

COLLISION OF ORBITS ON AN ELLIPTIC SURFACE

DRAGOS GHIOCA AND NEGIN SHADGAR

ABSTRACT. Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\pi : \mathcal{E} \rightarrow C$ 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 fiber E of \mathcal{E}). We obtain a precise characterization, 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 for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, we have that $[m_{i,\lambda}](\sigma_{P_i}(\lambda)) = \sigma_Q(\lambda)$ (for $i = 1, 2$) on the smooth fiber E_λ of \mathcal{E} .

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 $\text{End}(E)$ the ring of group endomorphisms of E (defined over an algebraic closure \overline{L} of L). It is known (see [Sil07, Chapter 2]) that $\text{End}(E)$ 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 $\text{End}(E)$ 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 $[n]$ (resp. $[\alpha]$) the corresponding endomorphism of E .

Throughout our paper, C is a smooth, projective (irreducible) curve defined over $\overline{\mathbb{Q}}$. Also, we consider $\pi : \mathcal{E} \rightarrow C$ be an elliptic surface, where the generic fiber 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 fiber $E_\lambda := \pi^{-1}(\{\lambda\})$ is an elliptic curve defined over $\overline{\mathbb{Q}}$. We will often refer to E_λ as the λ -*fiber* of π . Each section σ of π (i.e. a map $\sigma : C \rightarrow \mathcal{E}$ such that $\pi \circ \sigma = \text{id}|_C$) 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 fiber E_λ above λ is a point $P_\lambda := \sigma_P(\lambda)$ on the elliptic curve E_λ ; we will refer to P_λ as the λ -*specialization of the point* P and we 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 -specialization of P_i .

We say that \mathcal{E} is *isotrivial* if the j -invariant (see [Sil07, Chapter 3]) of the generic fiber E is a constant function (on C); for isotrivial elliptic surfaces \mathcal{E} , all smooth fibers 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 $\mathcal{E} = E_0 \times_{\text{Spec}(\overline{\mathbb{Q}})} C$. In this case, we say that a section σ_P of \mathcal{E} is *constant* if $P \in E_0(\overline{\mathbb{Q}})$.

2020 *Mathematics Subject Classification.* Primary 37P15; Secondary 11G35.

Key words and phrases. elliptic surfaces; unlikely intersections; collision of orbits.

In our paper, we study the following question for elliptic surfaces $\mathcal{E} \rightarrow C$ defined over $\overline{\mathbb{Q}}$; as before, we denote by E the generic fiber 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 non-torsion), we obtain necessary and sufficient conditions (in terms of the dynamics of P_1, P_2, Q under the action of $\text{End}(E)$) 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 $\mathcal{E} \rightarrow C$ be an elliptic surface and let $P_1, P_2, Q \in E(\overline{\mathbb{Q}}(C))$ be non-torsion points on the generic fiber E of π . Furthermore, if \mathcal{E} is isotrivial, then 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 for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, we have that $[m_{i,\lambda}](P_{i,\lambda}) = Q_\lambda$ on the λ -fiber 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 for some $i \in \{1, 2\}$, we have $[k](P_i) = Q$ on E .*
- (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 strenghtens the main result of [GHT18, Theorem 1.1], which we state below as Theorem 1.2.

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 for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, we have that $[m_{i,\lambda}](P_{i,\lambda}) = Q_\lambda$ (for $i = 1, 2$) on the λ -fiber E_λ of π , then at least one of the following two conditions holds:*

- (i) *there exists a nonzero integer k such that for some $i \in \{1, 2\}$, we have $[k](P_i) = Q$;*
- (ii) *there exist nontrivial endomorphisms $\alpha_1, \alpha_2 \in \text{End}(E)$ 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 $\mathcal{E} = E_0 \times_{\text{Spec}(\overline{\mathbb{Q}})} C$, if $P_1, P_2, Q \in E_0(\overline{\mathbb{Q}})$ then the problem considered in Theorem 1.1 loses its relevance since we have in this case (no matter what is the fiber 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 $i = 1, 2$).

Our Theorem 1.1 fits into the larger theme of unlikely intersections in arithmetic dynamics, as we will explain below.

