Pacific Journal of Mathematics

A VARIANT OF A THEOREM BY AILON–RUDNICK FOR ELLIPTIC CURVES

DRAGOS GHIOCA, LIANG-CHUNG HSIA AND THOMAS J. TUCKER

Volume 295 No. 1 July 2018

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.1

A VARIANT OF A THEOREM BY AILON–RUDNICK FOR ELLIPTIC CURVES

DRAGOS GHIOCA, LIANG-CHUNG HSIA AND THOMAS J. TUCKER

Given a smooth projective curve C defined over $\overline{\mathbb{Q}}$ and given two elliptic surfaces $\mathcal{E}_1 \to C$ and $\mathcal{E}_2 \to C$ along with sections $\sigma_{P_i}, \sigma_{Q_i}$ (corresponding to points P_i, Q_i of the generic fibers) of $\mathcal{E}_i$ (for $i = 1, 2$), we prove that if there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ such that for some integers $m_{1,t}, m_{2,t}$, we have $[m_{i,t}](\sigma_{P_i}(t)) = \sigma_{Q_i}(t)$ on $\mathcal{E}_i$ (for $i = 1, 2$), then at least one of the following conclusions must hold:

i. There exist isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ such that $\varphi(P_1) = \psi(P_2)$.
ii. Q_i is a multiple of P_i for some $i = 1, 2$.

A special case of our result answers a conjecture made by Silverman.

1. Introduction

Ailon and Rudnick [2004] showed that for two multiplicatively independent nonconstant polynomials $a, b \in \mathbb{C}[x]$ there is a nonzero polynomial $h \in \mathbb{C}[x]$, depending on a and b such that $\gcd(a^n - 1, b^n - 1) \mid h$ for all positive integer n. In this paper, we prove a similar result for elliptic curves; instead of working with the multiplicative group $\mathbb{G}_m$, we work with the group law on an elliptic curve defined over a function field. The result of Ailon–Rudnick relies crucially on the Serre–Ihara–Tate theorem (see [Lang 1965]), while our result relies crucially on recent Bogomolov-type results for elliptic surfaces due to DeMarco and Mavraki [2017].

Throughout our article, we work with elliptic surfaces over $\overline{\mathbb{Q}}$; more precisely, given a projective, smooth curve C defined over $\overline{\mathbb{Q}}$, an *elliptic surface* $\mathcal{E}/C$ is given by a morphism $\pi : \mathcal{E} \to C$ over $\overline{\mathbb{Q}}$ where the generic fiber of π is an elliptic curve E defined over $K = \overline{\mathbb{Q}}(C)$, while for all but finitely many $t \in C(\overline{\mathbb{Q}})$, the fiber $\mathcal{E}_t := \pi^{-1}(\{t\})$ is an elliptic curve defined over $\overline{\mathbb{Q}}$. Recall that a section σ of π (i.e., a map $\sigma : C \to \mathcal{E}$ such that $\pi \circ \sigma = \mathrm{id}|_C$) gives rise to a K-rational point of E. Conversely, a point $P \in E(K)$ corresponds to a section of π; if we need to indicate the dependence on P, we will denote it by σ_P. So, for all but finitely many $t \in C(\overline{\mathbb{Q}})$, the intersection of the image of σ_P in $\mathcal{E}$ with the fiber above t

MSC2010: primary 11G50; secondary 11G35, 14G25.
Keywords: heights, elliptic surfaces, unlikely intersections in arithmetic dynamics.

is a point $P_t := \sigma_P(t)$ on the elliptic curve $\mathcal{E}_t := \pi^{-1}(\{t\})$. For any integer k, the multiplication-by-k map $[k]$ on E extends to a morphism on $\mathcal{E}$; if there is no risk of confusion, we still denote the extension by $[k]$.

We prove the following result:

Theorem 1-1. *Let $\pi_i : \mathcal{E}_i \to C$ be elliptic surfaces over a curve C defined over $\overline{\mathbb{Q}}$ with generic fibers E_i, and let $\sigma_{P_i}, \sigma_{Q_i}$ be sections of π_i (for $i = 1, 2$) corresponding to points $P_i, Q_i \in E_i(\overline{\mathbb{Q}}(C))$. If there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ for which there exist some $m_{1,t}, m_{2,t} \in \mathbb{Z}$ such that $[m_{i,t}]\sigma_{P_i}(t) = \sigma_{Q_i}(t)$ for $i = 1, 2$, then at least one of the following properties must hold*:

(i) *There exist isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ such that $\varphi(P_1) = \psi(P_2)$.*

(ii) *For some $i \in \{1, 2\}$, there exists $k_i \in \mathbb{Z}$ such that $[k_i]P_i = Q_i$ on E_i.*

We note here that, in contrast to similar results such as [Ailon and Rudnick 2004], the ambient algebraic group ($\mathcal{E}_1 \times \mathcal{E}_2$ in our case, as opposed to $\mathbb{G}_m$ for Ailon and Rudnick) need not be defined over the field of constants in $k(C)$.

A special case of our result (when both Q_1 and Q_2 are the zero elements) answers in the affirmative [Silverman 2004b, Conjecture 7]; this is carried out in a more general setting (over the complex numbers and also, giving a more precise connection to the original GCD problem of Ailon–Rudnick) in our Proposition 4-3 from Section 4. We also note that the special case of Theorem 1-1 when $Q_1 = Q_2 = 0$ was solved by Masser and Zannier [2014] when both elliptic surfaces are defined over $\mathbb{C}$.

Silverman's question [2004b, Conjecture 7] was motivated by work of Ailon and Rudnick [2004], who showed that the greatest common divisor of $a^n - 1$ and of $b^n - 1$ for multiplicatively independent polynomials $a, b \in \mathbb{C}[T]$ has bounded degree (see also the generalization in [Corvaja and Zannier 2013b] along with the related results from [Corvaja and Zannier 2008; 2011; 2013a]). In turn, the result of Ailon and Rudnick was motivated by the work of Bugeaud–Corvaja–Zannier [Bugeaud et al. 2003] who obtained an upper bound for $\gcd(a^k - 1, b^k - 1)$ (as k varies in $\mathbb{N}$) for given $a, b \in \overline{\mathbb{Q}}$. On the other hand, Silverman [2004a] showed that the degree of $\gcd(a^m - 1, b^n - 1)$ could be quite large when $a, b \in \overline{\mathbb{F}}_p[T]$; see also the authors' previous paper [Ghioca et al. 2017], where (using as technical ingredient [Ghioca 2014] in place of [DeMarco and Mavraki 2017]) we study the $\gcd(a^m - 1, b^n - 1)$ when a and b are polynomials over arbitrary fields of positive characteristic, along with other generalizations on the same theme. Finally, we mention the work of Denis [2011] who studied the same problem of the greatest common divisor in the context of Drinfeld modules.

