

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

Elliptic Curves
James Newton
Draft solutions

10/12/2025

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

[For all elliptic curves in this paper, the identity point O is the point at infinity.]

1. Let p be a prime number and let F be a formal group defined over $\mathbb{Z}_p$.

(a) [10 marks]

(i) Show that the multiplication by p homomorphism on F can be written as

$$[p](T) = pf(T) + g(T^p)$$

for power series $f(T), g(T) \in T\mathbb{Z}_p[[T]]$.

[You may assume existence and uniqueness of a normalized invariant differential for F without proof.]

(ii) Prove that, for every $x \in p\mathbb{Z}_p$,

$$\lim_{n \rightarrow \infty} [p^n](x) = 0.$$

(b) [15 marks]

(i) Suppose that a homomorphism $f : F \rightarrow F$ satisfies $f(T) = 0 \pmod{T^2}$. Show that $f(T) = 0$.

(ii) Show that $[p^n](T) \in (p, T)^{n+1}$ for every $n \geq 1$.

[Here (p, T) denotes the ideal in $\mathbb{Z}_p[[T]]$ generated by p and T .]

(iii) Prove that, for every $a \in \mathbb{Z}_p$, there exists a unique homomorphism $[a] : F \rightarrow F$ satisfying $[a](T) = aT \pmod{T^2}$.

[Hint for uniqueness: to compare two homomorphisms $f(T)$ and $g(T)$, consider the power series $F(f(T), i \circ g(T))$, where $i(T)$ is the inverse for the formal group F .]

2. (a) [7 marks] Consider an elliptic curve over $\mathbb{Q}$ defined by the equation

$$E : y^2 = x^3 + Ax + B,$$

with $A, B \in \mathbb{Z}$.

Show that if a point $P = (x_0, y_0) \neq O$ of $E(\mathbb{Q})$ has finite order, then $x_0, y_0 \in \mathbb{Z}$.

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

(b) [10 marks] Now suppose that E has equation

$$E : y^2 = x^3 + B,$$

for a non-zero integer B .

(i) For a point $P = (x_0, y_0) \in E(\mathbb{Q})$ with $y_0 \neq 0$, find a formula for the x -coordinate of $2P$ in terms of x_0 . You should write your formula in the form

$$x(2P) = \frac{a(x_0)}{4b(x_0)},$$

with $a(x)$ and $b(x)$ coprime polynomials.

(ii) By considering the polynomial $3x^2a(x) - (3x^3 - 27B)b(x)$, or otherwise, deduce that

$$y_0^2 (12x_0^2x(2P) - (3x_0^3 - 27B)) = 27B^2.$$

(iii) Show that if P has finite order, then the integer y_0 divides $27B^2$.

(c) [8 marks] Let p be a prime number and consider the elliptic curve $E : y^2 = x^3 + p$.

(i) Show that the order of $E(\mathbb{Q})_{\text{tors}}$ is odd and less than or equal to 25.

(ii) Find a specific prime p such that $E(\mathbb{Q})_{\text{tors}}$ is trivial, justifying your answer.

3. (a) [5 marks] Let E be the elliptic curve $y^2 = x^3 + 10x - 2$, and consider the point

$$P = (1, 3) \in E(\mathbb{Q}).$$

Explain how to use the computation of $3P$ to factorize the integer 4331.

[Note that $(13/6)^2 = 125 \pmod{4331}$.]

- (b) [5 marks] Find the torsion subgroup $C(\mathbb{Q})_{\text{tors}}$ for the elliptic curve over $\mathbb{Q}$ defined by

$$C : y^2 = x(x^2 - 25).$$

- (c) [15 marks] Find the rank of $C(\mathbb{Q})$. If the rank is greater than 0, give (with justification) an example of a point of infinite order.

[You might find it helpful to recall the formula $\hat{\phi}(u, v) = \left(\frac{1}{4} \left(\frac{v}{u} \right)^2, \frac{1}{8} \left(v - \frac{100v}{u^2} \right) \right)$ for the 2-isogeny from the curve $D : v^2 = u(u^2 + 100)$ to C .]