1.3. Unlikely intersections in arithmetic dynamics. The following result was proved by Masser-Zannier (see [MZ10, MZ12]); an alternative proof was derived by DeMarco-Mavraki (see [DM20]).

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

So, 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 [Zan12]).

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 [CZ23, 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 $\lambda \in C(\overline{\mathbb{Q}})$, we have that 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 non-torsion 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 non-torsion 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 non-torsion. 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 for some suitable nonzero integers $m_{1,\lambda}$, we have $[m_{1,\lambda}](P_{1,\lambda}) = Q_\lambda$ yields that also $[\ell](Q_\lambda) = 0$ for those λ 's. So, by the Pigeonhole Principle, there exists some torsion point R of E (such that $[\ell](R) = 0$) with the property that for infinitely many $\lambda \in C(\overline{\mathbb{Q}})$, we have $R_\lambda = Q_\lambda$. This means that $R = Q$, contradicting the assumption that Q is non-torsion. Therefore, the assumption that all three points P_1, P_2, Q are non-torsion is justified for Theorem 1.1.

The results of Masser-Zannier [MZ10, MZ12] (see Theorem 1.4 above) were the catalysts for an intense study in arithmetic dynamics of unlikely intersection questions (see the survey article [BIJMST19] for a more in-depth discussion of it as one of the central questions in arithmetic dynamics and also, see the book [Zan12] for a thorough study of the origins of the unlikely intersection questions in arithmetic geometry). In particular, the so-called question of *simultaneously preperiodic points* generated a great deal of research in recent years (see [BD11, BD13, GHT13, Ghi26] and the references therein). So, consider a family $F_\lambda(z)$ of polynomials parameterized by the \mathbb{C} -points λ on some projective smooth curve C ; also, let $\mathbf{a}, \mathbf{b} : C \rightarrow \mathbb{P}^1$. Then one obtains (see [FG02]) a complete characterization (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 the above 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* $\mathbf{c} : C \rightarrow \mathbb{P}^1$ and then asks for a precise characterization 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 $F_\lambda(z)$ (i.e., 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 as the *collision of orbits question* (see [AG, Ghi24]). Using the same strategy patented in [BD11] (and further refined in the subsequent papers [BD13, GHT13]), one can obtain global conditions which are *necessary* for this collision of orbits question; however, obtaining precise *necessary and sufficient* conditions is much more delicate compared to the previous question of simultaneously preperiodic points (see the discussion from both [AG, Remark 2.8] and [Ghi24, 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 $\text{End}(E_\lambda)$.

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 [HT17]. 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 [HT17, Theorem 1] establishes that there exist finitely many $\lambda \in \mathbb{C}$ such that

$$(1.4.1) \quad (z - \lambda) \mid \gcd(\mathbf{a}^m(z) - \mathbf{c}(z), \mathbf{b}^n(z) - \mathbf{c}(z)) \text{ for some } m, n \in \mathbb{N}.$$

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 [AG, Section 9]). This has its origins in the problem studied by Ailon-Rudnick [AR04], 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

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

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

In turn, the result of Ailon-Rudnick was motivated by the work of Bugeaud-Corvaja-Zannier [BCZ03] who established an upper bound for $\gcd(a^k - 1, b^k - 1)$ (as k varies in \mathbb{N}) for given $a, b \in \mathbb{Q}$. We also mention that this problem of bounding the greatest common divisor has been studied in several other directions as well: for elements close to S -units (see [CZ13, Luc05]), for polynomials defined over fields of positive characteristic (see [GHT17]), and also, for elliptic divisibility sequences (see [Sil04]). Furthermore, one of the open questions raised in [Sil04] was answered in the affirmative in [GHT18, Theorem 1.1] (stated above as Theorem 1.2).

1.5. Plan for our paper. Most of the work for obtaining the direct implication in Theorem 1.1 was done in [GHT18, Theorem 1.1] (see Theorem 1.2 above). 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 one of the three conditions (A), (B) and (C) (see Lemmas 4.4 and 4.5 and Proposition 4.6) and show that in each case there exist infinitely many points $\lambda \in C(\mathbb{Q})$ such that Q_λ is (an integer) multiple of both $P_{1,\lambda}$ and of $P_{2,\lambda}$. Once again, when the elliptic surface admits complex

multiplication (i.e., 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).

