Bull. Aust. Math. Soc. (First published online 2026), page 1 of 16*
doi:10.1017/S0004972726101592
*Provisional—final page numbers to be inserted when paper edition is published

COLLISION OF ORBITS ON AN ELLIPTIC SURFACE

DRAGOS GHIOCA and NEGIN SHADGAR

(Received 9 February 2026 UTC; accepted 19 May 2026 UTC)

Abstract

Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\pi : \mathcal{E} \longrightarrow C$ be an elliptic surface and let $\sigma_{P_1}, \sigma_{P_2}, \sigma_Q$ be sections of π (corresponding to points P_1, P_2, Q of the generic fibre E of $\mathcal{E}$). We obtain a precise characterisation, expressed solely in terms of the dynamical relations between the points P_1, P_2, Q with respect to the endomorphism ring of E, so that there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ with the property that $[m_{i,\lambda}](\sigma_{P_i}(\lambda)) = \sigma_Q(\lambda)$ (for $i = 1, 2$) for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, on the smooth fibre E_λ of $\mathcal{E}$.

2020 *Mathematics subject classification*: primary 37P15; secondary 11G35.

Keywords and phrases: elliptic surfaces, unlikely intersections, collision of orbits.

1. Introduction

1.1. Notation and setup for our problem. For an elliptic curve E defined over a field L of characteristic 0, we denote by $\mathrm{End}(E)$ the ring of group endomorphisms of E (defined over an algebraic closure $\overline{L}$ of L). It is known (see [33, Ch. 2]) that $\mathrm{End}(E)$ is isomorphic either with $\mathbb{Z}$ (when E has no complex multiplication) or with an order in an imaginary quadratic number field (when E has *complex multiplication*, also referred to as CM). So, we identify $\mathrm{End}(E)$ with either $\mathbb{Z}$ (in the non-CM case) or with an order $\mathcal{O}$ in an imaginary quadratic number field (in the CM case); more precisely, for each $n \in \mathbb{Z}$ (respectively, for each $\alpha \in \mathcal{O}$), we denote by $[n]$ (respectively, $[\alpha]$) the corresponding endomorphism of E.

Throughout our paper, C is a smooth, projective (irreducible) curve defined over $\overline{\mathbb{Q}}$. Also, we consider $\pi : \mathcal{E} \longrightarrow C$ as an elliptic surface, where the generic fibre of π is an elliptic curve E defined over $\overline{\mathbb{Q}}(C)$, while for all but finitely many points $\lambda \in C(\overline{\mathbb{Q}})$, the fibre $E_\lambda := \pi^{-1}(\{\lambda\})$ is an elliptic curve defined over $\overline{\mathbb{Q}}$. We often refer to E_λ as the *λ-fibre* of π. Each section σ of π (that is, a map $\sigma : C \to \mathcal{E}$ such that $\pi \circ \sigma = \mathrm{id}|_C$) gives rise to a $\overline{\mathbb{Q}}(C)$-rational point of E. Conversely, a point $P \in E(\overline{\mathbb{Q}}(C))$ corresponds to a section of π, denoted σ_P. For all but finitely many $\lambda \in C(\overline{\mathbb{Q}})$, the intersection of the image of σ_P in $\mathcal{E}$ with the smooth fibre E_λ above λ is a point $P_\lambda := \sigma_P(\lambda)$ on the elliptic curve E_λ; we refer to P_λ as the *λ-specialisation of the point P* and we

The research of the first author was partially supported by a Discovery Grant from the NSERC.
© The Author(s), 2026. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

drop the mention of the corresponding section σ_P. Furthermore, when working with a point $P_i \in E(\overline{\mathbb{Q}}(C))$ (for some index i), we use the notation $P_{i,\lambda}$ for the corresponding λ-specialisation of P_i.

We say that $\mathcal{E}$ is *isotrivial* if the j-invariant (see [33, Ch. 3]) of the generic fibre E is a constant function (on C); for isotrivial elliptic surfaces $\mathcal{E}$, all smooth fibres of π are isomorphic to E. If $\mathcal{E}$ is isotrivial, then at the expense of replacing C by a finite cover C' (defined over $\overline{\mathbb{Q}}$) and, also, replacing $\mathcal{E}$ by $\mathcal{E} \times_C C'$, we may assume $\mathcal{E}$ is a *constant elliptic surface*. So, when E is isotrivial, since our question is unchanged when replacing C by a finite cover, we always assume there exists an elliptic curve E_0 defined over $\overline{\mathbb{Q}}$ such that $\mathcal{E} = E_0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C$. In this case, we say that a section σ_P of $\mathcal{E}$ is *constant* if $P \in E_0(\overline{\mathbb{Q}})$.

We study the following question for elliptic surfaces $\mathcal{E} \to C$ defined over $\overline{\mathbb{Q}}$; as before, we denote by E the generic fibre of $\mathcal{E}$. So, with the above notation, given two *starting points* $P_1, P_2 \in E(\overline{\mathbb{Q}}(C))$ and one *target point* $Q \in E(\overline{\mathbb{Q}}(C))$ (all three of them nontorsion), we obtain necessary and sufficient conditions (in terms of the dynamics of P_1, P_2, Q under the action of $\mathrm{End}(E)$) so that Q_λ is contained in both the cyclic group generated by $P_{1,\lambda}$ and in the cyclic group generated by $P_{2,\lambda}$ inside E_λ.

1.2. Our main result. We prove the following statement.

THEOREM 1.1. *Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{E} \to C$ be an elliptic surface and let $P_1, P_2, Q \in E(\overline{\mathbb{Q}}(C))$ be nontorsion points on the generic fibre E of π. Furthermore, if $\mathcal{E}$ is isotrivial, assume that not all three sections $\sigma_{P_1}, \sigma_{P_2}, \sigma_Q$ are constant. Then, there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that $[m_{i,\lambda}](P_{i,\lambda}) = Q_\lambda$, for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, on the λ-fibre E_λ of π if and only if at least one of the following conditions holds:*

(A) *there exists a nonzero integer k such that $[k](P_i) = Q$ on E for some $i \in \{1, 2\}$;*
(B) *there exist nonzero integers k_1 and k_2 such that $[k_1](P_1) = [k_2](P_2)$ on E;*
(C) *E has complex multiplication by some order $\mathcal{O}$ in an imaginary quadratic number field and there exist nonzero $\alpha_1, \alpha_2, \beta \in \mathcal{O}$ with $\alpha_1/\alpha_2 \notin \mathbb{Q}$ such that $[\alpha_1](P_1) = [\alpha_2](P_2) = [\beta](Q)$ on E.*

Our Theorem 1.1 strengthens [23, Theorem 1.1], which we state next.

