$
2	✓		$\times_1$	$\times_1$	$\times$	$\times$	$\times$	$\times$
3		✓	$\times_{1'}$	$\times_{1'}$	$\times$	$\times$	$\times$	$\times$
6		✓	$\times_{1'}$	$\times_{1'}$	$\times$	$\times$	$\times$	$\times$
-1	$\times$	$\times$	$\times$	$\times$		✓	$\times_1$	$\times_1$
-2	$\times$	$\times$	$\times$	$\times$		✓	$\times_1$	$\times_1$
-3	$\times$	$\times$	$\times$	$\times$	✓		$\times_{1'}$	$\times_{1'}$
-6	$\times$	$\times$	$\times$	$\times$	✓		$\times_{1'}$	$\times_{1'}$

There are 16 possibilities left.

unseen ⇓

4, M

2. let $(b_1, b_2) = (1, 2)$, then homogenising:

$$\begin{cases} 2V^2 - U^2 = 18Z^2 & (1) \\ 2W^2 - 2V^2 = 36Z^2 & (2) \end{cases}$$

All U, V, W can't be zero at the same time. However, there is no solution such that $U = V = W = 0$ because it would imply $Z = 0$ therefore $(0, 0, 0, 0)$ does not define a point in $\mathbb{P}^3(\mathbb{Q})$. Equating $2{\cdot}(1)$ and (2) we get:

$$4V^2 - 2U^2 = 2W^2 - 2V^2 \text{ i.e. } 3V^2 - U^2 - W^2 = 0.$$

We are intereseted in solutions of the latter conic in $\mathbb{P}^2(\mathbb{Q})$. Because, U, V and W can't be zero all at the same time, so it defines a rational projective point for $3V^2 - U^2 - W^2 = 0$. But the latter conic has no $\mathbb{Q}_2$-points (because similarly to 4(a)(iii) we have $3a^2 - b^2 - c^2 = 3(a^2 + b^2 + c^2) \neq 0$ in $\mathbb{Z}/4\mathbb{Z}$ if a, b, c are not all zeros) and no $\mathbb{Q}_3$-points (because -1 is not a square in $\mathbb{F}_3$). We can rule out $(1, 2)$ so the image of δ has order a power of 2, is a multiple of 8 and is less than 15, therefore it is 8.

	1	2	3	6	-1	-2	-3	-6
1	✓	$\times_2$	$\times_1$	$\times_1$	$\times$	$\times$	$\times$	$\times$
2	✓	$\times_{2'}$	$\times_1$	$\times_1$	$\times$	$\times$	$\times$	$\times$
3	$\times_{2'}$	✓	$\times_{1'}$	$\times_{1'}$	$\times$	$\times$	$\times$	$\times$
6	$\times_{2'}$	✓	$\times_{1'}$	$\times_{1'}$	$\times$	$\times$	$\times$	$\times$
-1	$\times$	$\times$	$\times$	$\times$	$\times_{2'}$	✓	$\times_1$	$\times_1$
-2	$\times$	$\times$	$\times$	$\times$	$\times_{2'}$	✓	$\times_1$	$\times_1$
-3	$\times$	$\times$	$\times$	$\times$	✓	$\times_{2'}$	$\times_{1'}$	$\times_{1'}$
-6	$\times$	$\times$	$\times$	$\times$	✓	$\times_{2'}$	$\times_{1'}$	$\times_{1'}$

meth seen ⇓

4, M

We deduce that the image of δ has order 8. But by Mordell-Weil theorem it has also order 2^{t+r} where r is the rank of the elliptic curve and 2^t is the order of $E[2]$. As $t = 2$, we deduce that $r = 1$ *i.e.* the rank of E is 1.

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.

ExamModuleCode	**QuestionNumber**	**Comments for Students**
MATH70064	1	Question on the p-adic numbers, mostly well answered
MATH70064	2	Question very similar to the coursework, many students got high marks
MATH70064	3	Classical question, with the methodology explained during the course
MATH70064	4	Rational points on an elliptic curves and change of coordinates, not so well answered
MATH70064	5	Two descent method with rational 2-torsion, most students were aware of the 2-descent with various levels of mastery