Acknowledgments. First of all, we thank warmly Umberto Zannier for his always generous sharing of beautiful mathematical ideas, which led to writing this paper. We are also grateful to Simone Coccia, Patrick Ingram and Matteo Verzobio for helpful conversations. The research of the first author was partially supported by a Discovery Grant from the NSERC.

2. ARITHMETIC PROPERTIES FOR 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; i.e., $\mathcal{O} = \mathbb{Z}[\theta]$, where (for some $f \in \mathbb{N}$ and some square-free positive integer D) we have:

$$(2.0.1) \quad \theta = \begin{cases} f \cdot i\sqrt{D} & \text{if } D \not\equiv 3 \pmod{4} \\ f \cdot \frac{1+i\sqrt{D}}{2} & \text{if } D \equiv 3 \pmod{4} \end{cases}$$

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

$$(2.0.2) \quad N(a + b\theta) = (a + b\theta) \cdot (a + b\bar{\theta}),$$

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

In our proof, we will employ the following easy facts (see Lemmas 2.1 and 2.3) regarding the arithmetic of the ring \mathcal{O} .

Lemma 2.1. *With D, θ as in equation (2.0.1), let also a be an odd integer. Then there exist $m, r, s \in \mathbb{Z}$ such that*

$$(2.0.3) \quad m - \theta = (a + 4\theta) \cdot (r + s\theta).$$

Proof. We prove the desired conclusion for each of the two possible values for θ (see equation (2.0.1)). So, if $\theta = f \cdot i\sqrt{D}$, then (using the fact that $\theta^2 = -f^2D$), equation (2.0.3) simply asks that there exist $r, s \in \mathbb{Z}$ such that

$$(2.0.4) \quad -1 = as + 4r.$$

Equation (2.0.4) holds (for some suitable $r, s \in \mathbb{Z}$) because a is odd. Hence, we are left to analyze the second case for θ from equation (2.0.1). Now, when $\theta = f \cdot \frac{1+i\sqrt{D}}{2}$, then using that

$$a + 4\theta = (a + 2f) + i \cdot 2f\sqrt{D} \text{ and } r + s\theta = \left(r + \frac{sf}{2}\right) + i \cdot \frac{sf\sqrt{D}}{2},$$

we get the desired conclusion in Lemma 2.1, if there exist $m, r, s \in \mathbb{Z}$ such that

$$(2.0.5) \quad m - \frac{f}{2} = ar + \frac{asf}{2} + 2rf + sf^2 - sf^2D \quad \text{and}$$

$$(2.0.6) \quad -1 = (a + 2f)s + 4r + 2fs, \text{ i.e., } -1 = as + 4r + 4fs.$$

The existence of some $m \in \mathbb{Z}$ satisfying equation (2.0.5) is guaranteed once as is odd (regardless what is the value for r), which is true whenever s is odd (because we already know that a is odd). On the other hand, there exists an integer r satisfying equation (2.0.6) as long as

$$(2.0.7) \quad 4 \mid 1 + as.$$

Therefore, it suffices to choose an odd integer s satisfying equation (2.0.7) (again, note that a is odd) and then we can guarantee the existence of some integers m and r satisfying conditions (2.0.5) and (2.0.6).

This concludes our proof of Lemma 2.1. \square

Lemma 2.1 allows us to derive the following easy consequence.

Corollary 2.2. *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) $[\alpha](Q) \in U$, i.e., $[\alpha]$ induces a natural group homomorphism $[\widetilde{\alpha}]$ on U given by $[\alpha](Q) = [\widetilde{\alpha}](Q)$.
- (ii) if $\gcd(N(a+4\theta), N(\alpha)) = 1$, then $[\widetilde{\alpha}] : U \rightarrow U$ is a group automorphism.