As hinted in [Silverman 2004b], this *greatest common divisor* (GCD) *problem* may be studied in much higher generality; for example, if one knew the result of [DeMarco and Mavraki 2017] (see Theorem 2-3 below) in the context of abelian varieties, then our method would extend to a similar conclusion for arbitrary abelian

schemes over a base curve. DeMarco–Mavraki's theorem can be interpreted as an extension of Masser–Zannier's theorem (see [Masser and Zannier 2012]) in the same spirit as the Bogomolov conjecture is an extension of the classical Manin–Mumford conjecture. So, even though the extension to arbitrary abelian varieties of the results from [DeMarco and Mavraki 2017] is expected to be quite challenging, we mention that there is some progress in this direction due to Cinkir [2011], Gubler [2007], and Yamaki [2017], who proved various cases of the Bogomolov conjecture for abelian varieties defined over function fields.

Our Theorem 1-1 is related also to [Barroero and Capuano 2016, Theorem 1.1] (see also the extension from [Barroero and Capuano 2017]) where it is shown that given n linearly independent sections P_i on the Legendre elliptic family $y^2 = x(x-1)(x-t)$, there are at most finitely many parameters t such that the points $(P_i)_t$ satisfy two independent linear relations on the corresponding elliptic curve. Therefore, a special case of the result by Barroero and Capuano is that given sections P_1, P_2, Q_1, Q_2 on the Legendre elliptic surface, if these four sections are linearly independent, then there are at most finitely many t such that for some $m_t, n_t \in \mathbb{Z}$ we have $[m_t](P_1)_t = (Q_1)_t$ and $[n_t](P_2)_t = (Q_2)_t$. However, in our Theorem 1-1 we obtain the same conclusion under the weaker hypothesis that Q_i is not a multiple of P_i for $i = 1, 2$ and also that P_1 and P_2 are linearly independent. We also note that the constant case of Barroero and Capuano's theorem is covered by the results of Habegger and Pila [2016].

A special case of our Theorem 1-1 bears a resemblance to the classical Mordell–Lang problem proven by Faltings [1994] (see also [Hrushovski 1996] for the case of semiabelian varieties defined over function fields). Indeed, with the notation as in Theorem 1-1, assume there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ such that for some $m_t \in \mathbb{Z}$ we have

$$[m_t](P_i)_t = (Q_i)_t \quad \text{for } i = 1, 2. \tag{1-2}$$

Also assume there is no $m \in \mathbb{Z}$ such that $[m]P_i = Q_i$ for $i = 1, 2$. Then the conclusion of Theorem 1-1 yields the existence of isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ such that $\varphi(P_1) = \psi(P_2)$. Thus, using that (1-2) holds for infinitely many $t \in C(\overline{\mathbb{Q}})$ we see that

$$\varphi(Q_1) = \psi(Q_2). \tag{1-3}$$

Therefore, if we let $X \subset \mathcal{A} := \mathcal{E}_1 \times \mathcal{E}_2$ be the 1-dimensional subscheme corresponding to the section (Q_1, Q_2), and we let $\Gamma \subset \mathcal{A}$ be the subgroup spanned by $(0, P_2)$ and $(P_1, 0)$, then the existence of infinitely many $\gamma \in \Gamma$ such that for some $t \in C(\overline{\mathbb{Q}})$ we have $\gamma_t \in X$ implies that X is contained in a proper algebraic subgroup of $\mathcal{A}$ (as given by (1-3)). Such a statement can be viewed as a relative version of the classical Mordell–Lang problem; note that if $\mathcal{E}_1$ and $\mathcal{E}_2$ are constant elliptic

surfaces with generic fibers E_i^0 defined over $\overline{\mathbb{Q}}$, while $\Gamma \subset (E_1^0 \times E_2^0)(\overline{\mathbb{Q}})$, then this question is a special case of Faltings's theorem [1994] (formerly known as the Mordell–Lang conjecture). It is natural to ask whether the above relative version of the Mordell–Lang problem holds more generally when $\mathcal{A} \to C$ is an arbitrary semiabelian scheme, $X \subset \mathcal{A}$ is a 1-dimensional scheme and $\Gamma \subset \mathcal{A}$ is an arbitrary finitely generated group. This more general question is also related to the bounded height problems studied in [Amoroso et al. 2017] in the context of pencils of finitely generated subgroups of $\mathbb{G}_m^n$.

In the next section of this paper, we review some preliminary material. Following that, in Section 3, we prove Theorem 1-1. The proof in the case of nonconstant sections is quite similar to the proofs of the main results of [Ailon and Rudnick 2004] and [Hsia and Tucker 2017], while the case of constant sections requires a different argument. In Section 4, we give a positive answer to Silverman's conjecture [2004b, Conjecture 7].

2. Preliminaries

From now on, we fix an elliptic surface $\pi : \mathcal{E} \to C$, where C is a projective, smooth curve defined over $\overline{\mathbb{Q}}$. We denote by E the generic fiber of $\mathcal{E}$; this is an elliptic curve defined over $\overline{\mathbb{Q}}(C)$. For all but finitely many $t \in C(\overline{\mathbb{Q}})$, we have $\mathcal{E}_t := \pi^{-1}(\{t\})$ is an elliptic curve defined over $\overline{\mathbb{Q}}$.

2.1. ***Isotriviality.*** We say that $\mathcal{E}$ is *isotrivial* if the j-invariant of the generic fiber is a constant function (on C); for isotrivial elliptic surfaces $\mathcal{E}$, all smooth fibers of π are isomorphic (to the generic fiber E). If $\mathcal{E}$ is isotrivial, then there exists a finite cover $C' \to C$ such that $\mathcal{E}' := \mathcal{E} \times_C C'$ is a *constant* (*elliptic*) *surface* over C', i.e., there exists an elliptic curve E^0 defined over $\overline{\mathbb{Q}}$ such that $\mathcal{E}' = E^0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C'$. Furthermore, for a constant elliptic surface $E^0 \times_{\mathrm{Spec}(\overline{\mathbb{Q}})} C'$, we say that σ_P is a *constant section* if $P \in E^0(\overline{\mathbb{Q}})$.