THEOREM 1.2. *With the notation as in Theorem 1.1 for $\mathcal{E}, C, E, P_1, P_2, Q$, if there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that $[m_{i,\lambda}](P_{i,\lambda}) = Q_\lambda$ (for $i = 1, 2$) for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, on the λ-fibre E_λ of π, then, at least one of the following two conditions holds:*

(i) *there exists a nonzero integer k such that $[k](P_i) = Q$ for some $i \in \{1, 2\}$;*
(ii) *there exist nontrivial endomorphisms $\alpha_1, \alpha_2 \in \mathrm{End}(E)$ such that $\alpha_1(P_1) = \alpha_2(P_2)$.*

REMARK 1.3. Here, we explain the hypothesis appearing in our Theorem 1.1 regarding the points P_1, P_2, Q not being constant when $\mathcal{E}$ is isotrivial. Indeed, working (after replacing C by a suitable finite cover) with $\mathcal{E} = E_0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C$, if $P_1, P_2, Q \in E_0(\overline{\mathbb{Q}})$,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

then the problem considered in Theorem 1.1 loses its relevance since we have in this case (no matter what is the fibre of our elliptic surface) the same dynamical system (in terms of the two starting points and the target point). In particular, conditions (A)–(C) stated as in Theorem 1.1 no longer guarantee the existence of infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that Q_λ lives in the cyclic groups generated by $P_{i,\lambda}$ (for $i = 1, 2$).

1.3. Unlikely intersections in arithmetic dynamics. Our Theorem 1.1 fits into the larger theme of unlikely intersections in arithmetic dynamics. The following result was proved by Masser and Zannier (see [28, 29]); an alternative proof was given by DeMarco and Mavraki (see [16]).

THEOREM 1.4. *Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\pi : \mathcal{E} \longrightarrow C$ be an elliptic surface and let $P_1, P_2 \in E(\overline{\mathbb{Q}}(C))$ be nontorsion points on the generic fibre E of $\mathcal{E}$. Then, there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that $[m_{i,\lambda}](P_{i,\lambda}) = 0$ (for $i = 1, 2$), for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, on the λ-fibre E_λ of π if and only if there exist nontrivial endomorphisms $\alpha_1, \alpha_2 \in \mathrm{End}(E)$ such that $\alpha_1(P_1) = \alpha_2(P_2)$.*

Theorem 1.4 shows that the infinite occurrence of the *unlikely* event that *both* $P_{1,\lambda}$ and $P_{2,\lambda}$ are torsion on E_λ can only be explained by a global dynamical relation between the points P_1 and P_2; such a conclusion fits the pattern behind several other unlikely intersection problems, going back to classical questions in arithmetic geometry (for more details, see [36]). We also note that several extensions of the results from [28, 29] were obtained both in the case of elliptic surfaces (see [6]) and also in the general case of semi-abelian schemes (see [7, 8]).

Our Theorem 1.1 can be viewed as an extension of Theorem 1.4 since we replace the *target* $0 \in E$ from Theorem 1.4 with an arbitrary point $Q \in E(\overline{\mathbb{Q}}(C))$. Also, we note that for *one* starting point P_1 and a target point Q, it is known, as proved in [15, Theorem A2] (see also Lemma 4.2), that there exist infinitely many integers n such that $[n](P_{1,\lambda}) = Q_\lambda$. However, the fact that for some point $\lambda \in C(\overline{\mathbb{Q}})$, the point Q_λ is a multiple *both* of $P_{1,\lambda}$ and of $P_{2,\lambda}$ is an *unlikely event*, which can only be explained by a global dynamical relation between the starting points P_1, P_2 and the target point Q (as in conclusions (A)–(C) from Theorem 1.1).

REMARK 1.5. It makes sense to ask that Q is nontorsion in our Theorem 1.1 since otherwise (at the expense of replacing Q by a suitable multiple), we recover the setting from Theorem 1.4. Furthermore, once we work with a nontorsion target point Q in Theorem 1.1, it is automatic to consider that also the starting points $P_1, P_2 \in E(\overline{\mathbb{Q}}(C))$ are nontorsion. Indeed, if there exists a positive integer ℓ such that $[\ell](P_1) = 0$, then the existence of infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that $[m_{1,\lambda}](P_{1,\lambda}) = Q_\lambda$, for some suitable nonzero integers $m_{1,\lambda}$, yields $[\ell](Q_\lambda) = 0$ for those λ terms. So, by the pigeonhole principle, there exists some torsion point R of E (such that $[\ell](R) = 0$) with the property that $R_\lambda = Q_\lambda$ for infinitely many $\lambda \in C(\overline{\mathbb{Q}})$. This means that $R = Q$, contradicting the assumption that Q is nontorsion. Therefore, the assumption that all three points P_1, P_2, Q are nontorsion is justified for Theorem 1.1.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

The results of Masser and Zannier [28, 29] (see Theorem 1.4) were the catalysts for an intense study in arithmetic dynamics of unlikely intersection questions (see the survey article [10] for a more in-depth discussion of it as one of the central questions in arithmetic dynamics, and also the book [36] for a thorough study of the origins of unlikely intersection questions in arithmetic geometry). In particular, the so-called question of *simultaneously preperiodic points* (see also the survey [18]) generated a great deal of research in recent years (see [4, 5, 20, 21] and the references therein). Consider a family $F_\lambda(z)$ of polynomials parametrised by the $\mathbb{C}$-points λ on some projective smooth curve C; also, let $\mathbf{a}, \mathbf{b} : C \to \mathbb{P}^1$. Then, one obtains (see [17]) a complete characterisation (based on the dynamics of $\mathbf{a}, \mathbf{b}$ under the action of the family of maps $\{F_\lambda\}_{\lambda \in C}$) for the following unlikely scenario to happen: there exist infinitely many $\lambda \in C(\mathbb{C})$ such that both $\mathbf{a}(\lambda)$ and $\mathbf{b}(\lambda)$ are preperiodic under the action of $F_\lambda(z)$. The general principle behind this question involving simultaneously preperiodic points is that the aforementioned infinite occurrence of the unlikely event that both the orbits of $\mathbf{a}(\lambda)$ and of $\mathbf{b}(\lambda)$ are finite under the action of $F_\lambda(z)$ is explained only due to a *global dynamical relation* between the two starting points $\mathbf{a}$ and $\mathbf{b}$ under the action of $F_\eta(z)$, where η is the generic point on C.

It is natural to extend this study of unlikely intersections to the following scenario. With the above notation for the family of maps F_λ and for the *two starting points* $\mathbf{a}, \mathbf{b}$, one considers also a *target point* $\mathbf{c} : C \to \mathbb{P}^1$ and then asks for a precise characterisation of when the following unlikely scenario occurs: there exist infinitely many points $\lambda \in C(\mathbb{C})$ such that $\mathbf{c}(\lambda)$ lives in the forward orbits of both $\mathbf{a}(\lambda)$ and of $\mathbf{b}(\lambda)$ under the action of $F_\lambda(z)$ (that is, there exist positive integers m and n such that $F_\lambda^m(\mathbf{a}(\lambda)) = \mathbf{c}(\lambda)$ and $F_\lambda^n(\mathbf{b}(\lambda)) = \mathbf{c}(\lambda)$). This problem is often coined the *collision of orbits question* (see [3, 19]). Using the same strategy patented in [4] (and further refined in the subsequent papers [5, 21]), one can obtain global conditions that are *necessary* for this collision of orbits question; however, obtaining precise *necessary and sufficient* conditions is much more delicate compared with the previous question of simultaneously preperiodic points (see the discussion from both [3, Remark 2.8] and [19, Section 2]). Our Theorem 1.1 provides a complete answer to a variant of this collision of orbits question in the context of algebraic families of elliptic curves E_λ, this time replacing the orbit of a point under a polynomial (or rational) map with the orbit of the corresponding point on E_λ under the action of $\mathbb{Z}$, seen as a subring of $\mathrm{End}(E_\lambda)$.