Proof. Using Lemma 2.1, we know there exist $m, r, s \in \mathbb{Z}$ such that

$$(2.0.8) \quad m - \theta = (a + 4\theta) \cdot (r + s\theta).$$

Equation (2.0.8) (along with the fact $[a+4\theta](Q) = 0$) shows that $[\theta](Q) = [m](Q)$, i.e., $[\theta]$ induces the natural group homomorphism $[\widetilde{\theta}]$ on U given by

$$(2.0.9) \quad [\widetilde{\theta}](Q) = [m](Q).$$

In particular, this means that writing $\alpha := c + d\theta$ (for some $c, d \in \mathbb{Z}$), then $[\alpha]$ induces a group homomorphism $[\widetilde{\alpha}]$ on U . More precisely, equation (2.0.9) yields that

$$(2.0.10) \quad [\alpha](Q) = [c + dm](Q).$$

Equation (2.0.10) proves conclusion (i) of Corollary 2.2.

Now, assuming that $\gcd(N(a+4\theta), N(\alpha)) = 1$, we get 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 $[\widetilde{\alpha}]$ induce the group homomorphisms $[\widetilde{\alpha}]$ and $[\widetilde{\widetilde{\alpha}}]$ on U for which

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

Therefore, $[\widetilde{\alpha}]$ is a group automorphism of U , as desired for part (ii) of the conclusion in Corollary 2.2. \square

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 2.2 in our proof of Proposition 4.6 (which will deliver the converse implication in Theorem 1.1 for CM elliptic curves).

Lemma 2.3. *Let M be a positive integer. Then there exists $\ell \in \{1, \dots, M\}$ such that for each integer $a \in \mathbb{Z}$ satisfying*

$$(2.0.11) \quad a \equiv 2\ell - 1 \pmod{2M},$$

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

Proof. Once again, we split our analysis based on the two cases appearing for θ as in the formulas (2.0.1). Also, just as in the proof of Lemma 2.1, the case when $\theta = f \cdot i\sqrt{D}$ is easier than the case when $\theta = f \cdot \frac{1+i\sqrt{D}}{2}$ (and $D \equiv 3 \pmod{4}$); therefore, we will focus below on the latter case (especially, since the analysis for the former case is similar). So, using equation (2.0.2), we have that

$$(2.0.12) \quad N(a + 4\theta) = N\left(a + 2f + i \cdot 2f\sqrt{D}\right) = (a + 2f)^2 + 4f^2D.$$

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 $r_p \in \{0, 1, \dots, p-1\}$ such that if $a \equiv r_p \pmod{p}$, then $p \nmid N(a + 4\theta)$ (see equation (2.0.12)). Noting that $r_2 = 1$ (i.e., a has to be odd so that $N(a + 4\theta)$ is odd), we obtain the desired conclusion from Lemma 2.3. \square

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 $\mathcal{E} \rightarrow C$ be an elliptic surface and let $P_1, P_2, Q \in E(\mathbb{Q}(C))$ be non-torsion points on the generic fiber E of π . Assume there exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ such that for some nonzero integers $m_{1,\lambda}, m_{2,\lambda}$, we have that $[m_{i,\lambda}](P_{i,\lambda}) = Q_\lambda$ on the λ -fiber E_λ of π . Then at least one of the following three conditions must hold:*

- (A) *there exists a nonzero integer k such that for some $i \in \{1, 2\}$, we have $[k](P_i) = Q$ on E .*
- (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 .*

We note that Proposition 3.1 provides the direct implication in Theorem 1.1 without the non-constant 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. Therefore, 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 $\text{End}(E)$ with \mathcal{O} and for each $\gamma \in \mathcal{O}$, we denote by $[\gamma]$ the corresponding endomorphism of E .

Now, 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

$$(3.0.1) \quad [\alpha_1](P_1) = [\alpha_2](P_2).$$

We may also assume that $\frac{\alpha_1}{\alpha_2} \notin \mathbb{Q}$ since otherwise (after multiplying α_1 and α_2 in equation (3.0.1) 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 $\gamma \in \text{End}(E)$, 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

$$(3.0.2) \quad [n_{1,\lambda}](P_{1,\lambda}) = [n_{2,\lambda}](P_{2,\lambda}) = Q_\lambda.$$

In particular, we get

$$(3.0.3) \quad [n_{1,\lambda} \cdot \alpha_1](P_{1,\lambda}) = [n_{2,\lambda} \cdot \alpha_1](P_{2,\lambda}).$$

