F. Barroero *Res. Number Theory* (2024) 10:17
https://doi.org/10.1007/s40993-023-00494-2

Research in Number Theory

RESEARCH

Greatest common divisor results on semiabelian varieties and a conjecture of Silverman

Fabrizio Barroero, Laura Capuano and Amos Turchet*

*Correspondence:
amos.turchet@uniroma3.it
Dipartimento di Matematica e Fisica, Università degli Studi Roma 3, L.go S. L. Murialdo 1, 00146 Rome, Italy

Abstract

A divisibility sequence is a sequence of integers $\{d_n\}$ such that d_m divides d_n if m divides n. Results of Bugeaud, Corvaja, Zannier, among others, have shown that the gcd of two divisibility sequences corresponding to subgroups of the multiplicative group grows in a controlled way. Silverman conjectured that a similar behaviour should appear in many algebraic groups. We extend results by Ghioca–Hsia–Tucker and Silverman for elliptic curves and prove an analogue of Silverman's conjecture over function fields for abelian and split semiabelian varieties and some generalizations of this result. We employ tools coming from the theory of unlikely intersections as well as properties of the so-called Betti map associated to a section of an abelian scheme.

Keywords: Semiabelian varieties, Function fields, Betti map, Divisibility sequences

Mathematics Subject Classification: 11G10, 14K15, 14G05

1 Introduction

A sequence of positive integers $\{d_n\}$ is called a *divisibility sequence* if, for every m that divides n one has that d_m divides d_n. Well-known examples of divisibility sequences include some linear recurrence sequences such as the Fibonacci sequence and sequences of the form $d_n = a^n - 1$. In [14, Theorem 1] Bugeaud, Corvaja and Zannier proved that, given multiplicatively independent $a, b \in \mathbb{Z}$, for every $\varepsilon > 0$ there exists a constant $c = c(a, b, \varepsilon)$ such that

$$\log \gcd\{a^n - 1, b^n - 1\} \leq \varepsilon n + c \quad \text{for all } n \geq 1. \tag{1.1}$$

Recently Levin has vastly generalized this type of result in [31].

Ailon and Rudnick conjectured, see [3, Conjecture A], that a stronger statement should hold, namely

$$\gcd\{a^n - 1, b^n - 1\} = \gcd\{a - 1, b - 1\} \quad \text{for infinitely many } n \geq 1.$$

This result was in fact proved by the same authors, as a Corollary of [3, Theorem 1], for multiplicatively independent polynomials $a, b \in k[t]$, where k is a field of characteristic zero.

Motivated by the previous results, Silverman generalized the Ailon and Rudnick conjecture, considering a larger class of divisibility sequences. A divisibility sequence of the form $a^n - 1$ corresponds to a rank 1 subgroup of the multiplicative group $\mathbb{G}_m$. In this setting, the primes dividing $\gcd\{a^n - 1, b^n - 1\}$, and their multiplicities, can be encoded as a divisor on $\operatorname{Spec}\mathbb{Z}$. If we let n vary in the positive integers, we obtain a sequence of divisors D_{nP} on $\operatorname{Spec}\mathbb{Z}$ associated to the point $P = (a, b) \in \mathbb{G}_m^2$, where $nP = (a^n, b^n)$, called a *geometric divisibility sequence*. The same construction can be performed in other algebraic groups over $\mathbb{Q}$, e.g. elliptic curves, obtaining sequences of divisors on $\operatorname{Spec}\mathbb{Z}$. Silverman proposed the following conjecture:

Conjecture 1.1 ([46, Conjecture 10]) *Let $\mathcal{G}/\mathbb{Z}$ be a group scheme, let $\sigma_P \in \mathcal{G}(\mathbb{Z})$, and assume that*

(i) *the generic fiber $G = \mathcal{G} \times_{\mathbb{Z}} \mathbb{Q}$ is an irreducible commutative algebraic group of dimension at least 2 with no unipotent part;*
(ii) *the restriction $P \in G(\mathbb{Q})$ of σ_P to the generic fiber has the property that the subgroup $\mathbb{Z} \cdot P$ generated by P is Zariski dense in G.*

Then, the geometric divisibility sequence $(D_{nP})_{n\geq 1}$ corresponding to σ_P satisfies

$$D_{nP} = D_P \qquad \text{for infinitely many } n \geq 1.$$

The conjecture is completely open in full generality. Silverman [46] proved that Vojta's conjecture applied to blow ups of the generic fiber G implies statements analogous to [14, Theorem 1] for divisibility sequences when $G = \mathbb{G}_m^2$, $G = E^2$, and $G = E \times \mathbb{G}_m$, for an elliptic curve E.

