Honour School of Mathematics Part C: Paper C3.7
Master of Science in Mathematical Sciences: Paper C3.7

Elliptic Curves
James Newton
Draft solutions

08/03/2024

Do not turn this page until you are told that you may do so

1. (a) [6 marks] (i) State Hensel's lemma.
   (ii) Let $a \in \mathbb{Q}_7^\times$. Show that a has a cube root in $\mathbb{Q}_7$ if and only if $a = 7^n u$ with $n \in \mathbb{Z}$ divisible by 3, and $u \in \mathbb{Z}_7$ with $u \equiv \pm 1 \mod 7$.

   (b) [19 marks] Consider the elliptic curve with (projective) equation

$$\mathcal{C} : X^3 + Y^3 = 2Z^3$$

   and distinguished identity point $(1 : -1 : 0) \in \mathcal{C}(\mathbb{Q})$.
   (i) For a point $P = (x_1 : y_1 : 1)$ of $\mathcal{C}$, find a formula for the doubled point $2P$ in terms of rational functions in x_1 and y_1.
   [*You may find it useful to note that the tangent line to* $\mathcal{C}$ *at* $(1 : -1 : 0)$ *has equation* $X + Y = 0$.]
   (ii) What are the 2-torsion points of $\mathcal{C}(\mathbb{Q}_7)$?
   (iii) By considering your formula for $2P$, or otherwise, show that $\mathcal{C}(\mathbb{Q}_7)$ contains no point P of order 4.
   [*You may assume without proof that the points in* $\mathcal{C}(\mathbb{Q}_7) \cap \{Z = 0\}$ *do not have order* 4.]

Solution 1.

(a)(i) [Bookwork, 2 marks] Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leqslant 1\}$.
Let $f(x) \in R[x]$ and let $a_0 \in R$ satisfy $|f(a_0)| < |f'(a_0)|^2$. Then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| < |f'(a_0)|$. This solution moreover satisfies $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$.
[*Also acceptable to drop the 'moreover' part, or state that there exists a unique solution* a *with* $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$, *or state the special case with* $|f'(a_0)| = 1$.]

(a)(ii) [Easy seen similar, 4 marks] Suppose we have $\alpha^3 = a$. First we consider the 7-adic valuation of both sides. This tells us that $|a|_7 = 7^{-n}$ for $n \in \mathbb{Z}$ divisible by 3. Setting $u = 7^{-n}a$, we compute $|u|_7 = 1$ and $a = 7^n u$ as required. Now it remains to show that $u \in \mathbb{Z}_7^\times$ is a cube if and only if $u \equiv \pm 1 \mod 7$. First The cubes in $\mathbb{F}_7^\times$ are ± 1 so that tells us that $u \equiv \pm 1 \mod 7$ is necessary. Conversely, if $u \equiv \pm 1 \mod 7$ we can apply Hensel's lemma to the polynomial $x^3 - (\pm 1)$, with approximate root $a_0 = \pm 1$. The derivative $f'(a_0) = 3a_0^2$ has 7-adic valuation 1 in both cases, and $|f(a_0)|_7 < 1$. So we deduce that u does have a cube root in $\mathbb{Q}_7$.

(b)(i) [Similar to bookwork, but all calculations in lectures/notes have been for cubics in Weierstrass form. 8 marks] First we will need to compute the inverse map for this curve. Since $O = (1 : -1 : 0)$ is an inflection point, $-P$ is the third point on the intersection of $\mathcal{C}$ with the line through O and P. This line has equation $X + Y - (x_1 + y_1)Z = 0$. By symmetry (or a computation of the intersection), the third intersection point is $(y_1 : x_1 : 1)$, so we have $-(x_1 : y_1 : 1) = (y_1 : x_1 : 1)$.
Now we compute the doubling map. The point $-2P$ is the third point on the intersection with $\mathcal{C}$ of the tangent to $\mathcal{C}$ at P. This tangent line has (affine) equation $y = \frac{-x_1^2 x + 2}{y_1^2}$. Intersecting with the cubic gives an equation

$$x^3 + \left(\frac{-x_1^2 x + 2}{y_1^2}\right)^3 = 2$$

which rearranges to a cubic in x with first two terms

$$\left(\frac{y_1^6 - x_1^6}{y_1^6}\right) x^3 + \frac{6x_1^4}{y_1^6} x^2 + \cdots$$