On the other hand, specializing the relation from equation (3.0.1) on the fiber corresponding to the point $\lambda \in C(\overline{\mathbb{Q}})$ (and then multiplying by $n_{1,\lambda}$) yields

$$(3.0.4) \quad [n_{1,\lambda} \cdot \alpha_1](P_{1,\lambda}) = [n_{1,\lambda} \cdot \alpha_2](P_{2,\lambda}).$$

Combining equations (3.0.3) and (3.0.4) yields

$$(3.0.5) \quad [n_{2,\lambda} \cdot \alpha_1 - n_{1,\lambda} \cdot \alpha_2](P_{2,\lambda}) = 0 \text{ (on the corresponding fiber } E_\lambda).$$

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

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

i.e., the corresponding endomorphism $[m_\lambda]$ of E_λ is dominant. Therefore, equation (3.0.5) yields that $P_{2,\lambda}$ is a torsion point for the elliptic curve E_λ . Then knowing that $[n_{2,\lambda}](P_{2,\lambda}) = Q_\lambda$ (see equation (3.0.2)) yields that also Q_λ is a torsion point for E_λ .

Now, 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 yields (see Theorem 1.4) that there exist nonzero $\gamma, \delta \in \mathcal{O}$ such that

$$(3.0.6) \quad [\gamma](P_2) = [\delta](Q).$$

Combining equations (3.0.6) and (3.0.1) yields the desired conclusion (C) from Proposition 3.1:

$$[\alpha_1\gamma](P_1) = [\alpha_2\gamma](P_2) = [\alpha_2\delta](Q).$$

This concludes our proof of Lemma 3.2. \square

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

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 $\mathcal{E} \rightarrow C$ be an elliptic surface and let $P_1, P_2, Q \in E(\overline{\mathbb{Q}}(C))$ be non-torsion points on the generic fiber E of π . Assume that at least one of the following three conditions holds:*

- (A) *there exists a nonzero integer k such that for some $i \in \{1, 2\}$, we have $[k](P_i) = Q$ on E .*
- (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

$$(4.0.1) \quad [m_{1,\lambda}](P_{1,\lambda}) = [m_{2,\lambda}](P_{2,\lambda}) = Q_\lambda.$$

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

We will prove Proposition 4.1 as a consequence of three other results: Lemmas 4.4 and 4.5, along with Proposition 4.6; in each one of these three results, we assume one of the conditions (A)-(C) hold and then obtain the desired conclusion from equation (4.0.1). We start by stating in Lemma 4.2 a fact (proven in [CZ23, Theorem A2]), which will be used in our proofs.

4.1. A useful result. We thank once again Umberto Zannier for explaining to us how to derive Lemma 4.2 as a consequence of [CZ23, Theorem A2].

Lemma 4.2. *Let C be a smooth projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{E} \rightarrow C$ be an elliptic surface and let sections σ_P, σ_Q (corresponding to points P, Q of the generic fiber E) of \mathcal{E} ; furthermore, assume P is a non-torsion 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 for some nonzero integer n_λ , we have that $[n_\lambda](P_\lambda) = Q_\lambda$.

The proof of Lemma 4.2 is essentially contained in [CZ23, Theorem A2]. We explain next the small differences between our statement and the one from [CZ23]; even though [CZ23, Theorem A2] is stated for non-isotrivial 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, we have that σ_Q is not constant. So, in this case (at the expense of replacing C by a finite cover), we have $\mathcal{E} = E_0 \times_{\text{Spec}(\overline{\mathbb{Q}})} C$ for some elliptic curve E_0 defined over $\overline{\mathbb{Q}}$; also, we have that $P \in E_0(\overline{\mathbb{Q}})$, which means that $P = P_\lambda$ for all points $\lambda \in C(\overline{\mathbb{Q}})$. Also, due to our hypothesis, in this case we know that 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 fiber of \mathcal{E} with E_0). Furthermore, since P is non-torsion, the points $[n](P)$ are all distinct and thus, also the set of λ 's 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:

$$(4.1.1) \quad \mathcal{E} \text{ is not isotrivial (and } P \in E(\overline{\mathbb{Q}}(C)) \text{ is a non-torsion point); or}$$

$$(4.1.2) \quad \mathcal{E} \text{ is isotrivial, and } \sigma_P \text{ is not a constant section.}$$