1.4. Previous results and further connections to our work. A variant of the problem of collision of orbits is the following question studied by Hsia and Tucker [24]. Given polynomials $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{C}[z]$ (whose compositional powers $\mathbf{a}^m, \mathbf{b}^n, \mathbf{c}^k$ for any positive integers m, n, k are all distinct), then [24, Theorem 1] establishes that there exist finitely many $\lambda \in \mathbb{C}$ such that

$$(z - \lambda) \mid \gcd(\mathbf{a}^m(z) - \mathbf{c}(z), \mathbf{b}^n(z) - \mathbf{c}(z)) \quad \text{for some } m, n \in \mathbb{N}.$$

So, at its heart, the problem of collision of orbits is a question regarding the greatest common divisors of certain polynomials (see also the discussion from [3, Section 9]).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

This has its origins in the problem studied by Ailon and Rudnick [1], who proved that if $\mathbf{a}, \mathbf{b} \in \mathbb{C}[z]$ are multiplicatively independent, then there exists a nonzero polynomial $\mathbf{d} \in \mathbb{C}[z]$ such that

$$\gcd(\mathbf{a}(z)^k - 1, \mathbf{b}(z)^k - 1) \mid \mathbf{d}(z) \quad \text{for all } k \in \mathbb{N},$$

where $\mathbf{a}(z)^k, \mathbf{b}(z)^k$ are the (usual) kth powers of the polynomials $\mathbf{a}(z), \mathbf{b}(z)$.

In turn, the result of Ailon and Rudnick was motivated by the work of Bugeaud, Corvaja and Zannier [11] who established an upper bound for $\gcd(a^k - 1, b^k - 1)$ (as k varies in $\mathbb{N}$) for given $a, b \in \mathbb{Q}$. This problem of bounding the greatest common divisor has been studied in several other directions: for elements close to S-units [14, 27], for polynomials defined over fields of positive characteristic [22] and also for elliptic divisibility sequences [32]. One of the open questions raised in [32] was answered in the affirmative in [23, Theorem 1.1] (stated above as Theorem 1.2). Extensions of the results from [23] were also obtained in the more general case of semi-abelian schemes (see [9]).

1.5. Plan for our paper. Most of the work for obtaining the direct implication in Theorem 1.1 was done in [23, Theorem 1.1] (see Theorem 1.2). However, in the case when the elliptic surface admits complex multiplication, we need to sharpen the statement of Theorem 1.2(ii) to deliver conclusion (C) in our Theorem 1.1. This part is done in Section 3 (see Proposition 3.1).

We prove the converse implication from Theorem 1.1 by considering separately each of the three conditions (A), (B) and (C) (see Lemmas 4.4, 4.5 and Proposition 4.6) and show that, in each case, there exist infinitely many points $\lambda \in C(\overline{\mathbb{Q}})$ such that Q_λ is (an integer) multiple of both $P_{1,\lambda}$ and of $P_{2,\lambda}$. When the elliptic surface admits complex multiplication (that is, condition (C) holds), we need a more careful analysis; in particular, we need to employ some basic facts regarding the arithmetic of orders in an imaginary quadratic number field (for more details, see Section 2).

2. Arithmetic properties of an elliptic curve with complex multiplication

Let E be a CM elliptic curve defined over a field L of characteristic 0; let $\mathcal{O}$ be its endomorphism ring. We identify $\mathcal{O}$ with an order in some imaginary quadratic number field; that is, $\mathcal{O} = \mathbb{Z}[\theta]$, where (for some $f \in \mathbb{N}$ and some square-free positive integer D),

$$\theta = \begin{cases} f \cdot i\sqrt{D} & \text{if } D \not\equiv 3 \pmod 4, \\ f \cdot (1 + i\sqrt{D})/2 & \text{if } D \equiv 3 \pmod 4. \end{cases} \tag{2.1}$$

We recall the definition of the norm $N(\cdot)$ in the quadratic number field $\mathbb{Q}(i\sqrt{D})$; in particular, for any $a + b\theta \in \mathcal{O}$,

$$N(a + b\theta) = (a + b\theta) \cdot (a + b\bar{\theta}), \tag{2.2}$$

where $\bar{\gamma}$ is simply the complex conjugate of any $\gamma \in \mathbb{Q}(i\sqrt{D})$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

In our proof, we employ some simple facts (see Lemmas 2.1 and 2.5) regarding the arithmetic of the ring $\mathcal{O}$.

LEMMA 2.1. *With D, θ as in (2.1), let a be an odd integer. Then, there exist $m, r, s \in \mathbb{Z}$ such that*

$$m - \theta = (a + 4\theta) \cdot (r + s\theta). \tag{2.3}$$

Lemma 2.1 can be proven directly, but it is also an immediate consequence of the following more general result; we warmly thank the referee for suggesting Proposition 2.2.

PROPOSITION 2.2. *Let $\alpha \in \mathcal{O}$ with the property that there exists no rational prime divisor of α. Then, the composite map $\mathbb{Z} \hookrightarrow \mathcal{O} \to \mathcal{O}/\alpha \cdot \mathcal{O}$ is surjective.*

REMARK 2.3. In Lemma 2.1, since a is odd, we see that $\alpha = a + 4\theta \in \mathcal{O}$ satisfies the hypotheses of Proposition 2.2 and, therefore, there exists $m \in \mathbb{Z}$ such that $m - \theta \in \alpha \cdot \mathcal{O}$, that is, there exist $r, s \in \mathbb{Z}$ (depending on m) such that (2.3) holds.

PROOF OF PROPOSITION 2.2. From the hypotheses of Proposition 2.2, there exist coprime integers a and b such that $\alpha = a + b\theta$. To obtain the desired conclusion in Proposition 2.2, it suffices to show there exist $m, x, y \in \mathbb{Z}$ such that

$$m - \theta = (a + b\theta) \cdot (x + y\theta). \tag{2.4}$$

If $\theta = f \cdot i\sqrt{D}$ (see (2.1)), then using that $\theta^2 = -f^2 D$ along with the fact that $\gcd(a, b) = 1$, we immediately see that there exist suitable integers m, x, y as in (2.4).

Now, if $\theta = f \cdot ((1 + i\sqrt{D})/2)$ (see again (2.1) so that $D \equiv 3 \pmod 4$), we obtain

$$\theta^2 - 2f\theta + \frac{f^2(1 + D)}{4} = 0.$$

Then, there exist suitable integers m, x, y as in (2.4), as long as there exist integers x and y such that

$$1 = ay + bx + 2fby = ay + b \cdot (x + 2fy). \tag{2.5}$$

Since $\gcd(a, b) = 1$, there exist integers y_0 and x_0 such that $1 = ay_0 + bx_0$ and, therefore, letting $y = y_0$ and $x = x_0 - 2fy_0$, we see that (2.5) is verified (and, thus, (2.4) holds). This concludes our proof of Proposition 2.2. □

Lemma 2.1 allows us to derive the following easy consequence.