We deduce that the point $-2P$ has x-co-ordinate x_2, where

$$2x_1 + x_2 = \frac{-6x_1^4}{y_1^6 - x_1^6} = \frac{-6x_1^4}{(2-x_1^3)^2 - x_1^6} = \frac{-6x_1^4}{4-4x_1^3}$$

hence $x_2 = \frac{2x_1^4-8x_1}{4-4x_1^3} = \frac{x_1^4-4x_1}{2-2x_1^3}$. Substituting in to the equation of the tangent line, or using the fact that $-2(-P) = 2P$, tells us that $-2P = (x_2, y_2)$ with $y_2 = \frac{y_1^4-4y_1}{2-2y_1^3}$. Taking the inverse gives

$$2P = \left(\frac{y_1^4 - 4y_1}{2-2y_1^3}, \frac{x_1^4-4x_1}{2-2x_1^3}\right)$$

(b)(ii) [A simple computation with the tangent line at a point. 5 marks.] We are looking for points $P = (x_1 : y_1 : z_1)$ whose tangent line passes through $O = (1 : -1 : 0)$. The tangent line has projective equation

$$x_1^2 X + y_1^2 Y - 2z_1^2 Z = 0$$

and substituting in O gives us $x_1^2 - y_1^2 = 0$. We deduce that $y_1 = \pm x_1$. Substituting back in to the equation for the curve gives $x_1^3 \pm x_1^3 = 2z_1^3$. So $y_1 = -x_1$ gives us $z_1 = 0$ and this corresponds to the point O. On the other hand $y_1 = x_1$ gives us $x_1^3 = z_1^3$ and this corresponds to points $(1 : 1 : \zeta)$ with $\zeta^3 = 1$ (or alternatively $(\zeta : \zeta : 1)$). That gives us the 4 2-torsion points of $\mathcal{C}(\mathbb{Q}_7)$, since Hensel's lemma tells us (as in part (a)) that $\mathbb{Q}_7$ contains 3 cube roots of 1.

[*Students may begin with the formula in the previous part, which shows that if P satisfies $x_1^3 = y_1^3 = 1$, then it gets mapped to a point at ∞. However there are three points in $\mathcal{C}(\mathbb{Q}_7)$ with $Z = 0$: $(1 : \zeta : 0)$ with $\zeta^3 = -1$. An extra argument with the doubling formula is needed to show that $x_1 = y_1$. 2 marks for noticing that $x_1^3 = y_1^3 = 1$ is required for a 2-torsion point.*]

(b)(iii) [New (or a more difficult version of examples they have seen, if they use the reduction map). 6 marks.] We are looking for a point $P \in \mathcal{C}(\mathbb{Q}_7)$ with $2P = (\zeta : \zeta : 1)$, $\zeta^3 = 1$. Looking at the formula for $2P$, we need

$$\frac{x^4 - 4x}{2-2x^3} = \zeta.$$

Taking 7-adic valuations gives $|x|_7|x^3 - 4| = |2 - 2x^3|_7$. We see from this that $|x|_7 \geqslant 1$. Also, if we had $|x|_7 > 1$, the valuation of the left hand side would be $|x|_7^4$, whereas the valuation of the right hand side would be $|x|_7^3$. We deduce that $|x|_7 = 1$. We know that $x^3 = \pm 1 \mod 7$, so we deduce also from comparing valuations that $x^3 = -1 \mod 7$. Now we go back to the equation

$$\frac{x^4 - 4x}{2-2x^3} = \zeta.$$

Reducing mod 7 gives us $x = 2\zeta \mod 7$. Cubing both sides gives $x^3 = 1 \mod 7$, a contradiction.

An alternative is to use the reduction mod 7 map. They will need to compute that $\widetilde{\mathcal{C}}(\mathbb{F}_7) \cong C_2 \times C_2 \times C_3$ so it contains no element of order 4 (showing that the cardinality is 12 is not sufficient).

2. Let p be a prime with $p > 5$, and consider the elliptic curve over $\mathbb{Q}$ with equation $\mathcal{E} : y^2 = x^3 + p$.

[*Throughout this question, any results on formal groups from lectures may be assumed provided they are clearly stated.*]

(a) [7 marks] Let q be a prime with $q \nmid 6p$. Show that the order $\#\mathcal{E}(\mathbb{Q})_{\text{tors}}$ of the torsion subgroup of $\mathcal{E}$ divides the order $\#\widetilde{\mathcal{E}}_q(\mathbb{F}_q)$ of the group of points on the reduction $\widetilde{\mathcal{E}}_q$ of the curve modulo q.