For each $\lambda \in C(\mathbb{C})$ such that the fiber E_λ is smooth, there exists a complex analytic uniformization map (see [Sil07, Chapter 6]) $\exp_\lambda : \mathbb{C}/\Gamma_\lambda \rightarrow E_\lambda(\mathbb{C})$ (where Γ_λ is a lattice inside \mathbb{C}) with the property that

$$(4.1.3) \quad \exp_\lambda(nz) = [n](\exp_\lambda(z)) \text{ for each integer } n.$$

Since the analytic map $\exp_\lambda : \mathbb{C}/\Gamma_\lambda \rightarrow E_\lambda(\mathbb{C})$ is a bijection, there is a locally analytic inverse of $\exp_\lambda(z)$ (i.e., 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 follows:

$$(4.1.4) \quad n \cdot \log_\lambda(P_\lambda) - \log_\lambda(Q_\lambda) \in \Gamma_\lambda.$$

We let $\omega_1(\lambda)$ and $\omega_2(\lambda)$ be generators for Γ_λ , which vary locally analytically (i.e., 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 [ACZ20, CMZ18, CDMZ22]). So, we write

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

where $a_1(\lambda), a_2(\lambda), b_1(\lambda), b_2(\lambda)$ are real analytic functions, where λ is a point of $C(\mathbb{C})$, which varies in a complex small disk denoted D . We write $A(\lambda) := (a_1(\lambda), a_2(\lambda))$ and $B(\lambda) := (b_1(\lambda), b_2(\lambda))$. So, equation (4.1.4) can be re-stated (on D) as follows:

$$(4.1.5) \quad [n](P_\lambda) = Q_\lambda \text{ if and only if } n \cdot A(\lambda) - B(\lambda) \in \mathbb{Z} \times \mathbb{Z}.$$

Now, viewing D as an open subset of \mathbb{R}^2 , we can compute the Jacobian matrix of the function $A = (a_1, a_2) : D \rightarrow \mathbb{R}^2$. In both cases (4.1.1) and (4.1.2) above, the Jacobian matrix of A has rank 2 generically; when \mathcal{E} is non-isotrivial, this is proven in [Zan12, Chapter 3], while if $\mathcal{E} = E_0 \times_{\text{Spec}(\mathbb{Q})} C$, this 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 , we have that

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

is real analytic on D and also its Jacobian matrix has rank 2. Arguing identically as in [CZ23, Theorem A2], one obtains that 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 equation (4.1.5) yields that $[n](P_\lambda) = Q_\lambda$ 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. \square

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. So, one views E as the generic fiber of an elliptic arithmetic surface $\pi : \mathcal{E} \rightarrow \text{Spec}(\mathcal{O}_K)$ (where \mathcal{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 \mathcal{O}_K (of good reduction), we denote by $R_v := \sigma_R(v)$ the corresponding specialization of R at the place v . Then it was proven (see [Ing13, IS09]) that for all sufficiently large positive integers n , there exists a (nonarchimedean) place v_n of K (such that the fiber $\pi^{-1}(v_n) =: E_{v_n}$ is smooth) with the property that on E_{v_n} we have:

$$(4.1.6) \quad [n](P_{v_n}) = 0 \text{ and moreover, } [m](P_{v_n}) \neq 0 \text{ when } 0 < m < n.$$

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 \mathcal{O}_K for which there exists *some* positive integer n such that $[n](P_v) = 0$.

Verzobio [Ver21] 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 (i.e., $\Phi(P) = \Psi(Q)$ for some nontrivial endomorphisms $\Phi, \Psi \in \text{End}(E)$), Verzobio [Ver21]

proved that again for all sufficiently large positive integers n , there exists a prime v_n of \mathcal{O}_K such that

$$(4.1.7) \quad [n](P_{v_n}) = Q_{v_n} \text{ and moreover, } [m](P_{v_n}) \neq Q_{v_n} \text{ when } 0 < m < n.$$

Furthermore, Matteo Verzobio confirmed to us that his method extends almost verbatim to cover the function field case (i.e., 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 [Ver21] to the function field case are contained in the papers [Nas16, Slo22].