Solution 1. (a)(i) [5 marks, Bookwork] As suggested in the hint, we use the normalized invariant differential $\omega_F = P(T)dT$ on F . Since $[p]$ is a homomorphism, $\omega_F \circ [p] = [p]'(T)P([p](T))dT$ is a multiple of ω_F . [2 marks]

Comparing constant terms, since $[p](T) = pT \pmod{T^2}$, we get $[p]'(T)P([p](T)) = pP(T)$. Since $P([p](T)) = 1 \pmod{T}$ and is hence invertible in $\mathbb{Z}_p[[T]]$, we deduce that $[p]'(T) \in p\mathbb{Z}_p[[T]]$. In other words, every coefficient of $[p]'(T)$ is in $p\mathbb{Z}_p$, and we deduce that $[p](T)$ has the desired form. [3 marks]

(a)(ii) [5 marks, Unseen but relatively easy. If they do (b)(ii) correctly they can apply it here for full credit.] We prove by induction on n that $|[p^n](x)|_p \leq p^{-(n+1)}$. The case $n = 0$ is clear, because $|x|_p \leq p^{-1}$. Suppose the inequality holds for $y = [p^n](x)$. Then $[p^{n+1}](x) = pf(y) + g(y^p)$, so $|[p^{n+1}](x)|_p \leq \max(p^{-1}|f(y)|_p, |g(y^p)|_p)$.

The power series $f(T), g(T)$ have no constant term, so $|f(y)|_p \leq |y|_p$ and $|g(y^p)|_p \leq |y|_p^p$. We deduce that $p^{-1}|f(y)|_p \leq p^{-(n+2)}$ and $|g(y^p)|_p \leq p^{-(n+1)p} \leq p^{-(n+2)}$. Hence $|[p^{n+1}](x)|_p \leq p^{-(n+2)}$ and we are done by induction.

(b)(i) [4 marks, Unseen] There are two approaches here. The first, direct, approach is to consider the identity

$$f(F(X, Y)) = F(f(X), f(Y)).$$

Suppose for a contradiction that the lowest degree non-zero term in $f(T)$ is aT^k , with degree $k \geq 2$. The degree k terms on the LHS of the above identity are $a(X+Y)^k$, whilst on the RHS we get $aX^k + aY^k$. Since $k \geq 2$ (and $R = \mathbb{Z}_p$ has characteristic 0), we get a contradiction.

The second approach (which is not much different!) is to use the logarithm map for F (defined over $\mathbb{Q}_p$). The composition $g = \log_F \circ f \circ \exp_F$ is an endomorphism of $\widehat{\mathbb{G}}_a$, which again has $g(T) = 0 \pmod{T^2}$. Now we have an identity $g(X+Y) = g(X) + g(Y)$ and we again get a contradiction if $g(T)$ is non-zero.

(b)(ii) [4 marks, Unseen, refines (a)(ii)] Part (a)(i) shows this is true for $n = 1$. (Or we could use $n = 0$ as base case.) We proceed by induction for general n .

Suppose $h(T) = [p^n](T) \in (p, T)^{n+1}$. Then $[p^{n+1}](T) = pf(h(T)) + g(h(T)^p)$. Considering the two terms in turn, since $f(T)$ has no constant term, $f(h(T)) \in (p, T)^{n+1}$ and hence $pf(h(T)) \in (p, T)^{n+2}$. Similarly, since $h(T)^p \in (p, T)^{p(n+1)} \subset (p, T)^{n+2}$, we have $g(h(T)^p) \in (p, T)^{n+2}$, and we are done.