(b) [8 marks] (i) Compute the order $\#\widetilde{\mathcal{E}}_5(\mathbb{F}_5)$ of the group of points on the reduction $\widetilde{\mathcal{E}}_5$ of the curve modulo 5.

(ii) Compute the number of points $\#\widetilde{\mathcal{E}}_p(\mathbb{F}_p)$ of the reduction $\widetilde{\mathcal{E}}_p$ of the curve modulo p.

(c) [10 marks] (i) Show that there is no point of $\mathcal{E}(\mathbb{Q}_p)$ reducing to the singular point

$$(0,0) \in \widetilde{\mathcal{E}}_p(\mathbb{F}_p).$$

(ii) Deduce that $\#\mathcal{E}(\mathbb{Q})_{\text{tors}} = 1$.

Solution 2.

(a) [Bookwork, 7 marks] The discriminant of the cubic $x^3 + p$ is $27p^2$, so the primes $q \nmid 6p$ are the primes of good reduction. We recall from lectures that the reduction map defines a homomorphism

$$\mathcal{E}(\mathbb{Q}_q) \to \widetilde{\mathcal{E}}_q(\mathbb{F}_q)$$

with kernel the points $\mathcal{E}_1(\mathbb{Q}_q) = \{(x,y) : |x|_q > 1, |y|_q > 1\}$ (together with the point at infinity). We recall also that the group $\mathcal{E}_1(\mathbb{Q}_q)$ is isomorphic to the group $\mathcal{F}_{\mathcal{E}}(q\mathbb{Z}_q)$ associated to a formal group law over $\mathbb{Z}_q$. The crucial fact we use about formal groups is that if $z \in q\mathbb{Z}_q$ is a torsion point in $\mathcal{F}_{\mathcal{E}}(q\mathbb{Z}_q)$, then it has q-power order, and if its order is $q^n > 1$, then we have $|z|_q \geqslant q^{1/(q^n - q^{n-1})}$. Since this lower bound is $> q^{-1}$, the group $\mathcal{F}_{\mathcal{E}}(q\mathbb{Z}_q)$ is actually torsion-free. [It's also OK for them to state the result from lecturers that this group is torsion-free.]

Now we know that $\mathcal{E}_1(\mathbb{Q}_q)$ is torsion-free, so we deduce that the reduction homomorphism is injective on the torsion subgroup $\mathcal{E}(\mathbb{Q}_q)^{\text{tors}}$. In other words, $\mathcal{E}(\mathbb{Q}_q)^{\text{tors}}$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}_q(\mathbb{F}_q)$. $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ is itself obviously a subgroup of $\mathcal{E}(\mathbb{Q}_q)^{\text{tors}}$, so we get the desired conclusion that its order divides $\#\widetilde{\mathcal{E}}_q(\mathbb{F}_q)$.

(b)(i) [Easy seen similar, 3 marks] Modulo 5, cubing is a bijection. So $x^3 + p$ takes on the 5 different residue classes mod 5 as x varies. In particular it takes the square values $0, 1, -1$ once each. We deduce that there are $1 + 2 \times 2 = 5$ solutions in $\mathbb{F}_5$ to $y^2 = x^3 + p$. Adding in the point at infinity gives $\#\widetilde{\mathcal{E}}_5(\mathbb{F}_5) = 6$.

(b)(ii) [Similar but less familiar, 5 marks.] Note that p is a prime of bad reduction. We have to count solutions to $y^2 = x^3$ in $\mathbb{F}_p$. The point at infinity and $(0,0)$ contribute two points. Otherwise, writing $y = g^i$ and $x = g^j$ for a primitive root g, we need to solve $2i = 3j$ for $i, j \in \mathbb{Z}/(p-1)\mathbb{Z}$. The equation implies that j is even, and for each even j there are two possible values of i, given by $i = 3(j/2) \mod (p-1)/2$. That gives $p - 1$ more solutions, for a total of $p + 1$.