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 fiber E_λ is an elliptic curve), we have $[k](P_{1,\lambda}) = Q_\lambda$. On the other hand, 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, we do *not* have that both sections σ_{P_2} and σ_Q are constant since otherwise, we would get that also 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. \square

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

Proof. So, we know 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, we obtain that the hypotheses from Lemma 4.2 are met by the triple $(\mathcal{E}, [k_1](P_1), Q)$. Indeed, if $\mathcal{E} = E_0 \times_{\text{Spec}(\overline{\mathbb{Q}})} C$ (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

$$(4.2.1) \quad [nk_1](P_{1,\lambda}) = Q_\lambda.$$

Equation (4.2.1) yields that also $[nk_2](P_{2,\lambda}) = Q_\lambda$, thus providing the desired conclusion in Proposition 4.1. \square

So, in order to complete the proof of Proposition 4.1, it suffices to prove the conclusion (4.0.1) using the hypothesis (C).

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 equation (2.0.1) 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*

$$(4.3.1) \quad [\alpha_1](P_1) = [\alpha_2](P_2) = [\beta](Q) \quad (\text{in } E).$$

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 , then its j -invariant must be contained in $\overline{\mathbb{Q}}$ (see [Sil94, Chapter 2]), i.e., \mathcal{E} is isotrivial. So, the hypothesis from Proposition 4.1 yields that at least one of the sections $\sigma_{P_1}, \sigma_{P_2}, \sigma_Q$ is not constant. However, due to relation (4.3.1), we get that *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 equation (2.0.2)). Let $\ell \in \{1, \dots, M\}$ satisfying the conclusion of Lemma 2.3, i.e., for each (odd) integer a satisfying $a \equiv 2\ell - 1 \pmod{2M}$, we have that

$$(4.3.2) \quad \gcd(N(a + 4\theta), 2M) = 1.$$

Lemma 4.7. *There exist infinitely many $\lambda \in C(\overline{\mathbb{Q}})$ with the property that there exist 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

$$(4.3.3) \quad [n_\lambda]([2M](Q_\lambda)) = [1 - 2\ell - 4\theta](Q_\lambda).$$

The desired conclusion from 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). \square

Now, let 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 2.2, part (i) yields that for any $\gamma \in \mathcal{O}$, we have a natural induced group homomorphism $\widetilde{[\gamma]} : U_\lambda \rightarrow U_\lambda$ given by $Q \mapsto [\gamma](Q)$. Furthermore, part (ii) of Corollary 2.2 yields that $\widetilde{[\beta]}$, $\widetilde{[\alpha_1]}$ and $\widetilde{[\alpha_2]}$ are group automorphisms of U_λ .

Lemma 4.8. *With the above notation, we have that*

$$(4.3.4) \quad [N(\alpha_1)](P_{1,\lambda}), [N(\alpha_2)](P_{2,\lambda}) \in U_\lambda.$$

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

Proof of Lemma 4.8. Let $i \in \{1, 2\}$. Equation (4.3.1) yields that $[\alpha_i](P_{i,\lambda}) \in U_\lambda$ and therefore, also $[\widetilde{\alpha_i} \cdot \alpha_i](P_{i,\lambda}) \in U_\lambda$; thus, we obtain the conclusion from equation (4.3.4). Furthermore, we have the more precise relation coming from equation (4.3.1):

$$(4.3.5) \quad [N(\alpha_i)](P_{i,\lambda}) = [\widetilde{\alpha_i} \cdot \beta](Q_\lambda).$$

Because the induced maps $\widetilde{[\alpha_i]}$ and $\widetilde{[\beta]}$ are group automorphisms of U_λ , then we obtain 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. \square

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

$$(4.3.6) \quad [k_{1,\lambda}N(\alpha_1)](P_{1,\lambda}) = [k_{2,\lambda}N(\alpha_2)](P_{2,\lambda}) = Q_\lambda.$$