2.2. ***Canonical height on an elliptic surface.*** For each $t \in C(\overline{\mathbb{Q}})$ such that $\mathcal{E}_t$ is an elliptic curve, we let $\hat{h}_{\mathcal{E}_t}$ be the Néron–Tate canonical height for the points in $\mathcal{E}_t(\overline{\mathbb{Q}})$ (for more details, see [Silverman 1986]). There are two important properties of the canonical height which we will use:

(i) $\hat{h}_{\mathcal{E}_t}(P_t) = 0$ if and only if P_t is a torsion point of $\mathcal{E}_t$, i.e., there exists a positive integer k such that $[k]P_t = 0$; and

(ii) for each $k \in \mathbb{Z}$ we have $\hat{h}_{\mathcal{E}_t}([k]P_t) = k^2 \cdot \hat{h}_{\mathcal{E}_t}(P_t)$.

Also, we let $\hat{h}_E$ be the Néron–Tate canonical height on the generic fiber E constructed with respect to the Weil height on the function field $\overline{\mathbb{Q}}(C)$; for more details, see [Silverman 1994a]. Property (ii) above holds also on the generic fiber,

i.e., $\hat{h}_E([k]P) = k^2 \cdot \hat{h}_E(P)$. On the other hand, property (i) above holds only if $\mathcal{E}$ is nonisotrivial. Furthermore, if $\mathcal{E} = E \times_C C$ is a constant family (where E is an elliptic curve defined over $\overline{\mathbb{Q}}$), then for any $P \in E(\overline{\mathbb{Q}}(C))$, we have that $\hat{h}_E(P) = 0$ if and only if $P \in E(\overline{\mathbb{Q}})$.

2.3. ***Variation of the canonical height.*** We let h_C be a given Weil height for points in $C(\overline{\mathbb{Q}})$ corresponding to a divisor of degree 1 on C.

Let σ_P be a section of the elliptic surface $\mathcal{E} \to C$ corresponding to a point P on the generic fiber E. Then, for all but finitely many $t \in C(\overline{\mathbb{Q}})$, the intersection of the image of σ_P in $\mathcal{E}$ with the fiber above t is a point P_t, on the elliptic curve $\mathcal{E}_t$. The following important fact will be used in our proof (see [Tate 1983; Silverman 1983]):

$$\lim_{h_C(t)\to\infty} \frac{\hat{h}_{\mathcal{E}_t}(P_t)}{h_C(t)} = \hat{h}_E(P). \tag{2-1}$$

Furthermore, the following more precise result holds, as proven by Silverman [1994b]:

$$\hat{h}_{\mathcal{E}_t}(P_t) = h_{C,\eta(P)}(t) + O_P(1), \tag{2-2}$$

where $\eta(P)$ is a divisor on C of degree equal to $\hat{h}_E(P)$ and $h_{C,\eta(P)}$ is a given Weil height for the points in $C(\overline{\mathbb{Q}})$ corresponding to the divisor $\eta(P)$, while the implicit constant from the term $O_P(1)$ is only dependent on the section σ_P (and implicitly on the divisor $\eta(P)$), but not on $t \in C(\overline{\mathbb{Q}})$.

2.4. ***Points of small height on sections.*** We will use [DeMarco and Mavraki 2017, Theorem 1.4], which extends [DeMarco et al. 2016] (and in turn, uses the extensive analysis from [Silverman 1994b] regarding the variation of the canonical height in an elliptic fibration). We also note that the case of isotrivial elliptic curves from Theorem 2-3 was previously proven by Zhang [1998], as part of Zhang's famous proof of the classical Bogomolov conjecture.

Theorem 2-3 [DeMarco and Mavraki 2017, Theorem 1.4]. *Let $\mathcal{E}_1, \mathcal{E}_2$ be elliptic fibrations over the same $\overline{\mathbb{Q}}$-curve C. Let P_i be a section of $\mathcal{E}_i$ (for $i = 1, 2$) with the property that there exists an infinite sequence $\{t_n\} \subset C(\overline{\mathbb{Q}})$ such that*

$$\lim_{n\to\infty} \hat{h}_{(\mathcal{E}_i)_{t_n}}((P_i)_{t_n}) = 0 \quad \text{for } i = 1, 2.$$

Then there exist group homomorphisms $\phi : \mathcal{E}_1 \to \mathcal{E}_2$ and $\psi : \mathcal{E}_2 \to \mathcal{E}_2$, not both trivial, such that $\phi(P_1) = \psi(P_2)$.

3. Proof of our main result

Propositions 3-1 and 3-9 are key to our proof.

Proposition 3-1. *Let C be a projective, smooth curve defined over $\overline{\mathbb{Q}}$, and let $h_C(\cdot)$ be a Weil height for the algebraic points of C corresponding to a divisor of degree 1. Let P and Q be sections of an elliptic surface $\pi : \mathcal{E} \to C$ with generic fiber E, and assume there exists no $k \in \mathbb{Z}$ such that $[k]P = Q$. In addition, assume $\hat{h}_E(P) > 0$. If there exists an infinite sequence $\{t_i\} \subset C(\overline{\mathbb{Q}})$ such that for each $i \in \mathbb{N}$ there exists some $m_i \in \mathbb{Z}$ such that $[m_i]P_{t_i} = Q_{t_i}$, then $h_C(t_i)$ is uniformly bounded and $\lim_{i\to\infty} \hat{h}_{\mathcal{E}_{t_i}}(P_{t_i}) = 0$.*

We note that the special case of Proposition 3-1 when $\pi : \mathcal{E} \to C$ is a constant elliptic surface follows from [Silverman 1983].