Remark 1.2 Corvaja and Zannier obtained results analogous to [14] and [46] in the function field case, such as [20, Corollary 2.3]. In this setting, they prove an analogue of (1.1) with more explicit and uniform bounds, which in particular allows one to recover the theorem of Ailon and Rudnick, and therefore proving some cases of the analogue of Conjecture 1.1 in the function field case. For further details we refer to [50, Section II.3].

In the spirit of Ailon and Rudnick's result [3], it is natural to study the conjecture in the function field case and consider group schemes $\mathcal{G} \to \mathcal{C}$, where $\mathcal{C}$ is a nonsingular irreducible projective curve defined over $\overline{\mathbb{Q}}$. If the generic fiber G of $\mathcal{G}$ is the product of two elliptic curves E_1 and E_2 defined over $\overline{\mathbb{Q}}(\mathcal{C})$, this problem has been studied by Silverman [45] in the isotrivial case and by Ghioca et al. [25] in general. In this setting, given a point $P = (P_1, P_2) \in G(\overline{\mathbb{Q}}(\mathcal{C}))$, the divisor D_{nP} can be defined explicitly as

$$D_{nP} := \sum_{\gamma \in \mathcal{C}} \min\{\operatorname{ord}_\gamma(\sigma^*_{nP_1}(\mathcal{O}_1)), \operatorname{ord}_\gamma(\sigma^*_{nP_2}(\mathcal{O}_2))\}(\gamma). \tag{1.2}$$

The group scheme $\mathcal{G} = \mathcal{E}_1 \times \mathcal{E}_2 \to \mathcal{C}$ is the product of two elliptic surfaces with generic fibers E_1 and E_2, and we denote by σ_{nP_i} the section of $\mathcal{E}_i \to \mathcal{C}$ corresponding to the point nP_i and by $\mathcal{O}_i$, the image of the identity section of $\mathcal{E}_i \to \mathcal{C}$ for $i = 1, 2$. We can view D_{nP} as the "greatest common divisor" of $\sigma^*_{nP_1}(\mathcal{O}_1)$ and $\sigma^*_{nP_2}(\mathcal{O}_2)$, which are divisors in $\operatorname{Div}(\mathcal{C})$; for this reason, we will usually denote the right-hand side of (1.2) as $\gcd\{\sigma^*_{nP_1}(\mathcal{O}_1), \sigma^*_{nP_2}(\mathcal{O}_2)\}$. When the subgroup generated by P is Zariski-dense in $G(\overline{\mathbb{Q}}(\mathcal{C}))$, then it is proven in [25] that the expected conclusion holds, i.e. $D_{nP} = D_P$ for infinitely many n.

The first goal of this paper is to prove the function field case of Conjecture 1.1 for split semiabelian varieties.

Theorem 1.3 *Let $\mathcal{G}$ be a semiabelian scheme over a curve $\mathcal{C}$, defined over the algebraic numbers. Let G be the generic fiber of $\mathcal{G}$ and suppose it is a split semiabelian variety of relative dimension greater than* 1. *Let $P \in G(\overline{\mathbb{Q}}(\mathcal{C}))$ be a point in the generic fiber such that $\mathbb{Z} \cdot P$ is Zariski dense and let $\sigma_P : \mathcal{C} \to \mathcal{G}$ be the corresponding section. Then,*

(i) *there exists a divisor D on $\mathcal{C}$ such that, for every $n \geq 1$, one has $D_{nP} \leq D$;*
(ii) *$D_{nP} = D_P$ for infinitely many $n \geq 1$. Moreover, the set of n for which the equality holds is the complement in $\mathbb{N}$ of a finite union of arithmetic progressions.*

In the case when $\mathcal{G}$ is the product of two schemes of relative dimension 1, the definition of D_{nP} is analogous to (1.2). In general, the image of the identity section is not a divisor in $\mathcal{G}$ and we need to introduce a more general definition, see Definition 2.1. Nonetheless the support of the divisors D_{nP} are the points of $\mathcal{C}$ where the section σ_{nP} intersects the identity section.