(b)(iii) [7 marks, Unseen] Uniqueness follows from (b)(i): suppose there are two homomorphisms $f, g : F \rightarrow F$ with $f(T), g(T) = aT \pmod{T^2}$. Then the difference $F(f(T), ig(T))$ between the two homomorphisms is a homomorphism with linear term $aT - aT = 0$. So (b)(i) implies that $F(f(T), ig(T)) = 0$ and hence $g(T) = f(T)$ (by the uniqueness of inverses). [3 marks]

Existence follows from (b)(ii), which shows that if we have a sequence a_n of integers with $a_n = a \pmod{p^n}$, then we get a well-defined power series

$$[a](T) = \lim_{n \rightarrow \infty} [a_n](T).$$

Moreover, $[a](T) = [a_n](T) \pmod{(p, T)^{n+1}}$. Clearly $[a](T)$ has linear term aT . To show that it's a homomorphism we note that, since $[a_n]$ is a homomorphism, we have $[a](F(X, Y)) - F([a](X), [a](Y)) = 0 \pmod{(p, T)^{n+1}}$ for every n , and hence $[a](F(X, Y)) - F([a](X), [a](Y)) = 0$. [4 marks]

Solution 2. (a) [7 marks, Bookwork] We use the fact that the groups $(\mathcal{F}(p\mathbb{Z}_p), +_{\mathcal{F}})$ associated to formal groups over $\mathbb{Z}_p$ are torsion-free for odd primes, whilst for $p = 2$ every torsion point is 2-torsion. [2 marks for recalling this fact or similar]

Suppose $O \neq P = (x_0, y_0) \in E(\mathbb{Q})_{\text{tors}}$. We deduce that for odd p , P is not in the kernel of reduction $E_1(\mathbb{Q}_p)$, so $|x_0|_p \leq 1$ and $|y_0|_p \leq 1$. For $p = 2$, if P has order 2 then its coordinates are in $\mathbb{Z}$ (e.g. Gauss's lemma tells us that the rational roots of $x^3 + Ax + B$ are in $\mathbb{Z}$). If it does not have order 2, then we again deduce that P is not in the kernel of reduction, so $|x_0|_2 \leq 1$ and $|y_0|_2 \leq 1$. Putting everything together, $|x_0|_p \leq 1$ and $|y_0|_p \leq 1$ for all primes p , so $x_0, y_0 \in \mathbb{Z}$. [4 marks for argument at odd primes, 1 mark for considering $p = 2$ separately]

(b)(i) [5 marks, Seen Similar] The tangent line through P has equation

$$y - y_0 = \frac{3x_0^2}{2y_0}(x - x_0).$$

[2 marks for computing tangent]

Intersecting with the curve gives a cubic equation in x :

$$(y_0 + \frac{3x_0^2}{2y_0}(x - x_0))^2 = x^3 + B$$

whose roots, with multiplicity, are x_0, x_0 and $x(2P)$. Considering the coefficient of x^2 , we deduce that

$$2x_0 + x(2P) = \frac{9x_0^4}{4y_0^2},$$

so $x(2P) = \frac{9x_0^4 - 8x_0y_0^2}{4y_0^2}$. We rewrite using $y_0^2 = x_0^3 + B$:

$$x(2P) = \frac{x_0^4 - 8Bx_0}{4(x_0^3 + B)}.$$

[3 marks for rest of computation]

(b)(ii) [4 marks, Seen Similar] Multiplying out the suggested polynomial, we get $3x^2a(x) - (3x^3 - 27B)b(x) = 3x^6 - 24Bx^3 - 3x^6 - 3Bx^3 + 27Bx^3 + 27B^2 = 27B^2$.

We deduce that $y_0^2(12x_0^2x(2P) - (3x_0^3 - 27B)) = b(x_0)(3x_0^2 \frac{a(x_0)}{b(x_0)} - (3x_0^3 - 27B)) = 27B^2$, as desired.

(b)(iii) [1 mark, Seen Similar] We use part (a): this implies that both factors on the left hand side of the equation in (b)(ii) are integers, so $y_0^2 | 27B^2$.

(c)(i) [4 marks, Unseen] First we note that there are no points of order two in $E(\mathbb{Q})$, since $x^3 + p$ is irreducible over $\mathbb{Q}$. So the order of $E(\mathbb{Q})_{\text{tors}}$ is odd. Now suppose $O \neq P \in E(\mathbb{Q})$ is a point of finite order. Part (b)(iii) gives us 8 possibilities for the value of $y(P)$: it is an integer with $y(P)^2 | 27p^2$, so it is equal to $\pm 1, \pm 3, \pm p, \pm 3p$. For each value of $y(P)$, we have at most 3 possibilities for $x(P)$ (the three roots of a cubic), which gives at most 24 points. Adding in O , we get at most 25 elements in $E(\mathbb{Q})_{\text{tors}}$.