Proof. Since $[m_i]P_{t_i} = Q_{t_i}$, we have

$$m_i^2 \cdot \hat{h}_{\mathcal{E}_{t_i}}(P_{t_i}) = \hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}). \tag{3-2}$$

Since $[k]P \neq Q$ for any $k \in \mathbb{Z}$ and the sequence $\{t_i\}$ is infinite, then

$$\lim_{i\to\infty} |m_i| = \infty. \tag{3-3}$$

We claim first that $h_C(t_i)$ is uniformly bounded. Indeed, assuming (at the expense, perhaps, of replacing $\{t_i\}$ by an infinite subsequence) that $\lim_{i\to\infty} h_C(t_i) = \infty$, (2-1) coupled with (3-2) and (3-3) yields a contradiction. To see this, we divide both sides of (3-2) by $h_C(t_i)$ and then take limits. Because $\hat{h}_E(P) > 0$, (3-3) implies that the left-hand side equals

$$\lim_{i\to\infty} m_i^2 \cdot \frac{\hat{h}_{\mathcal{E}_{t_i}}(P_{t_i})}{h_C(t_i)} = \infty, \tag{3-4}$$

while the right-hand side equals

$$\lim_{i\to\infty} \frac{\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i})}{h_C(t_i)} = \hat{h}_E(Q) < \infty, \tag{3-5}$$

which is a contradiction. So, indeed, $h_C(t_i)$ must be uniformly bounded.

Next we prove that also $\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i})$ is uniformly bounded. Using (2-2) (see [Silverman 1994b]) we know that there exists a divisor $\eta(Q)$ of C of degree equal to $\hat{h}_E(Q)$ such that

$$\hat{h}_{\mathcal{E}_t}(Q_t) = h_{C,\eta(Q)}(t) + O(1), \tag{3-6}$$

where $h_{C,\eta(Q)}$ is a Weil height on $C(\overline{\mathbb{Q}})$ corresponding to the divisor $\eta(Q)$. Since h_C is a Weil height associated to a divisor D on C of degree 1, then for any positive integer $m > \deg(\eta(Q))$, the divisor $D_1 := mD - \eta(Q)$ has positive degree and therefore, is ample. Then [Hindry and Silverman 2000, Proposition B.3.2] implies

that any Weil height h_{C,D_1} associated to the divisor D_1 satisfies $h_{C,D_1}(t) \geq O(1)$ for all $t \in C(\overline{\mathbb{Q}})$. So,

$$mh_C(t) + O(1) \geq h_{C,\eta(Q)}(t) \quad \text{for } t \in C(\overline{\mathbb{Q}}). \tag{3-7}$$

Therefore $h_{C,\eta(Q)}(t_i)$ is uniformly bounded (since $h_C(t_i)$ is uniformly bounded). Then (3-6) provides the desired claim that

$$\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}) \text{ is bounded as } i \to \infty. \tag{3-8}$$

Finally, the fact that $\lim_{i\to\infty} \hat{h}_{\mathcal{E}_i}(P_i) = 0$ follows easily from combining equations (3-2), (3-3), and (3-8). □

Proposition 3-9. *Let P and Q be sections of a constant elliptic fibration $\pi : \mathcal{E} \to C$, and assume there exists no $k \in \mathbb{Z}$ such that $[k]P = Q$. In addition, assume P is a nontorsion, constant section. If there exists an infinite sequence $\{t_i\} \subset C(\overline{\mathbb{Q}})$ such that for each $i \in \mathbb{N}$ there exists some $m_i \in \mathbb{Z}$ such that $[m_i]P_{t_i} = Q_{t_i}$, then $\lim_{i\to\infty} h_C(t_i) = \infty$.*

Proof. Each fiber $\mathcal{E}_{t_i}$ is isomorphic to the generic fiber E^0, and so, because P is a constant section,

$$\hat{h}_{\mathcal{E}_{t_i}}(P_{t_i}) = \hat{h}_{E^0}(P^0), \tag{3-10}$$

where P^0 is the intersection of P with the generic fiber and $\hat{h}_{E^0}(\cdot)$ is the Néron–Tate canonical height of the elliptic curve E^0 defined over $\overline{\mathbb{Q}}$ (i.e., it is not the canonical height on the generic fiber of $\mathcal{E}$ seen as an elliptic curve defined over the function field $\overline{\mathbb{Q}}(C)$).

Furthermore, since P^0 is not a torsion point of E^0, then $\hat{h}_{E^0}(P^0) > 0$. Thus, from the equality $[m_i]P_{t_i} = Q_{t_i}$, along with (3-10) coupled with the fact that $|m_i| \to \infty$ (because $[k]P \neq Q$ for all integers k), we must have

$$\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}) = m_i^2 \hat{h}_{E^0}(P^0) \to \infty. \tag{3-11}$$

Then, using (2-2), we have

$$\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}) = h_{C,\eta(Q)}(t_i) + O(1), \tag{3-12}$$

where $h_{C,\eta(Q)}$ is a Weil height on C corresponding to a certain divisor $\eta(Q)$. So, (3-11) and (3-12) yield $h_{C,\eta(Q)}(t_i) \to \infty$ and thus, $h_C(t_i) \to \infty$ (see [Hindry and Silverman 2000, Proposition B.3.5], along with our similar argument from the proof of Proposition 3-1). □

Now we can prove our main result.

Proof of Theorem 1-1. First we note that if P_i is a torsion section (for some $i \in \{1, 2\}$), then conclusion (ii) holds trivially since then we would obtain that there

exist infinitely many $t \in C(\overline{\mathbb{Q}})$ such that $(Q_i)_t = [k](P_i)_t$ for the same integer k. So, from now on, we assume that both P_1 and P_2 are nontorsion sections on $\mathcal{E}_1, \mathcal{E}_2$, respectively. In particular, this means that if $\hat{h}_{E_i}(P_i) = 0$, then $\mathcal{E}_i$ must be an isotrivial elliptic surface.

We assume there exists an infinite sequence $\{t_i\} \subset C(\overline{\mathbb{Q}})$ such that for each $i \in \mathbb{N}$ there exist $m_{i,1}, m_{i,2} \in \mathbb{Z}$ with the property that $[m_{i,1}](P_1)_{t_i} = (Q_1)_{t_i}$ and also $[m_{i,2}](P_2)_{t_i} = (Q_2)_{t_i}$. In addition, we assume conclusion (ii) does not hold, i.e., there is no $m \in \mathbb{Z}$ such that $[m]P_i = Q_i$ for some $i \in \{1, 2\}$. We split our analysis into two cases.

Case 1. $\hat{h}_{E_i}(P_i) > 0$ for each $i = 1, 2$.