In the case of the split semiabelian variety $E \times \mathbb{G}_m$ defined over $\overline{\mathbb{Q}}(\mathcal{C})$, we answer a question of Silverman in [45, Remark 6].

Corollary 1.4 *Let $\mathcal{E} \to \mathcal{C}$ be an elliptic surface defined over $\overline{\mathbb{Q}}$ with generic fiber E, let $Q \in E(\overline{\mathbb{Q}}(\mathcal{C}))$ be a nontorsion point and let $\sigma_Q : \mathcal{C} \to \mathcal{E}$ be the corresponding section. Let $f \in \mathbb{G}_m(\overline{\mathbb{Q}}(\mathcal{C}))$, not a root of unity, and let $\sigma_f : \mathcal{C} \to \mathbb{G}_m \times \mathcal{C}$ the section given by (f, id). Then, the following hold:*

(i) *there exists an effective divisor $D \in \mathrm{Div}(\mathcal{C})$ such that*

$$D_{nP} = \sum_{\gamma \in \mathcal{C}} \min\{\mathrm{ord}_\gamma(\sigma^*_{nQ}(\mathcal{O})), \mathrm{ord}_\gamma\, \sigma^*_{f^n}(\mathbf{1}_{\mathbb{G}_m}))\}(\gamma) \leq D$$

for all positive integers $n \geq 1$, where $\mathcal{O}$ denotes the image of the identity section of $\mathcal{E} \to \mathcal{C}$ and $\mathbf{1}_{\mathbb{G}_m}$ is the image of the identity section of the constant scheme $\mathbb{G}_m \times \mathcal{C} \to \mathcal{C}$;
(ii) *$D_{nP} = D_P$ for infinitely many $n \in \mathbb{N}$, and the set of n for which the equality holds is the complement in $\mathbb{N}$ of a finite union of arithmetic progressions.*

We would like to point out that, also in the function field case, results of gcd-type are closely related to Vojta's conjecture over function fields, see for example [17,20,21,26,47].

Remark 1.5 We note that the conclusion (i) of Theorem 1.3 is stronger than what is predicted by the analogue of Conjecture 1.1. However, this stronger statement does not hold in general for a nonsplit semiabelian variety, due to the presence of the so-called *Ribet sections*. Indeed, a necessary condition for (i) of Theorem 1.3 to hold is that the union over n of the supports of D_{nP} is a finite set. This relies on a relative Manin-Mumford statement (see Theorem 3.2 and Remark 3.4), which has been proved in a series of papers by Masser and Zannier for abelian schemes (see [33–38]). In this setting, the necessary hypothesis that $\mathbb{Z} \cdot P$ is Zariski dense is also sufficient. For general semiabelian schemes this is not the case: Bertrand [10] showed that there exists a section of a nonconstant extension of a CM elliptic curve by $\mathbb{G}_m$, which does not factor through any proper closed subgroup scheme (and therefore the above-mentioned hypothesis holds), but whose image meets

the torsion points of the various fibers of the semiabelian scheme infinitely often (see also [11]).

We can therefore see that, in this setting, the union of the supports of the D_{nP} is infinite and thus Theorem 1.3 does not hold. Note that this does not contradict the function field analogue of Conjecture 1.1 because, even if we cannot control the support of D_{nP} for all n, there might still be infinitely many values of n such that $D_{nP} = D_P$.

We have just mentioned that a fundamental ingredient for the proof of Theorem 1.3 is a Manin-Mumford type statement. Actually, already Ailon and Rudnick's result relies on Manin-Mumford in $\mathbb{G}_m^2$ which was proved by Ihara, Serre and Tate [29]. Its "modular counterpart" is a theorem of André [2], which is nothing but the André-Oort conjecture for $Y(1)^2$. Very recently Campagna and Dill [15], using André's theorem, proved an analogue of Ailon and Rudnick's result (and more) where the polynomials $t^n - 1$ are replaced by Hilbert class polynomials.

The second goal of the paper is to obtain a generalization of part (i) of Theorem 1.3 for sequences associated to two distinct points P and Q in a group scheme as before. This amounts to replacing the identity section in the definition of the divisor D_P with the image of the section σ_Q, thus considering the divisor D_{P-Q} (see Definition 2.1). In other words, we study the locus where the images of σ_P and σ_Q intersect. This was already studied in the case $E_1 \times E_2$ by Ghioca et al. [25, Theorem 1.1]. Here we consider the general case of split semiabelian schemes.