COROLLARY 2.4. *Let a be an odd integer, let Q be a torsion point of E satisfying $[a + 4\theta](Q) = 0$ and let U be the cyclic (finite) subgroup of E generated by Q. Then, for each $\alpha \in \mathcal{O}$, the following statements hold:*

(i) $[\alpha](Q) \in U$, *that is,* $[\alpha]$ *induces a natural group homomorphism* $\widetilde{[\alpha]}$ *on U given by* $\widetilde{[\alpha]}(Q) = [\alpha](Q)$;
(ii) *if* $\gcd(N(a + 4\theta), N(\alpha)) = 1$, *then* $\widetilde{[\alpha]} : U \to U$ *is a group automorphism.*

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

PROOF. By Lemma 2.1, there exist $m, r, s \in \mathbb{Z}$ such that

$$m - \theta = (a + 4\theta) \cdot (r + s\theta). \tag{2.6}$$

Equation (2.6) (along with the fact $[a + 4\theta](Q) = 0$) shows that $[\theta](Q) = [m](Q)$, that is, $[\theta]$ induces the natural group homomorphism $\widetilde{[\theta]}$ on U given by

$$\widetilde{[\theta]}(Q) = [m](Q). \tag{2.7}$$

In particular, writing $\alpha := c + d\theta$ (for some $c, d \in \mathbb{Z}$), this means that $[\alpha]$ induces a group homomorphism $\widetilde{[\alpha]}$ on U. More precisely, by (2.7),

$$[\alpha](Q) = [c + dm](Q). \tag{2.8}$$

Equation (2.8) proves conclusion (i) of Corollary 2.4.

Now, assuming that $\gcd(N(a + 4\theta), N(\alpha)) = 1$, we see that $[N(\alpha)]$ induces a natural group automorphism of the cyclic group U (whose order divides $N(a + 4\theta)$). Part (i) shows that $[\alpha]$ and $[\bar{\alpha}]$ induce the group homomorphisms $\widetilde{[\alpha]}$ and $\widetilde{[\bar{\alpha}]}$ on U for which

$$\widetilde{[\alpha]} \circ \widetilde{[\bar{\alpha}]} = \widetilde{[N(\alpha)]} \text{ is a group automorphism for } U.$$

Therefore, $\widetilde{[\alpha]}$ is a group automorphism of U, as desired for part (ii) of the conclusion in Corollary 2.4. □

The next result shows that we can always find (infinitely many) elements in $\mathcal{O}$ of the form $a + 4\theta$ whose norms are coprime with a given positive integer. In particular, this will allow us to employ Corollary 2.4 in our proof of Proposition 4.6 (which will deliver the converse implication in Theorem 1.1 for CM elliptic curves).

LEMMA 2.5. *Let M be a positive integer. Then, there exists $\ell \in \{1, \ldots, M\}$ such that for each integer $a \in \mathbb{Z}$ satisfying*

$$a \equiv 2\ell - 1 \pmod{2M},$$

we have $\gcd(N(a + 4\theta), 2M) = 1$.

PROOF. We split our analysis based on the two cases for θ in (2.1). The case when $\theta = f \cdot i\sqrt{D}$ is easier than the case when $\theta = f \cdot (1 + i\sqrt{D})/2$ (and $D \equiv 3 \pmod 4$); therefore, we focus here on the latter case (especially, since the analysis for the former case is similar). So, by (2.2),

$$N(a + 4\theta) = N(a + 2f + i \cdot 2f\sqrt{D}) = (a + 2f)^2 + 4f^2D. \tag{2.9}$$

For each prime p dividing $2M$, we have two cases, depending on whether $p \mid 2f \cdot D$ or not; either way, we can always find some residue class $r_p \in \{0, 1, \ldots, p - 1\}$ such that if $a \equiv r_p \pmod p$, then $p \nmid N(a + 4\theta)$ (see (2.9)). Since $r_2 = 1$ (that is, a has to be odd so that $N(a + 4\theta)$ is odd), we obtain the desired conclusion in Lemma 2.5. □

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

3. Proof of the direct implication in Theorem 1.1

In this section, we prove the following result.

PROPOSITION 3.1. *Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{E} \to C$ be an elliptic surface and let $P_1, P_2, Q \in E(\overline{\mathbb{Q}}(C))$ be nontorsion points on the generic fibre E of π. Assume there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that $[m_{i,\lambda}](P_{i,\lambda}) = Q_\lambda$ for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$ on the λ-fibre E_λ of π. Then, at least one of the following three conditions must hold:*

(A) *there exists a nonzero integer k such that $[k](P_i) = Q$ on E for some $i \in \{1, 2\}$;*
(B) *there exist nonzero integers k_1 and k_2 such that $[k_1](P_1) = [k_2](P_2)$ on E;*
(C) *E has complex multiplication by some order $\mathcal{O}$ in an imaginary quadratic number field and there exist nonzero $\alpha_1, \alpha_2, \beta \in \mathcal{O}$ with $\alpha_1/\alpha_2 \notin \mathbb{Q}$ such that $[\alpha_1](P_1) = [\alpha_2](P_2) = [\beta](Q)$ on E.*

Proposition 3.1 provides the direct implication in Theorem 1.1 without the nonconstant assumption for the corresponding sections $\sigma_{P_1}, \sigma_{P_2}, \sigma_Q$ (see also Remark 1.3).

PROOF OF PROPOSITION 3.1. First, we note that we work under the hypotheses from Theorem 1.2. If E does not have complex multiplication, then Theorem 1.2 delivers alternatives (A) or (B) from the conclusion of Proposition 3.1.

So, from now on, we assume that E has complex multiplication by some order $\mathcal{O}$ in an imaginary quadratic field. As always, we identify $\mathrm{End}(E)$ with $\mathcal{O}$ and for each $\gamma \in \mathcal{O}$, we denote by $[\gamma]$ the corresponding endomorphism of E.

If alternatives (A)–(B) do not hold in Proposition 3.1, then we may assume from now on (due to Theorem 1.2(ii)) that there exist nontrivial endomorphisms $\alpha_1, \alpha_2 \in \mathcal{O}$ such that

$$[\alpha_1](P_1) = [\alpha_2](P_2). \tag{3.1}$$

We may also assume that $\alpha_1/\alpha_2 \notin \mathbb{Q}$ since otherwise (after multiplying α_1 and α_2 in (3.1) by a suitable nonzero $\gamma \in \mathcal{O}$), we may assume α_1 and α_2 are nonzero integers and, therefore, conclusion (B) would be met. Furthermore, again multiplying by a suitable nonzero $\gamma \in \mathrm{End}(E)$, we may assume that α_1 is a nonzero integer, while $\alpha_2 \notin \mathbb{Z}$.