[*It was mentioned in lectures that the singular cubic $y^2 = x^3$ with the singular point $(0,0)$ removed can be identified with the affine line, which explains the count of $p + 1$.*]

(c)(i) [New but they have seen similar arguments with p-adic valuations, 5 marks.] The points reducing to $(0,0)$ are the (x,y) with $|x|_p < 1$ and $|y|_p < 1$. This should be explained somehow: for example, these points do reduce to $(0,0)$; if we have $|x|_p = 1$ or $|y|_p = 1$ then the other co-ordinate is necessarily a p-adic integer and the points then reduces to

a non-singular point; if we have $|x|_p > 1$ or $|y|_p > 1$ then the point reduces to the point at infinity.

It remains to check that there are no such points. We would have $y^2 = x^3 + p$ with $|x|_p < 1$. It follows that $|x^3|_p < p^{-1}$, so the valuation of the right hand side is p^{-1}. This is not the valuation of a square in $\mathbb{Q}_p$, so there are no such points.

(c)(ii) [Somewhat new, since they are asked to consider reduction at a prime of bad reduction, 5 marks.]

There is a short exact sequence

$$0 \to \mathcal{E}_1(\mathbb{Q}_p) \to \mathrm{red}^{-1}(\widetilde{\mathcal{E}}_p(\mathbb{F}_p)^{ns}) \to \widetilde{\mathcal{E}}_p(\mathbb{F}_p)^{ns} \to 0$$

with $\widetilde{\mathcal{E}}_p(\mathbb{F}_p)^{ns} = \widetilde{\mathcal{E}}_p(\mathbb{F}_p) - (0,0)$ is the group of nonsingular points. Part (c)(i) shows that $\mathcal{E}(\mathbb{Q}_p) = \mathrm{red}^{-1}(\widetilde{\mathcal{E}}_p(\mathbb{F}_p)^{ns})$. Using the same result on formal groups as in part (a), we know that $\mathcal{E}_1(\mathbb{Q}_p)$ is torsionfree. So $\mathcal{E}(\mathbb{Q})_{\mathrm{tors}}$ injects into $\widetilde{\mathcal{E}}_p(\mathbb{F}_p)^{ns}$, and therefore has order dividing p. We know from part (b)(i) that its order also divides 6. Since p and 6 are coprime, we deduce that $\mathcal{E}(\mathbb{Q})_{\mathrm{tors}}$ is trivial.

[*Note that they can't just quote part (a) here, since p is a prime of bad reduction.*]

3. (a) [10 marks] Consider an elliptic curve over $\mathbb{Q}$ defined by the equation

$$\mathcal{C} : y^2 = x(x^2 + B),$$

with B a non-zero integer, together with the 2-isogeny $\hat{\phi} : \mathcal{D} \to \mathcal{C}$ from the curve

$$\mathcal{D} : v^2 = u(u^2 - 4B)$$

given by

$$\hat{\phi}(u, v) = \left(\frac{1}{4} \left(\frac{v}{u} \right)^2, \frac{1}{8} \left(v + \frac{4Bv}{u^2} \right) \right).$$

Show that if there is a point $(u, v) \in \mathcal{D}(\mathbb{Q})$ with $u = rt^2$, for r a squarefree integer and $t \in \mathbb{Q}^\times$, then r divides $4B$ and there are integers l, m, n, not all 0, with $\gcd(l, m) = 1$, satisfying the equation

$$rl^4 - \left(\frac{4B}{r} \right) m^4 = n^2.$$

(b) [10 marks] Suppose p is a prime with $p \equiv 3 \mod 8$. Show that the elliptic curve over $\mathbb{Q}$

$$\mathcal{E} : y^2 = x(x^2 - p^2)$$

has rank zero.

[*You may use any results from lectures provided they are clearly stated. It may also help to recall that for an odd prime p we have that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 8$ and -1 is a quadratic residue modulo p if and only if $p \equiv 1 \mod 4$.*]

(c) [5 marks] Find a point of infinite order on the curve with equation $y^2 = x(x^2 - 7^2)$, justifying why it has infinite order.

Solution 3.