Applying then Proposition 3-1 to the sections P_i and Q_i, we obtain

$$\lim_{i\to\infty} \hat{h}_{(\mathcal{E}_1)_{t_i}}((P_1)_{t_i}) = \lim_{i\to\infty} \hat{h}_{(\mathcal{E}_2)_{t_i}}((P_2)_{t_i}) = 0. \tag{3-13}$$

Equation (3-13) along with Theorem 2-3 implies that conclusion (i) must hold in Theorem 1-1. Note that we obtain in this case that the morphisms $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ from the conclusion of Theorem 2-3 are *both* isogenies since P_1 and P_2 are nontorsion sections.

Case 2. Either $\hat{h}_{E_1}(P_1) = 0$ or $\hat{h}_{E_2}(P_2) = 0$.

Without loss of generality, we assume $\hat{h}_{E_1}(P_1) = 0$. Therefore (since P_1 is not torsion) $\mathcal{E}_1$ is an isotrivial elliptic surface, and furthermore, at the expense of replacing C by a finite cover (and also performing a base extension for $\mathcal{E}_1$ and $\mathcal{E}_2$), we may assume that $\mathcal{E}_1$ is a constant family. Thus, $\mathcal{E}_1 = E_1^0 \times_C C$ for some elliptic curve E_1^0 defined over $\overline{\mathbb{Q}}$. Then also P_1 is a constant (nontorsion) section, because $\hat{h}_{\mathcal{E}_1}(P_1) = 0$. Finally, we let $h_C(\cdot)$ be a Weil height for the algebraic points of C with respect to a divisor of degree 1.

If $\hat{h}_{E_2}(P_2) > 0$, then Proposition 3-1 applied to P_2 and Q_2 implies that $h_C(t_i)$ is uniformly bounded, which contradicts the conclusion of Proposition 3-9 applied to P_1 and Q_1. Therefore, we must have $\hat{h}_{E_2}(P_2) = 0$, and also $\mathcal{E}_2$ is an isotrivial elliptic surface. At the expense of (yet another) base extension, we may assume that also $\mathcal{E}_2 = E_2^0 \times C$ is a constant fibration. Then P_2 is a constant, nontorsion section on $\mathcal{E}_2$. We let P_i^0 be the intersection of P_i (for $i = 1, 2$) with the generic fiber of $\mathcal{E}_i$.

Now, if either Q_1 or Q_2 is also a constant section, then we get a contradiction since we assumed conclusion (ii) does not hold. Indeed, if for some $i = 1, 2$ both P_i and Q_i are constant sections on the constant elliptic surface $\mathcal{E}_i$, then the existence of a point $t \in C(\overline{\mathbb{Q}})$ such that for some $k \in \mathbb{Z}$ we have $[k](P_i)_t = (Q_i)_t$ implies that actually $[k]P_i = Q_i$ on $\mathcal{E}_i$. So, we may assume that Q_1 and Q_2 are both nonconstant sections on $\mathcal{E}_1$, respectively $\mathcal{E}_2$. Then, there is a (neither vertical, nor horizontal) curve $X \subset E_1^0 \times E_2^0$ containing all points $((Q_1)_t, (Q_2)_t)$ for $t \in C(\overline{\mathbb{Q}})$. Furthermore, our hypothesis means that this curve X intersects the subgroup $\Gamma \subset E_1^0 \times E_2^0$ spanned

by the points $(P_1^0, 0)$ and $(0, P_2^0)$ in an infinite set. The classical Mordell–Lang conjecture (proven by Faltings [1994]) implies that X itself is a coset of an algebraic subgroup of $E_1^0 \times E_2^0$. Hence, because X projects dominantly onto each coordinate, there exists a nontrivial isogeny $\tau : E_1^0 \to E_2^0$, and also there exist endomorphisms ϕ_i of E_i^0, not both trivial, such that

$$\tau(\phi_1(Q_1)) = \phi_2(Q_2). \tag{3-14}$$

Then, using (for any i such that $m_{i,1}$ and $m_{i,2}$ are nonzero) that

$$[m_{i,1}]P_1^0 = (Q_1)_{t_i} \quad \text{and} \quad [m_{i,2}]P_2^0 = (Q_2)_{t_i}$$

along with the fact that $\tau\big(\phi_1((Q_1)_{t_i})\big) = \phi_2((Q_2)_{t_i})$, we obtain the conclusion in Theorem 1-1 with $\varphi := \tau \circ [m_{i,1}] \circ \phi_1$ and $\psi := [m_{i,2}] \circ \phi_2$. Finally, note that since P_1 and P_2 are nontorsion, then also φ and ψ are dominant morphisms. Indeed, if φ were trivial, then using that τ is an isogeny and that $m_{i,1} \neq 0$, we would obtain that ϕ_1 must be trivial. But then $\phi_2(Q_2) = 0$ (using (3-14)), which implies that $\phi_2 = 0$ because we assumed that Q_2 is a nontorsion section. So, if φ were trivial (and a completely similar argument works assuming ψ were trivial), we would get that both ϕ_1 and ϕ_2 are trivial, a contradiction.

This concludes the proof of Theorem 1-1. □

4. Common divisors of elliptic sequences

In this section, we apply Theorem 1-1 to prove Silverman's conjecture [2004b, Conjecture 7] concerning common divisors of elliptic sequences; actually, our Proposition 4-3 provides a slightly more general statement than the original conjecture. We first recall the terminology and notation from [Silverman 2004b] that we will use in this section.

Let k be an algebraically closed field of characteristic 0. Let C be a smooth projective curve defined over k and let $K = k(C)$ be the function field of C. For any point $\gamma \in C(k)$, we let $\operatorname{ord}_\gamma(D)$ denote the coefficient of γ in $D \in \operatorname{Div}(C)$. The *greatest common divisor* for any two effective divisors $D_1, D_2 \in \operatorname{Div}(C)$ is defined as

$$\operatorname{GCD}(D_1, D_2) = \sum_{\gamma \in C} \min\{\operatorname{ord}_\gamma(D_1), \operatorname{ord}_\gamma(D_2)\} \cdot (\gamma) \in \operatorname{Div}(C).$$

For an elliptic curve E defined over K, let $\pi : \mathcal{E} \to C$ be an elliptic surface whose generic fiber is E and let $P \in E(K)$. Recall that the section corresponding to P is denoted by $\sigma_P : C \to \mathcal{E}$. We denote the image of σ_P by $\overline{P} := \sigma_P(C) \subset \mathcal{E}$.