LEMMA 3.2. *Assume α_1 is a nonzero integer and $\alpha_2 \notin \mathbb{Z}$. Then, there exist nonzero $\gamma, \beta \in \mathcal{O}$ such that $[\gamma\alpha_1](P_1) = [\gamma\alpha_2](P_2) = [\beta](Q)$.* □

PROOF OF LEMMA 3.2. According to the hypotheses of Proposition 3.1, there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ and there exist nonzero integers $n_{i,\lambda}$ (for $i = 1, 2$) such that

$$[n_{1,\lambda}](P_{1,\lambda}) = [n_{2,\lambda}](P_{2,\lambda}) = Q_\lambda. \tag{3.2}$$

In particular,

$$[n_{1,\lambda} \cdot \alpha_1](P_{1,\lambda}) = [n_{2,\lambda} \cdot \alpha_1](P_{2,\lambda}). \tag{3.3}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

However, specialising the relation from (3.1) on the fibre corresponding to the point $\lambda \in C(\overline{\mathbb{Q}})$ (and then multiplying by $n_{1,\lambda}$) yields

$$[n_{1,\lambda} \cdot \alpha_1](P_{1,\lambda}) = [n_{1,\lambda} \cdot \alpha_2](P_{2,\lambda}). \tag{3.4}$$

Combining (3.3) and (3.4) yields

$$[n_{2,\lambda} \cdot \alpha_1 - n_{1,\lambda} \cdot \alpha_2](P_{2,\lambda}) = 0 \quad \text{(on the corresponding fibre } E_\lambda). \tag{3.5}$$

Now, because $\alpha_2 \notin \mathbb{Q}$ (and $n_{1,\lambda} \neq 0$, while $\alpha_1, n_{2,\lambda} \in \mathbb{Z}$), we obtain

$$m_\lambda := n_{2,\lambda} \cdot \alpha_1 - n_{1,\lambda} \cdot \alpha_2 \neq 0 \quad \text{in } \mathcal{O},$$

that is, the corresponding endomorphism $[m_\lambda]$ of E_λ is dominant. Therefore, from (3.5), $P_{2,\lambda}$ is a torsion point for the elliptic curve E_λ. Since $[n_{2,\lambda}](P_{2,\lambda}) = Q_\lambda$ (see (3.2)), Q_λ is also a torsion point for E_λ.

The fact that there exist infinitely many points $\lambda \in C(\overline{\mathbb{Q}})$ such that both $P_{2,\lambda}$ and Q_λ are torsion points for the elliptic curve E_λ implies (see Theorem 1.4) that there exist nonzero $\gamma, \delta \in \mathcal{O}$ such that

$$[\gamma](P_2) = [\delta](Q). \tag{3.6}$$

Combining (3.6) and (3.1) yields the desired conclusion (C) from Proposition 3.1, namely $[\alpha_1\gamma](P_1) = [\alpha_2\gamma](P_2) = [\alpha_2\delta](Q)$. This concludes our proof of Lemma 3.2. □

Lemma 3.2 finishes our proof of Proposition 3.1 by delivering the desired conclusion (C).

4. Proof of the converse implication in Theorem 1.1

In this section, we prove the following main result.

PROPOSITION 4.1. *Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{E} \to C$ be an elliptic surface and let $P_1, P_2, Q \in E(\overline{\mathbb{Q}}(C))$ be nontorsion points on the generic fibre E of π. Assume that at least one of the following three conditions holds:*

(A) *there exists a nonzero integer k such that $[k](P_i) = Q$ on E for some $i \in \{1, 2\}$;*
(B) *there exist nonzero integers k_1 and k_2 such that $[k_1](P_1) = [k_2](P_2)$ on E;*
(C) *E has complex multiplication by some order $\mathcal{O}$ in an imaginary quadratic number field and there exist nonzero $\alpha_1, \alpha_2, \beta \in \mathcal{O}$ with $\alpha_1/\alpha_2 \notin \mathbb{Q}$ such that $[\alpha_1](P_1) = [\alpha_2](P_2) = [\beta](Q)$ on E.*

Furthermore, assume that if E is isotrivial, then not all three sections $\sigma_{P_1}, \sigma_{P_2}, \sigma_Q$ are constant. Then, there exist infinitely many points $\lambda \in C(\overline{\mathbb{Q}})$ such that, for some nonzero integers $m_{1,\lambda}$ and $m_{2,\lambda}$, we have

$$[m_{1,\lambda}](P_{1,\lambda}) = [m_{2,\lambda}](P_{2,\lambda}) = Q_\lambda. \tag{4.1}$$

Combining Propositions 4.1 and 3.1, we obtain the full result in Theorem 1.1.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

We prove Proposition 4.1 as a consequence of three other results: Lemma 4.4, Lemma 4.5 and Proposition 4.6. In each of these three results, we assume one of the conditions (A)–(C) holds and then obtain the desired conclusion from (4.1). We start by stating in Lemma 4.2, a fact (proven in [15, Theorem A2]) that is used in our proofs.

4.1. A useful result. We thank Umberto Zannier once again for explaining to us how to derive Lemma 4.2 as a consequence of [15, Theorem A2].

LEMMA 4.2. *Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{E} \to C$ be an elliptic surface and let σ_P, σ_Q (corresponding to points P, Q of the generic fibre E) be sections of $\mathcal{E}$; furthermore, assume P is a nontorsion point of $E(\overline{\mathbb{Q}}(C))$. Also, if $\mathcal{E}$ is isotrivial, assume that not both sections σ_P and σ_Q are constant.*

Then, there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that $[n_\lambda](P_\lambda) = Q_\lambda$ for some nonzero integer n_λ.

The proof of Lemma 4.2 is essentially contained in [15, Theorem A2]. We explain next the small differences between our statement and that from [15]; even though [15, Theorem A2] is stated for nonisotrivial elliptic surfaces defined over $\mathbb{R}$, its proof contains all the necessary ingredients for the conclusion from Lemma 4.2.

PROOF OF LEMMA 4.2. First, we consider the special case when $\mathcal{E}$ is isotrivial *and* σ_P is a constant section. In this case, due to our assumption, σ_Q is not constant. So, in this case (at the expense of replacing C by a finite cover), $\mathcal{E} = E_0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C$ for some elliptic curve E_0 defined over $\overline{\mathbb{Q}}$; also, $P \in E_0(\overline{\mathbb{Q}})$, which means that $P = P_\lambda$ for *all* points $\lambda \in C(\overline{\mathbb{Q}})$. Due to our hypothesis, in this case, Q is *not* a constant point; hence, Q is a generic point for E_0. Hence, for any integer n, there exists some $\lambda \in C(\overline{\mathbb{Q}})$ such that $Q_\lambda = [n](P)$ on E_0 (as we identify, in this case, each fibre of $\mathcal{E}$ with E_0). Furthermore, since P is nontorsion, the points $[n](P)$ are all distinct and thus the set of λ terms for which $Q_\lambda = [n](P)$ is infinite, as desired.