Theorem 1.6 *Let $\mathcal{G}$ be a semiabelian scheme over a curve $\mathcal{C}$, defined over the algebraic numbers. Let G be the generic fiber of $\mathcal{G}$ and suppose it is a split semiabelian variety of dimension greater than 1. Let $P, Q \in G(\overline{\mathbb{Q}}(\mathcal{C}))$ be such that $nP \neq Q$ for all $n \in \mathbb{Z}$ and $\mathbb{Z} \cdot P$ is Zariski dense in G. Then, there exists an effective divisor $D \in \mathrm{Div}(\mathcal{C})$, independent of n, such that $D_{nP,Q} \leq D$.*

Clearly, part (i) of Theorem 1.3 is nothing but Theorem 1.6 with $Q = O$.

Remark 1.7 If $G = \mathbb{G}_m^2$, the previous theorem is related to [40, Theorem 1.3], which in this setting implies that, if f_1, f_2, g_1, g_2 are multiplicatively independent polynomials in $\overline{\mathbb{Q}}[t]$ with no common zeros, then there exists a polynomial $h \in \overline{\mathbb{Q}}[t]$ such that for every $n_1, n_2, m_1, m_2 \geq 0$ one has

$$\gcd\{f_1^{n_1} - g_1^{m_1}, f_2^{n_2} - g_2^{m_2}\} \mid h.$$

Our theorem in this case shows that there exists a polynomial $h \in \overline{\mathbb{Q}}[t]$ such for every $n \in \mathbb{N}$

$$\gcd\{f_1^n - g_1, f_2^n - g_2\} \mid h$$

under the weaker hypothesis that $f^n \neq g$ for every $n \geq 0$.

The proofs of Theorem 1.6 and (i) of Theorem 1.3 consists of two parts: first, one needs to show that the supports of all $D_{nP,Q}$ lie in a finite set (Theorem 3.3) and then that the order at each point of the support is bounded independently of n (Proposition 4.2).

The first goal is achieved by combining several unlikely intersection results and applying an argument already introduced in [6] to deduce the main theorem of [25] from one of the results in [5].

For the second, we first deal with the case $Q = O$ by generalizing an idea of Silverman [45] in Lemma 4.1. We then deal with the general abelian case by linking the order at a point γ of a divisor D_P to the multiplicity of the Betti map relative to P at γ, as done in [19] for the one dimensional case. The linearity of the Betti map allows us to apply Lemma 4.1 and obtain the desired bound independent of n for the multiplicity of $D_{nP,Q}$ at any point of its support. For powers of the multiplicative group we reduce to a result of Ostafe [40] and deduce the general split semiabelian case as a combination of the two bounds.

Remark 1.8 We finally point out that, given a nonisotrivial elliptic surface $\mathcal{E} \to \mathcal{C}$ and a point P in the generic fiber $E(\overline{\mathbb{Q}}(\mathcal{C}))$, the order of the divisor D_{nP} at a point γ is the multiplicity of intersection of the section σ_{nP} and the zero section in γ. This multiplicity has been studied independently by Corvaja, Demeio, Masser and Zannier [19] and by Ulmer and Urzúa [48], who proved that the set of $\gamma \in \mathcal{C}$ such that a multiple of σ_P intersects the zero section in γ with multiplicity ≥ 2 when P is nontorsion is finite, while the set of $\gamma \in \mathcal{C}$ such that a multiple of σ_P intersects the zero section in γ is always infinite. This implies that the intersection between a multiple of σ_P and the zero section is almost always transverse (for analogous results in the case of curves in $\mathbb{G}_m^2$ see [32]). On the other hand, for our purposes, the problem is somehow orthogonal: we need to show that, for *fixed* $\gamma \in \mathcal{C}$, the multiplicity of the intersections of σ_{nP} and $\sigma_{\mathcal{O}}$ in γ does not go to infinity when $n \to \infty$.

2 Setting and Notations

In this section we fix the setting and the notation that will be used in the rest of the paper.

We denote by $\mathcal{C}$ a nonsingular projective curve defined over $\overline{\mathbb{Q}}$. For a given group scheme $\mathcal{G}$ over $\mathcal{C}$ defined over $\overline{\mathbb{Q}}$ we will denote by G its generic fiber, which is an algebraic group defined over $\overline{\mathbb{Q}}(\mathcal{C})$. In this paper we will always assume that G is irreducible and commutative, and we will write the operation additively, unless G is a power of the multiplicative group.