Let E_1 and E_2 be elliptic curves defined over K, let $\mathcal{E}_i/C$ be elliptic surfaces with generic fibers E_i, and let $P_i \in E_i(K)$ for $i = 1, 2$. The greatest common divisor

of P_1 and P_2 is given by

$$\mathrm{GCD}(P_1, P_2) = \mathrm{GCD}(\sigma_{P_1}^*(\overline{O}_{\mathcal{E}_1}), \sigma_{P_2}^*(\overline{O}_{\mathcal{E}_2})),$$

where $\overline{O}_{\mathcal{E}_i} := \sigma_{O_i}(C)$ is the zero section on $\mathcal{E}_i$ corresponding to the identity O_i of E_i and $\sigma_{P_i}^*(\overline{O}_{\mathcal{E}_i})$ is the pull-back under $\sigma_i : C \to \mathcal{E}_i$ of $\overline{O}_{\mathcal{E}_i}$ as a divisor of $\mathcal{E}_i$ for $i = 1, 2$. Thus, for any given $Q_i \in E_i(K)$, $\mathrm{GCD}(P_1 - Q_1, P_2 - Q_2)$ is the greatest common divisor of the two points $P_i - Q_i \in E_i$ for $i = 1, 2$. In the following, points P_1 and P_2 are called (K-) *dependent* if there are morphisms $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ not both trivial such that $\varphi(P_1) = \psi(P_2)$; otherwise they are called *independent*. Note that if one of P_1 and P_2 is a torsion point, then they are automatically dependent.

Motivated by the result of [Ailon and Rudnick 2004], Silverman conjectured that an elliptic analogue also exists. For the convenience of the reader, we recall his conjecture.

Conjecture 4-1 Silverman [1994b, Conjecture 7]. *Let $K = k(C)$ be the function field of a smooth projective curve C over an algebraically closed field k of characteristic 0, let E_1/K and E_2/K be elliptic curves, and let $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$ be K-independent points.*

(i) *There is a constant $c = c(K, E_1, E_2, P_1, P_2)$ such that*

$$\deg \mathrm{GCD}([n_1]P_1, [n_2]P_2) \le c \quad \textit{for all } n_1, n_2 \ge 1.$$

(ii) *Further, there is an equality*

$$\mathrm{GCD}([n]P_1, [n]P_2) = \mathrm{GCD}(P_1, P_2) \quad \textit{for infinitely many } n \ge 1.$$

Remark 4-2. Silverman [1994b, Theorem 8] showed that Conjecture 4-1 is true provided that both E_1 and E_2 have constant j-invariant as a consequence of Raynaud's theorem [1983].

As an application of Theorem 1-1, we prove that Conjecture 4-1 holds (even in a slightly stronger form); we strengthen further the conclusion from Conjecture 4-1 when $k = \overline{\mathbb{Q}}$.

Proposition 4-3. *Let k be an algebraically closed field of characteristic 0. Let C be a smooth projective curve defined over k, let $K = k(C)$ and let E_i/K, $i = 1, 2$, be elliptic curves defined over K. Let $P_i, Q_i \in E_i(K)$ for $i = 1, 2$ and furthermore, assume that P_1 and P_2 are K-independent.*

(i) *If $k = \overline{\mathbb{Q}}$, then there exists an effective divisor $D \in \mathrm{Div}(C)$ such that*

$$\mathrm{GCD}([n_1]P_1 - Q_1, [n_2]P_2 - Q_2) \le D$$

for all integers n_i such that $[n_i]P_i \ne Q_i$, $i = 1, 2$.

(ii) *For an arbitrary algebraically closed field k of characteristic* 0, *there exists an effective divisor $D_0 \in \mathrm{Div}(C)$ such that*

$$\mathrm{GCD}([n_1]P_1, [n_2]P_2) \leq D_0$$

for all nonzero integers n_i.

(iii) *The set*

$$\{n \geq 1 : \mathrm{GCD}([n]P_1, [n]P_2) = \mathrm{GCD}(P_1, P_2)\}$$

has positive density in $\mathbb{N}$.

(iv) *For all but finitely many primes q, we have*

$$\mathrm{GCD}([q]P_1, [q]P_2) = \mathrm{GCD}(P_1, P_2).$$

Remark 4-4. The conclusion of Proposition 4-3 (i) for an arbitrary algebraically closed field k of characteristic 0 would follow from our method once the validity of DeMarco–Mavraki's result [DeMarco and Mavraki 2017] (see Theorem 2-3) is extended over function fields. In turn, their result is contingent on establishing the smooth variation of the canonical height in fibers of an elliptic surface defined over a function field (over $\overline{\mathbb{Q}}$).

The proof of Proposition 4-3 relies on Theorem 1-1 and the following lemma which is a variant of [Silverman 2004b, Lemma 4] bounding $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{O}_{\mathcal{E}}))$ for $\gamma \in C$ and all integers $n \neq 0$.

Lemma 4-5. *Let k be an algebraically closed field of characteristic* 0. *Let E be an elliptic curve defined over $k(C)$ and let $\mathcal{E} \to C$ be an elliptic surface whose generic fiber is E. Let $\gamma \in C(k)$ and let $P, Q \in E(k(C))$ be given. There exists a constant $m = m(\gamma, E, P, Q)$ such that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \leq m$ for all integers n such that $[n]P \neq Q$.*

Proof. Observe that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$ if and only if $\sigma_{[n]P}(\gamma) = \sigma_Q(\gamma)$. Moreover, $\sigma_Q(\gamma)$ is a torsion point of $\mathcal{E}_\gamma$ if and only if there are more than one n such that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$.

It suffices to prove the assertion when $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$ for more than one integer n. Thus, we assume that $\sigma_Q(\gamma)$ is a torsion point of $\mathcal{E}_\gamma$. Let ℓ be the order of $\sigma_Q(\gamma)$ and assume that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$ for some integer n such that $[n]P \neq Q$. It follows that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is finite and

$$\sigma_{[\ell n]P}(\gamma) = [\ell]\sigma_{[n]P}(\gamma) = [\ell]\sigma_Q(\gamma) = O_{\mathcal{E}_\gamma}, \tag{4-6}$$

which is the zero element for the elliptic curve $\mathcal{E}_\gamma$.

If Q is the zero element of E, then it follows from [Silverman 2004b, Lemma 4] that the value of $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{O}_{\mathcal{E}}))$ is bounded independently of $n \neq 0$ and we are done in this case.