So, from now on, we assume that (exactly) one the following two conditions is met:

$$\mathcal{E} \text{ is not isotrivial (and } P \in E(\overline{\mathbb{Q}}(C)) \text{ is a nontorsion point); or} \tag{4.2}$$

$$\mathcal{E} \text{ is isotrivial and } \sigma_P \text{ is not a constant section.} \tag{4.3}$$

For each $\lambda \in C(\mathbb{C})$ such that the fibre E_λ is smooth, there exists a complex analytic uniformisation map (see [33, Ch. 6]) $\exp_\lambda : \mathbb{C}/\Gamma_\lambda \to E_\lambda(\mathbb{C})$ (where Γ_λ is a lattice inside $\mathbb{C}$) with the property that

$$\exp_\lambda(nz) = [n](\exp_\lambda(z)) \text{ for each integer } n.$$

Since the analytic map $\exp_\lambda : \mathbb{C}/\Gamma_\lambda \to E_\lambda(\mathbb{C})$ is a bijection, there is a locally analytic inverse of $\exp_\lambda(z)$ (that is, the elliptic logarithm $\log_\lambda(z)$) in a small open subset of $E_\lambda(\mathbb{C})$ (with respect to the induced complex topology on $E_\lambda(\mathbb{C})$). So, our desired conclusion that $[n](P_\lambda) = Q_\lambda$ can be re-written as

$$n \cdot \log_\lambda(P_\lambda) - \log_\lambda(Q_\lambda) \in \Gamma_\lambda. \tag{4.4}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

We let $\omega_1(\lambda)$ and $\omega_2(\lambda)$ be generators for Γ_λ, which vary locally analytically (that is, when λ lives in a sufficiently small open subset of $C(\mathbb{C})$). We write $\log_\lambda(P_\lambda)$ and $\log_\lambda(Q_\lambda)$ as linear combinations with real coefficients (*Betti coordinates*) of $\omega_1(\lambda), \omega_2(\lambda)$ (for more details on Betti coordinates and their applications, see [2, 12, 13]). So, we write

$$\log_\lambda(P) = a_1(\lambda)\omega_1(\lambda) + a_2(\lambda)\omega_2(\lambda) \quad \text{and} \quad \log_\lambda(Q) = b_1(\lambda)\omega_1(\lambda) + b_2(\lambda)\omega_2(\lambda),$$

where $a_1(\lambda), a_2(\lambda), b_1(\lambda), b_2(\lambda)$ are real analytic functions and λ is a point of $C(\mathbb{C})$, which varies in a complex small disk denoted by D. We write $A(\lambda) := (a_1(\lambda), a_2(\lambda))$ and $B(\lambda) := (b_1(\lambda), b_2(\lambda))$. Then, (4.4) can be re-stated (on D) as

$$[n](P_\lambda) = Q_\lambda \quad \text{if and only if} \quad n \cdot A(\lambda) - B(\lambda) \in \mathbb{Z} \times \mathbb{Z}. \tag{4.5}$$

Now, viewing D as an open subset of $\mathbb{R}^2$, we can compute the Jacobian matrix of the function $A = (a_1, a_2) : D \to \mathbb{R}^2$. In both cases (4.2) and (4.3), the Jacobian matrix of A has rank 2 generically; when $\mathcal{E}$ is non-isotrivial, this is proven in [36, Ch. 3], while if $\mathcal{E} = E_0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C$, it follows from the fact that P is a generic point for E_0. Hence, at the expense of shrinking D, we may assume the Jacobian matrix of A has rank 2 on the entire set D. Then, for large n,

$$F_n(\lambda) := A(\lambda) - \frac{B(\lambda)}{n}$$

is real analytic on D and its Jacobian matrix has rank 2. Arguing identically as in [15, Theorem A2], for large n, $F_n(D)$ contains a nonempty open set $V \subset \mathbb{R}^2$, which is independent of n. Clearly, for large n, V contains rational points whose coordinates have denominators dividing n. More precisely, there exist at least cn^2 (for some positive real number c, depending on V, but independent of n) suitable $\lambda \in D$ such that $nF_n(\lambda) \in \mathbb{Z} \times \mathbb{Z}$. Then, (4.5) yields $[n](P_\lambda) = Q_\lambda$ for each of these cn^2 points $\lambda \in C$. As n can be chosen arbitrarily large, we obtain the desired conclusion in Lemma 4.2. □

REMARK 4.3. When $Q = 0 \in E$ and E is an elliptic curve defined over a number field K, a stronger version of Lemma 4.2 was studied in the context of *primary primes* for an elliptic divisibility sequence. One views E as the generic fibre of an elliptic arithmetic surface $\pi : \mathcal{E} \to \mathrm{Spec}(O_K)$ (where O_K is the ring of algebraic integers in K). Also, for any given point $R \in E(K)$, one considers the corresponding section σ_R of π and for a prime v of O_K (of good reduction), we denote by $R_v := \sigma_R(v)$ the corresponding specialisation of R at the place v. Then, it was proven (see [25, 26]) that for all sufficiently large positive integers n, there exists a (non-Archimedean) place v_n of K (such that the fibre $\pi^{-1}(v_n) =: E_{v_n}$ is smooth) with the property that on E_{v_n},

$$[n](P_{v_n}) = 0 \quad \text{and, moreover,} \quad [m](P_{v_n}) \neq 0 \quad \text{when } 0 < m < n.$$

The existence of primary primes for all sufficiently large positive integers n is a *stronger* conclusion than the fact that there are infinitely many primes v of O_K for which there exists *some* positive integer n such that $[n](P_v) = 0$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

Verzobio [35] extended the study of primary primes by considering a target point $Q \neq 0$. Under the hypothesis that the target point Q is dynamically related to the starting point P (that is, $\Phi(P) = \Psi(Q)$ for some nontrivial endomorphisms $\Phi, \Psi \in \mathrm{End}(E)$), Verzobio [35] proved that again for all sufficiently large positive integers n, there exists a prime v_n of O_K such that

$$[n](P_{v_n}) = Q_{v_n} \quad \text{and, moreover,} \quad [m](P_{v_n}) \neq Q_{v_n} \quad \text{when } 0 < m < n.$$

Furthermore, Matteo Verzobio confirmed to us that his method extends almost verbatim to cover the function field case (that is, when E is an elliptic curve defined over $\overline{\mathbb{Q}}(C)$, which is the setting of Lemma 4.2); the necessary ingredients for modifying the argument from [35] to the function field case are contained in the papers [30, 34].

4.2. Proof of Proposition 4.1 assuming conditions (A) or (B) hold. The following result is an easy consequence of Lemma 4.2.

LEMMA 4.4. *The conclusion in Proposition 4.1 holds assuming condition (A) is satisfied.*

PROOF. Without loss of generality, assume there exists a nonzero integer k such that $[k](P_1) = Q$; in particular, this means that for *all* points $\lambda \in C(\overline{\mathbb{Q}})$ (for which the corresponding fibre E_λ is an elliptic curve), we have $[k](P_{1,\lambda}) = Q_\lambda$. However, Lemma 4.2 yields infinitely many points $\lambda \in C(\overline{\mathbb{Q}})$ along with nonzero integers n_λ such that $[n_\lambda](P_{2,\lambda}) = Q_\lambda$.