Given a point $P \in G(\overline{\mathbb{Q}}(\mathcal{C}))$, different from the identity of G, we denote by $\sigma_P : \mathcal{C} \to \mathcal{G}$ the corresponding section of the group scheme. Similarly, we will denote by $\mathcal{O}$ the identity section of $\mathcal{G}$, and, by abuse of notation, we will identify $\mathcal{O}$ with its image $\mathcal{O}(\mathcal{C})$.

We are interested in studying the intersection of the image $\sigma_P(\mathcal{C})$ with the image of the identity section $\mathcal{O}$. We will encode the information of this intersection in a divisor of $\mathcal{C}$, that we will denote by D_P. Similarly, if we are given two distinct points P, Q we can study the intersection of $\sigma_P(\mathcal{C})$ and $\sigma_Q(\mathcal{C})$ by means of a divisor $D_{P,Q}$.

Definition 2.1 Let $\mathcal{G}, \mathcal{C}, \mathcal{O}$ and σ_P as above. Then the *divisor* D_P *associated to* P is defined as follows: if $\sigma_P(\mathcal{C}) \cap \mathcal{O} = \emptyset$, then we set $D_P = 0$. On the other hand, if $\sigma_P(\mathcal{C}) \cap \mathcal{O} \neq \emptyset$ (note that the $\sigma_P(\mathcal{C})$ is always distinct from $\mathcal{O}$ since P is distinct from the identity), then the intersection is a proper closed subscheme of $\mathcal{C}$ via the isomorphism $\sigma_P : \mathcal{C} \to \sigma_P(\mathcal{C})$. Since $\mathcal{C}$ is a nonsingular projective curve the subscheme is an effective divisor that we define to be D_P.

Given another point $Q \in G(\overline{\mathbb{Q}}(\mathcal{C}))$, different from P, we define similarly $D_{P,Q}$ as D_{P-Q}, i.e. the divisor associated to the point $P - Q$.

In the case where the group scheme $\mathcal{G}$ is defined over $\mathbb{Z}$, the previous definition was given in [46, Definition 4]. Similar to the arithmetic case of Silverman, we can make the order of the divisor $D_{P,Q}$ at a point of $\mathcal{C}$ explicit.

Remark 2.2 Given P, Q as before, with corresponding sections σ_P, σ_Q, let $P_\gamma = \sigma_P(\gamma)$. The support of $D_{P,Q}$ consists precisely of the $\gamma \in \mathcal{C}(k)$ such that $\sigma_Q(\gamma) = \sigma_P(\gamma) = P_\gamma$. Let $\mathcal{I}_P, \mathcal{I}_Q$ be the ideal sheaves corresponding to σ_P and σ_Q in the completed local ring $\hat{\mathcal{O}}_{\mathcal{G},P_\gamma}$. Then the order of γ in $D_{P,Q}$ is

$$\operatorname{ord}_\gamma D_{P,Q} = \operatorname{length} \frac{\hat{\mathcal{O}}_{\mathcal{G},P_\gamma}}{\langle \mathcal{I}_P, \mathcal{I}_Q \rangle}.$$

In particular the divisor $D_{P,Q}$ encodes information both on the points where the two curves $\sigma_P(\mathcal{C})$ and $\sigma_Q(\mathcal{C})$ intersects, and on the multiplicity of their intersection.

Remark 2.3 When $\mathcal{G}$ has relative dimension 1, Definition 2.1 can be made even more explicit. Indeed in this case the image of the zero section is a divisor on $\mathcal{G}$. In this case the divisor D_P can be defined as the pullback $\sigma_P^*(\mathcal{O})$ (and $D_{P,Q} = \sigma_P^*(\sigma_Q(\mathcal{C}))$). This coincides with Definition 2.1 but has the disadvantage that is does not extend to higher dimension (one possible approach in this direction is to use the language of ideal sheaves).

We will now make the construction of the divisor D_P explicit in a couple of relevant situations, namely when G is an elliptic curve or the multiplicative group.