(ii) [4 marks, Unseen] There are many choices here. For example we could take $p = 3$ and apply (b)(iii), checking none of the possible values for $y(P)^2$, $(1, 9, 81)$, give rational values for $x(P)$. Alternatively, for $p = 7$, or indeed any prime $\equiv 2 \pmod{5}$: check by reduction mod 5 that $E(\mathbb{Q})_{\text{tors}}$ has order dividing 4, which implies it has order 1, since we have already observed it has odd order. The slightly tricky part here is that the first prime $p = 2$ has an integral point $(-1, 1)$ satisfying the Nagell-Lutz bound.

Solution 3. (a) [5 marks, Seen Similar] First we compute $2P$. The tangent line at P has gradient $(13/6)$. So the x -coordinate of $2P$ satisfies $(13/6)^2 = 2 + x(2P)$. We deduce that $x(2P) = 123 \pmod{4331}$. To compute $2P + P$, we need to invert $(x(2P) - x(P)) = 122$ to get the gradient of the line joining P and $2P$. We apply the Euclidean algorithm:

$$4331 = 36 * 122 + 61$$

$$122 = 2 * 61$$

So $61|4331$ and we have a factorization $4331 = 61 \times 71$. [2 marks for each point addition, 1 mark for correct conclusion about factorization]

(b) [5 marks, Seen Similar] Since 3 is a prime of good reduction, $C(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $C(\mathbb{F}_3)$, which has size 4 (each value of x gives a 2-torsion point). On the other hand, $C(\mathbb{Q})$ contains full 2-torsion: $\{O, (0, 0), (\pm 5, 0)\}$. So we deduce that these four points give the rational torsion subgroup. [3 marks for mod 3 computation, 2 more marks for conclusion. Full credit for alternative solutions using Lutz–Nagell]

(c) [15 marks, Seen Similar, although not so many examples with positive rank.] We run the standard 2-descent process, so we have maps $\phi, \hat{\phi}$ between C and D and we compute $G/\hat{\phi}(H)$, $H/\phi(G)$, where $G = C(\mathbb{Q})$ and $H = D(\mathbb{Q})$.

The map $q : H/\phi(G) \rightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ has image contained in (the cosets of) squarefree integers dividing 100. It is therefore contained in the group generated by $(-1, 2, 5)$. A squarefree integer is contained in the image of q if and only if the equation

$$W_r : rl^4 + (100/r)m^4 = n^2$$

has integer solutions with (l, m) coprime. For $r = -1$, comparing signs of the left and right hand sides tells us there are no such solutions. [5 marks for correct set-up and translation in terms of W_r]

For $r = 2$ the equation says $2l^4 + 50m^4 = n^2$. Considering the equation mod 5, using the fact that 2 is not a square mod 5, tells us that 5 must divide l and n . Rewriting the equation in terms of $l' = l/5$ and $n' = n/5$ gives $50(l')^4 + 2m^4 = (n')^2$. Repeating the same argument shows that $5|m$, which contradicts coprimality of l and m . So we deduce that 2 is not in the image of q . [3 marks]

For $r = 5$ the equation says $5l^4 + 20m^4 = n^2$. This has the solution $(l, m, n) = (1, 1, 5)$. We get a point $P = (5, 25)$ in $D(\mathbb{Q})$ with image 5 under q . Its image in $C(\mathbb{Q})$ is $(25/4, -75/8)$ which necessarily has infinite order because it is not integral. [2 marks]

At this point we have shown that $H/\phi(G)$ has size 2, generated by the point P of infinite order.

Now we consider $G/\hat{\phi}(H)$. The image of the map $\hat{q}$ must be contained in squarefree integers dividing 25. But the 2-torsion points already give the full group of order 4 generated by $-1, 5$. [2 marks]

We conclude that $G/2G$ has order at most 8, with the torsion subgroup contributing 4. It follows that the rank is at most one, and the existence of the infinite order point $\hat{\phi}(P)$ shows that the rank is exactly one. [3 marks]