(a) [Bookwork, 10 marks] Since $u(u^2 - 4B) = v^2$, u and $u^2 - 4B$ are the same modulo squares, which means we can write:

$$u^2 - 4B = rs^2, \quad u = rt^2, \quad \text{for some } s \in \mathbb{Q}.$$

Hence: $(rt^2)^2 - 4B = rs^2$. Let $t = \ell/m$, where $\ell, m \in \mathbb{Z}$ and $\gcd(\ell, m) = 1$. Then: $r^2\ell^4/m^4 - 4B = rs^2$, and so: $r^2\ell^4 - 4Bm^4 = r(m^2 s)^2$. Now the LHS of this last equation is in $\mathbb{Z}$, and so the RHS is also in $\mathbb{Z}$; that is: $r(m^2 s)^2 \in \mathbb{Z}$. Since r is square free, we must therefore have $m^2 s \in \mathbb{Z}$. Define: $n = m^2 s \in \mathbb{Z}$. Then our equation becomes:

$$r^2\ell^4 - 4Bm^4 = rn^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \ \gcd(\ell, m) = 1,$$

which gives the desired equation. It remains to prove that r divides $4B$. It is sufficient to show, for any prime p, that $p|r \Rightarrow p|4B$. Suppose $p|r$. Then $p|4Bm^4$. If p does not divide $4B$, then $p|m$ and we see that p^2 divides $r^2\ell^4 - 4Bm^4$ and hence $p|n$. So $p^3|rs^2$. Finally, we deduce that $p|\ell$ which contradicts coprimality of ℓ and m. So p did divide $4B$ after all and we are done.

(b) [Seen many similar examples of 2-descent, 10 marks. The same question appears in the 2013 exam paper.]

We rename $\mathcal{E}$ as $\mathcal{C}$ and use the setup of part (a). First we consider the group $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$. We recall from lectures that this admits an injective homomorphism

$$q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

with image described in part (a). In particular, the image is a subgroup of $\{\pm 1, \pm 2, \pm p, \pm 2p\}$, and we have to consider the solvability of equations $rl^4 + (4p^2/r)m^4 = n^2$. We see that for $r < 0$ there are no non-trivial solutions (since the left hand size is then $\leqslant 0$).

We need to analyse the remaining possibilities for r:

($r = 2$) Consider $2l^4 + 2p^2m^4 = n^2$. We deduce that $2l^4 \equiv n^2 \mod p$. Since $p \equiv 3 \mod 8$ this implies that $p|l$ and $p|n$. We can then re-arrange the equation to $2p^2(l/p)^4 + 2m^4 = (n/p)^2$. The same reasoning shows that $p|m$, contradicting coprimality of l and m. So 2 is not in the image of q.

($r = p$) Consider $pl^4 + 4pm^4 = n^2$, equivalently $l^4 + 4m^4 = p(n/p)^2$. This shows that $l^4 = -4m^4 \mod p$. Since l and m are coprime, we deduce that -4 (or, equivalently, -1) is a square mod p. But this contradicts $p \equiv 3 \mod 8$. So p is not in the image of q.

($r = 2p$) Consider $2pl^4 + 2pm^4 = n^2$, equivalently $l^4 + m^4 = 2p(n/2p)^2$. Again this contradicts the fact that -1 is not a square mod p.

So we conclude that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is trivial.

On the other hand, the size of $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ is bounded by 4, with image under the homomorphism $\hat{q}$ a subgroup of $\{\pm 1, \pm p\} \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. All 4 elements appear as the images of the four 2-torsion points $\infty, (0,0), (p,0), (-p,0)$. We conclude that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ has size 4, and is generated by the 2-torsion points. It follows from the Mordell–Weil theorem that the rank of $\mathcal{C}(\mathbb{Q})$ is zero.

(c) [New, 5 marks] One way to find such a point is via 2-descent. Following the working of part (b), we find that we can solve the equation $2l^4 + 2 \cdot 7^2 m^4 = n^2$, with $l = m = 1$, $n = 10$. This gives us the point $(2, 20)$ on the curve $v^2 = u(u^2 + 4 \cdot 7^2)$, which is of infinite order since we can compute that the torsion points on this curve are just $\{O, (0,0)\}$. Indeed, reducing mod 3 we see that the torsion points are isomorphic to a subgroup of C_4 (hence cyclic) whilst reducing mod 5 we see that the torsion points are isomorphic to a subgroup of $C_2 \times C_2$.

We then get a point of infinite order $\hat{\phi}(2, 20) = (25, -120)$ on our original curve.

[*If they somehow spot the rational point* $(25, \pm 120)$ *I'll give 2 marks, but they need to prove that it has infinite order to get full marks. They are given the formula for* $\hat{\phi}$ *earlier to help with this part of the question.*]