Equation (4.3.6) 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. \square

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

REFERENCES

- [AR04] N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$* , Acta Arith. **113** (2004), no. 1, 31–38.
- [ACZ20] Y. André, P. Corvaja, and U. Zannier, *The Betti map associated to a section of an abelian scheme*, Invent. Math. **222** (2020), no. 1, 161–202.
- [AG] S. Asgarli and D. Ghioca, *Collision of orbits for families of polynomials defined over fields of positive characteristic*, submitted for publication, 36 pages.
- [BD11] M. H. Baker and L. DeMarco, *Preperiodic points and unlikely intersections*, Duke Math. J. **159** (2011), no. 1, 1–29.
- [BD13] M. H. Baker and L. DeMarco, *Special curves and postcritically finite polynomials*, Forum Math. Pi **1** (2013), e3, 35 pp. 28 (2022), 1623–1636.
- [BIJMST19] R. L. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman, T. J. Tucker, *Current trends and open problems in arithmetic dynamics*, Bull. Amer. Math. Soc. (N.S.) **56** (2019), no. 4, 611–685.
- [BCZ03] 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.
- [CDMZ22] 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.
- [CMZ18] P. Corvaja, D. Masser, and U. Zannier, *Torsion hypersurfaces on abelian schemes and Betti coordinates*, Math. Ann. **371** (2018), no. 3–4, 1013–1045.
- [CZ13] 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** (2013), no. 5, 1927–1942.
- [CZ23] 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** (2023), no. 5, 1268–1337.
- [DM20] L. DeMarco and N. M. Mavraki, *Variation of canonical height and equidistribution*, Amer. J. Math. **142** (2020), no. 2, 443–473.
- [FG02] C. Favre and T. Gauthier, *The arithmetic of polynomial dynamical pairs*. Annals of Mathematics Studies, **214**. Princeton University Press, Princeton, NJ, 2022. xvii+232 pp.
- [Ghi24] D. Ghioca, *Collision of orbits for a one-parameter family of Drinfeld modules*, J. Number Theory **257** (2024), 320–340.
- [Ghi26] D. Ghioca, *Simultaneously preperiodic points for a family of polynomials in positive characteristic*, Canad. J. Math. **78** (2026), no. 1, 199–221.
- [GHT13] D. Ghioca, L.-C. Hsia, and T. J. Tucker, *Preperiodic points for families of polynomials*, Algebra Number Theory **7** (2013), no. 3, 701–732.
- [GHT17] 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.
- [GHT18] D. Ghioca, L.-C. Hsia, and T. J. Tucker, *A variant of a theorem by Ailon-Rudnick for elliptic curves*, Pacific J. Math. **295** (2018), no. 1, 1–15.
- [HT17] L.-C. Hsia and T. J. Tucker, *Greatest common divisors of iterates of polynomials*, Algebra Number Theory **11** (2017), no. 6, 1437–1459.
- [Ing13] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), no. 2, 473–486.
- [IS09] P. Ingram and J. H. Silverman, *Primitive divisors in arithmetic dynamics*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 2, 289–302.
- [Luc05] F. Luca, *On the greatest common divisor of $u - 1$ and $v - 1$ with u and v near S -units*, Monatsh. Math. **146** (2005), no. 3, 239–256.
- [MZ10] D. W. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), no. 6, 1677–1691.
- [MZ12] D. W. Masser and U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Ann. **352** (2012), no. 2, 453–484.

- [Nas16] B. Naskrecki, *Divisibility sequences of polynomials and heights estimates*, New York J. Math. **22** (2016), 989–1020.
- [Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics, **151**. Springer-Verlag, New York, 1994. xiv+525 pp.
- [Sil04] J. H. Silverman, *Common divisors of elliptic divisibility sequences over function fields*, Manuscripta Math. **114** (2004), no. 4, 431–446.
- [Sil07] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition. Graduate Texts in Mathematics, **106**. Springer, Dordrecht, 2009. xx+513 pp.
- [Slo22] R. Slob, *Primitive divisors of sequences associated to elliptic curves over function fields*, New York J. Math. **28** (2022), 230–249.
- [Ver21] M. Verzobio, *Primitive divisors of sequences associated to elliptic curves with complex multiplication*, Res. Number Theory **7** (2021), no. 2, Paper No. 37, 29 pp.
- [Zan12] 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. xiv+160 pp.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2
Email address: `dghioca@math.ubc.ca`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2
Email address: `negin@math.ubc.ca`