Assume that $Q \neq O$. Then (4-6) yields the inequality

$$\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \leq \mathrm{ord}_\gamma(\sigma^*_{[\ell n]P}(\overline{O}_{\mathcal{E}})).$$

Note that the right-hand side of the above inequality involves only $\mathrm{ord}_\gamma(\sigma^*_{[m]P}(\overline{O}_{\mathcal{E}}))$, which is bounded independently of the integer m in question as remarked above. Hence, we conclude that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is bounded independently of $n \neq 0$ (and n such that $[n]P \neq Q$). As $Q \neq O$, we also have that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is finite if $n = 0$. Thus we obtain that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is bounded independently of n such that $[n]P \neq Q$, which concludes our proof. □

Proof of Proposition 4-3. We first prove part (i) in Proposition 4-3. So, for each $\gamma \in C(\overline{\mathbb{Q}})$, let $m_{i,\gamma}$ be an upper bound for $\mathrm{ord}_\gamma(\sigma^*_{[n]P_i}(\overline{Q}_i))$ as in Lemma 4-5. Set $m_\gamma = \min\{m_{1,\gamma}, m_{2,\gamma}\}$. Since P_1 and P_2 are independent, by Theorem 1-1 we may take $m_\gamma = 0$ for all but finitely many points $\gamma \in C(\overline{\mathbb{Q}})$; let S be the finite set of points $\gamma \in C(\overline{\mathbb{Q}})$ for which $m_\gamma > 0$. Let

$$D := \sum_{\gamma \in S} m_\gamma(\gamma).$$

Then, D is an effective divisor of C. Now it follows directly from Lemma 4-5 that $\mathrm{GCD}([n_1]P_1 - Q_1, [n_2]P_2 - Q_2) \leq D$ for all n_i such that $[n_i]P \neq Q_i$ for both $i = 1, 2$. Indeed,

$$\begin{aligned}
&\mathrm{GCD}([n_1]P_1 - Q_1, [n_2]P_2 - Q_2) \\
&\qquad = \mathrm{GCD}(\sigma^*_{[n_1]P_1 - Q_1}(\overline{O}_{\mathcal{E}_1}), \sigma^*_{[n_2]P_2 - Q_2}(\overline{O}_{\mathcal{E}_2})) \\
&\qquad = \mathrm{GCD}(\sigma^*_{[n_1]P}(\overline{Q_1}), \sigma^*_{[n_2]P_2}(\overline{Q_2})) \\
&\qquad = \sum_{\gamma \in C(\overline{\mathbb{Q}})} \min\bigl\{\mathrm{ord}_\gamma(\sigma^*_{[n_1]P_1}(\overline{Q_1})), \mathrm{ord}_\gamma(\sigma^*_{[n_2]P_2}(\overline{Q_2}))\bigr\} \\
&\qquad \leq \sum_{\gamma \in C(\overline{\mathbb{Q}})} \min\{m_{1,\gamma}, m_{2,\gamma}\} \cdot (\gamma) \leq \sum_{\gamma \in S} m_\gamma(\gamma).
\end{aligned}$$

For the proof of part (ii) in Proposition 4-3, we let $Q_i = O_i$ be the zero element of E_i for $i = 1, 2$. If $k = \overline{\mathbb{Q}}$, then the result follows immediately from part (i). Now, for the general case, we note that it suffices to prove the existence of at most finitely many $t \in C(k)$ such that both $(P_1)_t$ and $(P_2)_t$ are torsion points on the elliptic fiber $\mathcal{E}_{1,t}$ and $\mathcal{E}_{2,t}$ respectively; indeed, the fact that the multiplicity of each such t appearing in a divisor $\mathrm{GCD}([n_1]P_1, [n_2]P_2)$ is bounded follows exactly as in the proof of part (i), using Lemma 4-5. On the other hand, if there exist infinitely many $t \in C(k)$ such that both $(P_1)_t$ and $(P_2)_t$ are torsion, then (according to [Masser and Zannier 2014, Theorem, p. 117]) P_1 and P_2 are related, which yields a contradiction.

The conclusion of part (iii) in Proposition 4-3 was proven by Silverman [2004b, Theorem 8 (b)] in the case where both E_1, E_2 have constant j-invariants. We generalize his argument as follows. For each of the finitely many $\gamma \in C(k)$ which does not appear in the support of $\mathrm{GCD}(P_1, P_2)$, but for which there exists some positive integer n such that γ is contained in the support of the divisor $\mathrm{GCD}([n]P_1, [n]P_2)$, or equivalently,

$$\text{the divisor } \mathrm{GCD}([n]P_1, [n]P_2) - (\gamma) \text{ is effective,} \tag{4-7}$$

we let n_γ be the smallest such positive integer n for which (4-7) holds. Then, it is easy to see that γ is contained in the support of $\mathrm{GCD}([n]P_1, [n]P_2)$ if and only if $n_\gamma \mid n$. Also, for each of these points γ which are not in the support of $\mathrm{GCD}(P_1, P_2)$, we have $n_\gamma > 1$. This implies that for any positive integer n which is not divisible by any of the finitely many integers n_γ, we have

$$\mathrm{GCD}([n]P_1, [n]P_2) = \mathrm{GCD}(P_1, P_2).$$

The conclusion in part (iv) in Proposition 4-3 follows from the proof of part (iii) since $\mathrm{GCD}([q]P_1, [q]P_2) = \mathrm{GCD}(P_1, P_2)$ for all primes q which do not divide any of the finitely many numbers $n_\gamma > 1$. □

Acknowledgments

We thank Myrto Mavraki and Joe Silverman for several useful conversations. We are grateful to the anonymous referee for numerous comments and suggestions which improved our paper. The research of Ghioca was partially supported by an NSERC Discovery grant. Hsia was supported by MOST grant 104-2115-M-003-004-MY2. Tucker was partially supported by NSF Grant DMS-0101636.

References

[Ailon and Rudnick 2004] 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. MR Zbl

[Amoroso et al. 2017] F. Amoroso, D. Masser, and U. Zannier, "Bounded height in pencils of finitely generated subgroups", *Duke Math. J.* **166**:13 (2017), 2599–2642. MR Zbl

[Barroero and Capuano 2016] F. Barroero and L. Capuano, "Linear relations in families of powers of elliptic curves", *Algebra Number Theory* **10**:1 (2016), 195–214. MR Zbl

[Barroero and Capuano 2017] F. Barroero and L. Capuano, "Unlikely intersections in products of families of elliptic curves and the multiplicative group", *Quart. J. Math.* **68**:4 (2017), 1117–1138.