Note that if $\mathcal{E}$ is isotrivial, *not* both sections σ_{P_2} and σ_Q are constant since otherwise, σ_{P_1} is constant (since $[k](P_1) = Q$ for a nonzero integer k), which contradicts one of the hypotheses in Proposition 4.1. Thus, indeed, we can apply Lemma 4.2 to the triple $(\mathcal{E}, P_2, Q)$. This concludes our proof of Lemma 4.4. □

LEMMA 4.5. *The conclusion in Proposition 4.1 holds assuming condition (B) is satisfied.*

PROOF. There exist nonzero integers k_1 and k_2 such that $[k_1](P_1) = [k_2](P_2)$. Arguing as in the proof of Lemma 4.4 shows that the hypotheses from Lemma 4.2 are met by the triple $(\mathcal{E}, [k_1](P_1), Q)$. Indeed, if $\mathcal{E} = E_0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C$ (for some elliptic curve E_0 defined over $\overline{\mathbb{Q}}$) and both $[k_1](P_1)$ and Q were points in $E_0(\overline{\mathbb{Q}})$, then also $P_1, P_2 \in E_0(\overline{\mathbb{Q}})$ (note that $[k_1](P_1) = [k_2](P_2)$ and $k_1 k_2 \neq 0$).

Now, applying Lemma 4.2 to the points $[k_1](P_1)$ and Q yields the existence of infinitely many points $\lambda \in C(\overline{\mathbb{Q}})$ along with nonzero integers n such that

$$[nk_1](P_{1,\lambda}) = Q_\lambda. \tag{4.6}$$

From (4.6), $[nk_2](P_{2,\lambda}) = Q_\lambda$, thus providing the desired conclusion in Proposition 4.1. □

So, to complete the proof of Proposition 4.1, it suffices to prove conclusion (4.1) using hypothesis (C).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

4.3. Proof of Proposition 4.1 assuming condition (C) holds. So, E is a CM elliptic curve whose endomorphism ring is identified with an order $\mathcal{O} = \mathbb{Z}[\theta]$ in an imaginary quadratic field (see (2.1) for the definition of θ).

PROPOSITION 4.6. *With the notation as in Proposition 4.1, assume in addition that E has complex multiplication by $\mathcal{O} = \mathbb{Z}[\theta]$. Also, we assume there exist nonzero $\alpha_1, \alpha_2, \beta \in \mathcal{O}$ with $\alpha_1/\alpha_2 \notin \mathbb{Q}$ such that*

$$[\alpha_1](P_1) = [\alpha_2](P_2) = [\beta](Q) \quad (\text{in } E). \tag{4.7}$$

Then, there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ with the property that there exist nonzero integers $m_{1,\lambda}, m_{2,\lambda}$ such that

$$[m_{1,\lambda}](P_{1,\lambda}) = [m_{2,\lambda}](P_{2,\lambda}) = Q_\lambda.$$

PROOF. First, we note that since E has CM, its j-invariant must be contained in $\overline{\mathbb{Q}}$ (see [31, Ch. 2]), that is, $\mathcal{E}$ is isotrivial. So, the hypothesis from Proposition 4.1 shows that at least one of the sections $\sigma_{P_1}, \sigma_{P_2}, \sigma_Q$ is not constant. However, due to relation (4.7), *none* of these three sections is constant.

Let $M := N(\alpha_1) \cdot N(\alpha_2) \cdot N(\beta)$, where $N(\cdot)$ is the usual norm for $\mathbb{Q}(i\sqrt{D})$ (see (2.2)). Let $\ell \in \{1, \dots, M\}$ satisfy the conclusion of Lemma 2.5, that is, for each (odd) integer a satisfying $a \equiv 2\ell - 1 \pmod{2M}$,

$$\gcd(N(a + 4\theta), 2M) = 1.$$

LEMMA 4.7. *There exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ with the property that there exists some positive integer a_λ such that $a_\lambda \equiv 2\ell - 1 \pmod{2M}$ and $[a_\lambda + 4\theta](Q_\lambda) = 0$.*

PROOF OF LEMMA 4.7. Letting $a_\lambda = 2Mn_\lambda + (2\ell - 1)$ (for some $n_\lambda \in \mathbb{N}$), we can re-write the conclusion from Lemma 4.7 as

$$[n_\lambda]([2M](Q_\lambda)) = [1 - 2\ell - 4\theta](Q_\lambda).$$

The desired conclusion in Lemma 4.7 follows from Lemma 4.2 applied to the starting point $[2M](Q)$ and with the target point $[1 - 2\ell - 4\theta](Q)$ (note the hypotheses from Lemma 4.2 are met because σ_Q is not a constant section). □

Now, choose a point $\lambda \in C(\overline{\mathbb{Q}})$ along with a suitable positive integer a_λ as in the conclusion of Lemma 4.7; we let U_λ be the cyclic subgroup of E_λ generated by Q_λ. Corollary 2.4(i) shows that for any $\gamma \in \mathcal{O}$, we have a natural induced group homorphism $\widetilde{[\gamma]} : U_\lambda \longrightarrow U_\lambda$ given by $Q \mapsto [\gamma](Q)$. Furthermore, Corollary 2.4(ii) shows that $\widetilde{[\beta]}$, $\widetilde{[\bar{\alpha}_1]}$ and $\widetilde{[\bar{\alpha}_2]}$ are group automorphisms of U_λ.

LEMMA 4.8. *With the above notation,*

$$[N(\alpha_1)](P_{1,\lambda}),\ [N(\alpha_2)](P_{2,\lambda}) \in U_\lambda. \tag{4.8}$$

Moreover, both $[N(\alpha_1)](P_{1,\lambda})$ and $[N(\alpha_2)](P_{2,\lambda})$ are generators for the cyclic group U_λ.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

PROOF OF LEMMA 4.8. Let $i \in \{1, 2\}$. Equation (4.7) yields $[\alpha_i](P_{i,\lambda}) \in U_\lambda$ and, therefore, also $[\bar{\alpha}_i \cdot \alpha_i](P_{i,\lambda}) \in U_\lambda$; thus, we obtain the conclusion from (4.8). Furthermore, we have the more precise relation coming from (4.7):

$$[N(\alpha_i)](P_{i,\lambda}) = [\bar{\alpha}_i \cdot \beta](Q_\lambda).$$

Because the induced maps $\widetilde{[\bar{\alpha}_i]}$ and $\widetilde{[\beta]}$ are group automorphisms of U_λ, we see that $[N(\alpha_i)](P_{i,\lambda})$ is a generator for the cyclic group U_λ (for each $i = 1, 2$).

This concludes our proof of Lemma 4.8. □

Lemma 4.8 yields the existence of positive integers $k_{1,\lambda}$ and $k_{2,\lambda}$ such that

$$[k_{1,\lambda}N(\alpha_1)](P_{1,\lambda}) = [k_{2,\lambda}N(\alpha_2)](P_{2,\lambda}) = Q_\lambda. \tag{4.9}$$

Equation (4.9) along with the fact that there exist infinitely many such points $\lambda \in C(\overline{\mathbb{Q}})$ (according to Lemma 4.7) deliver the desired conclusion in Proposition 4.6. □

As previously explained, Lemmas 4.4 and 4.5, along with Proposition 4.6 finish our proof of Proposition 4.1.