[Bugeaud et al. 2003] Y. Bugeaud, P. Corvaja, and U. Zannier, "An upper bound for the GCD of $a^n - 1$ and $b^n - 1$", *Math. Z.* **243**:1 (2003), 79–84. MR Zbl

[Cinkir 2011] Z. Cinkir, "Zhang's conjecture and the effective Bogomolov conjecture over function fields", *Invent. Math.* **183**:3 (2011), 517–562. MR Zbl

[Corvaja and Zannier 2008] P. Corvaja and U. Zannier, "Some cases of Vojta's conjecture on integral points over function fields", *J. Algebraic Geom.* **17**:2 (2008), 295–333. Addendum in *Asian J. Math.* **14**:4 (2010), 581–584. MR Zbl

[Corvaja and Zannier 2011] P. Corvaja and U. Zannier, "An *abcd* theorem over function fields and applications", *Bull. Soc. Math. France* **139**:4 (2011), 437–454. MR Zbl

[Corvaja and Zannier 2013a] P. Corvaja and U. Zannier, "Algebraic hyperbolicity of ramified covers of $\mathbb{G}_m^2$ (and integral points on affine subsets of $\mathbb{P}_2$)", *J. Differential Geom.* **93**:3 (2013), 355–377. MR Zbl

[Corvaja and Zannier 2013b] 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.* **15**:5 (2013), 1927–1942. MR Zbl

[DeMarco and Mavraki 2017] L. DeMarco and N. M. Mavraki, "Variation of canonical height and equidistribution", preprint, 2017. arXiv

[DeMarco et al. 2016] L. DeMarco, X. Wang, and H. Ye, "Torsion points and the Lattès family", *Amer. J. Math.* **138**:3 (2016), 697–732. MR Zbl

[Denis 2011] L. Denis, "Facteurs communs et torsion en caractéristique non nulle", *J. Théor. Nombres Bordeaux* **23**:2 (2011), 347–352. MR Zbl

[Faltings 1994] G. Faltings, "The general case of S. Lang's conjecture", pp. 175–182 in *Barsotti Symposium in Algebraic Geometry* (Abano Terme, Italy, 1991), edited by V. Cristante and W. Messing, Perspect. Math. **15**, Academic Press, San Diego, CA, 1994. MR Zbl

[Ghioca 2014] D. Ghioca, "A Bogomolov type statement for function fields", *Bull. Inst. Math. Acad. Sin.* (*N.S.*) **9**:4 (2014), 641–656. MR Zbl

[Ghioca et al. 2017] 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. MR Zbl

[Gubler 2007] W. Gubler, "The Bogomolov conjecture for totally degenerate abelian varieties", *Invent. Math.* **169**:2 (2007), 377–400. MR Zbl

[Habegger and Pila 2016] P. Habegger and J. Pila, "O-minimality and certain atypical intersections", *Ann. Sci. Éc. Norm. Supér.* (4) **49**:4 (2016), 813–858. MR Zbl

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, 2000. MR Zbl

[Hrushovski 1996] E. Hrushovski, "The Mordell–Lang conjecture for function fields", *J. Amer. Math. Soc.* **9**:3 (1996), 667–690. MR Zbl

[Hsia and Tucker 2017] L.-C. Hsia and T. J. Tucker, "Greatest common divisors of iterates of polynomials", *Algebra Number Theory* **11**:6 (2017), 1437–1459. MR Zbl

[Lang 1965] S. Lang, "Division points on curves", *Ann. Mat. Pura Appl.* (4) **70** (1965), 229–234. MR Zbl

[Masser and Zannier 2012] D. Masser and U. Zannier, "Torsion points on families of squares of elliptic curves", *Math. Ann.* **352**:2 (2012), 453–484. MR Zbl

[Masser and Zannier 2014] D. Masser and U. Zannier, "Torsion points on families of products of elliptic curves", *Adv. Math.* **259** (2014), 116–133. MR Zbl

[Raynaud 1983] M. Raynaud, "Courbes sur une variété abélienne et points de torsion", *Invent. Math.* **71**:1 (1983), 207–233. MR Zbl

[Silverman 1983] J. H. Silverman, "Heights and the specialization map for families of abelian varieties", *J. Reine Angew. Math.* **342** (1983), 197–211. MR Zbl

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986. MR Zbl

[Silverman 1994a] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR Zbl

[Silverman 1994b] J. H. Silverman, "Variation of the canonical height on elliptic surfaces, III: Global boundedness properties", *J. Number Theory* **48**:3 (1994), 330–352. MR Zbl

[Silverman 2004a] J. H. Silverman, "Common divisors of $a^n - 1$ and $b^n - 1$ over function fields", *New York J. Math.* **10** (2004), 37–43. MR Zbl

[Silverman 2004b] J. H. Silverman, "Common divisors of elliptic divisibility sequences over function fields", *Manuscripta Math.* **114**:4 (2004), 431–446. MR Zbl

[Tate 1983] J. Tate, "Variation of the canonical height of a point depending on a parameter", *Amer. J. Math.* **105**:1 (1983), 287–294. MR Zbl

[Yamaki 2017] K. Yamaki, "Non-density of small points on divisors on abelian varieties and the Bogomolov conjecture", *J. Amer. Math. Soc.* **30**:4 (2017), 1133–1163. MR Zbl

[Zhang 1998] S.-W. Zhang, "Equidistribution of small points on abelian varieties", *Ann. of Math.* (2) **147**:1 (1998), 159–165. MR Zbl

Received March 8, 2017. Revised November 10, 2017.

DRAGOS GHIOCA
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BRITISH COLUMBIA
VANCOUVER, BC
CANADA

dghioca@math.ubc.ca

LIANG-CHUNG HSIA
DEPARTMENT OF MATHEMATICS
NATIONAL TAIWAN NORMAL UNIVERSITY
TAIPEI
TAIWAN

hsia@math.ntnu.edu.tw

THOMAS J. TUCKER
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ROCHESTER
ROCHESTER, NY
UNITED STATES

ttucker@math.rochester.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2018 is US $475/year for the electronic version, and $640/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 295 No. 1 July 2018