Acknowledgements

First of all, we warmly thank Umberto Zannier for his always generous sharing of beautiful mathematical ideas, which led to writing this paper. We are grateful to the anonymous referee for useful comments and suggestions. We also thank Laura Capuano, Simone Coccia, Patrick Ingram and Matteo Verzobio for helpful conversations.

References

[1] N. Ailon and Z. Rudnick, 'Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$', *Acta Arith,* **113**(1) (2004), 31–38.
[2] Y. André, P. Corvaja and U. Zannier, 'The Betti map associated to a section of an abelian scheme', *Invent. Math.* **222**(1) (2020), 161–202.
[3] S. Asgarli and D. Ghioca, 'Collision of orbits for families of polynomials defined over fields of positive characteristic', *Math. Z.* **313**(2) (2026), Article no. 29, 39 pages.
[4] M. H. Baker and L. DeMarco, 'Preperiodic points and unlikely intersections', *Duke Math. J.* **159**(1) (2011), 1–29.
[5] M. H. Baker and L. DeMarco, 'Special curves and postcritically finite polynomials', *Forum Math. Pi* **1** (2013), Article no. e3, 35 pages.
[6] F. Barroero and L. Capuano, 'Linear relations in families of powers of elliptic curves', *Algebra Number Theory* **10**(1) (2016), 195–214.
[7] F. Barroero and L. Capuano, 'Unlikely intersections in products of families of elliptic curves and the multiplicative group', *Quart. J. Math. Oxford Ser. (2)* **68**(4) (2017), 1117–1138.
[8] F. Barroero and L. Capuano, 'Unlikely intersections in families of abelian varieties and the polynomial Pell equation', *Proc. Lond.Math. Soc. (3)* **120**(2) (2020), 192–219.
[9] F. Barroero, L. Capuano and A. Turchet, 'Greatest common divisor results on semiabelian varieties and a conjecture of Silverman', *Res. Number Theory* **10**(1) (2024), Article no. 17, 16 pages.
[10] R. L. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman and T. J. Tucker, 'Current trends and open problems in arithmetic dynamics', *Bull. Amer. Math. Soc. (N.S.)* **56**(4) (2019), 611–685.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

[11] Y. Bugeaud, P. Corvaja and U. Zannier, 'An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$', *Math. Z.* **243** (2003), 79–84.
[12] P. Corvaja, J. Demeio, D. Masser and U. Zannier, 'On the torsion values for sections of an elliptic scheme', *J. reine angew. Math.* **782** (2022), 1–41.
[13] P. Corvaja, D. Masser and U. Zannier, 'Torsion hypersurfaces on abelian schemes and Betti coordinates', *Math. Ann.* **371**(3-4) (2018), 1013–1045.
[14] P. Corvaja and U. Zannier, 'Greatest common divisors of $u - 1$, $v - 1$ in positive characteristic and rational points on curves over finite fields', *J. Eur. Math. Soc. (JEMS)* **15**(5) (2013), 1927–1942.
[15] P. Corvaja and U. Zannier, 'Finiteness theorems on elliptical billiards and a variant of the dynamical Mordell–Lang conjecture', *Proc. Lond. Math. Soc. (3)* **127**(5) (2023), 1268–1337.
[16] L. DeMarco and N. M. Mavraki, 'Variation of canonical height and equidistribution', *Amer. J. Math.* **142**(2) (2020), 443–473.
[17] C. Favre and T. Gauthier, *The Arithmetic of Polynomial Dynamical Pairs*, Annals of Mathematics Studies, 214 (Princeton University Press, Princeton, NJ, 2022).
[18] D. Ghioca, 'Unlikely intersections in arithmetic dynamics', *CMS Notes* **49**(4) (2017), 12–13.
[19] D. Ghioca, 'Collision of orbits for a one-parameter family of Drinfeld modules', *J. Number Theory* **257** (2024), 320–340.
[20] D. Ghioca, 'Simultaneously preperiodic points for a family of polynomials in positive characteristic', *Canad. J. Math.* **78**(1) (2026), 199–221.
[21] D. Ghioca, L.-C. Hsia and T. J. Tucker, 'Preperiodic points for families of polynomials', *Algebra Number Theory* **7**(3) (2013), 701–732.
[22] D. Ghioca, L.-C. Hsia and T. J. Tucker, 'On a variant of the Ailon–Rudnick theorem in finite characteristic', *New York J. Math.* **23** (2017), 213–225.
[23] D. Ghioca, L.-C. Hsia and T. J. Tucker, 'A variant of a theorem by Ailon–Rudnick for elliptic curves', *Pacific J. Math.* **295**(1) (2018), 1–15.
[24] L.-C. Hsia and T. J. Tucker, 'Greatest common divisors of iterates of polynomials', *Algebra Number Theory* **11**(6) (2017), 1437–1459.
[25] P. Ingram, 'Elliptic divisibility sequences over certain curves', *J. Number Theory* **123**(2) (2007), 473–486.
[26] P. Ingram and J. H. Silverman, 'Primitive divisors in arithmetic dynamics', *Math. Proc. Cambridge Philos. Soc.* **146**(2) (2009), 289–302.
[27] F. Luca, 'On the greatest common divisor of $u - 1$ and $v - 1$ with u and v near S-units', *Monatsh. Math.* **146**(3) (2005), 239–256.
[28] D. W. Masser and U. Zannier, 'Torsion anomalous points and families of elliptic curves', *Amer. J. Math.* **132**(6) (2010), 1677–1691.
[29] D. W. Masser and U. Zannier, 'Torsion points on families of squares of elliptic curves', *Math. Ann.* **352**(2) (2012), 453–484.
[30] B. Naskrecki, 'Divisibility sequences of polynomials and heights estimates', *New York J. Math.* **22** (2016), 989–1020.
[31] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer-Verlag, New York, 1994).
[32] J. H. Silverman, 'Common divisors of elliptic divisibility sequences over function fields', *Manuscripta Math.* **114**(4) (2004), 431–446.
[33] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106, 2nd edn (Springer, Dordrecht, 2009).
[34] R. Slob, 'Primitive divisors of sequences associated to elliptic curves over function fields', *New York J. Math.* **28** (2022), 230–249.
[35] M. Verzobio, 'Primitive divisors of sequences associated to elliptic curves with complex multiplication', *Res. Number Theory* **7**(2) (2021), Article no. 37, 29 pages.
[36] U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, with appendixes by David Masser, Annals of Mathematics Studies, 181 (Princeton University Press, Princeton, NJ, 2012).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592

DRAGOS GHIOCA, Department of Mathematics,
University of British Columbia, Vancouver, BC V6T 1Z2, Canada
e-mail: dghioca@math.ubc.ca

NEGIN SHADGAR, Department of Mathematics,
University of British Columbia, Vancouver, BC V6T 1Z2, Canada
e-mail: negin@math.ubc.ca

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 04:04:15, subject to the Cambridge Core terms of use
, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101592