Example 2.4 Let E be an elliptic curve defined over $\overline{\mathbb{Q}}(\mathcal{C})$, and let $P \in E(\overline{\mathbb{Q}}(\mathcal{C}))$ be a point. We fix an elliptic scheme $\mathcal{E} \to \mathcal{C}$ with zero section $\mathcal{O}$ which is a proper model of E over $\mathcal{C}$, and a positive integer n. Then we can use Remark 2.3 with $\mathcal{G} = \mathcal{E}$ to define the divisor D_{nP} as follows: one considers the section σ_{nP} associated to the point $nP \in E(\overline{\mathbb{Q}}(\mathcal{C}))$. The section σ_{nP} defines a pullback map on divisors $\sigma_{nP}^* : \operatorname{Div}(\mathcal{E}) \to \operatorname{Div} \mathcal{C}$ so that $\sigma_{nP}^*(\mathcal{O})$, i.e. the pullback of the zero section of the elliptic scheme $\mathcal{E} \to \mathcal{C}$, is a divisor on $\mathcal{C}$, which we denote by D_{nP}.

If γ is a point of $\mathcal{C}$ over which $\mathcal{E}$ has good reduction, then γ is in the support of D_{nP} if and only if $\sigma_{nP}(\gamma) = \mathcal{O}(\gamma)$ in the elliptic curve $\mathcal{E}_\gamma$.

Example 2.5 Similarly, if $f \in \mathbb{G}_m(\overline{\mathbb{Q}}(\mathcal{C})) = \overline{\mathbb{Q}}(\mathcal{C})^\times$ is a rational function, we can use Remark 2.3 to define the divisor $D_{f^n} = \sigma_{f^n}^*(\mathbf{1}_{\mathbb{G}_m})$ for every positive integer n. Here σ_{f^n} denotes the section of $\mathcal{G}$ corresponding to the rational function f^n and $\mathbf{1}_{\mathbb{G}_m}$ is the identity section corresponding to the point $1 \in \mathbb{G}_m(\overline{\mathbb{Q}}(\mathcal{C}))$. The construction is completely analogous to the case of Example 2.4.

In this setting, a point $\gamma \in \mathcal{C}(\overline{\mathbb{Q}})$ is in the support of D_{f^n} if and only if $\sigma_{f^n}(\gamma) = 1$ in $\mathbb{G}_m = \mathbb{G}_m \times \{\gamma\}$, i.e. if $f^n(\gamma) = 1$.

We conclude this section by stressing the link between the divisor D_{nP} and the gcd problems mentioned in the introduction.

Example 2.6 Let G be the semiabelian variety $E \times \mathbb{G}_m$, where E is some elliptic curve defined over $\overline{\mathbb{Q}}(\mathcal{C})$. Then, the divisor D_P associated to a point of G can be expressed

as a gcd of the divisors defined in Examples 2.4 and 2.5. Indeed, given a nonzero point $Q \in E(\overline{\mathbb{Q}}(\mathcal{C}))$, a function $f \in \mathbb{G}_m(\overline{\mathbb{Q}}(\mathcal{C})) \setminus \{1\}$, and the point $P = (Q, f) \in G(\overline{\mathbb{Q}}(\mathcal{C}))$, Definition 2.1 yields three divisors D_Q, D_f and D_P in $\mathcal{C}$. Then, it is easy to check that $D_P = \gcd(D_Q, D_f) = \sum_{\gamma \in \mathcal{C}} \min\{\mathrm{ord}_\gamma(\sigma_Q^*(\mathcal{O})), \mathrm{ord}_\gamma\, \sigma_f^*(\mathbf{1}_{\mathbb{G}_m}))(\gamma)$ (cf. [46, Theorem 4] for an analogue over the integers).

3 Unlikely Intersections and finiteness of the support

We start this section by formulating two theorems that are going to be the key ingredient to control the support of the divisors appearing in Theorems 1.3 and 1.6. The first is a consequence of Pink's conjecture (Conjecture 6.1 in [41]) and is obtained as a combination of several results.

Theorem 3.1 *Let $\mathcal{C}$ be a nonsingular projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{G} \to \mathcal{C}$ a group scheme defined over $\overline{\mathbb{Q}}$ and denote by G its generic fiber. Suppose that G is a split semiabelian variety of dimension at least 2. Let $P \in G(\overline{\mathbb{Q}}(\mathcal{C}))$ and σ_P be the corresponding section. If the set*

$$\{\gamma \in \mathcal{C}(\overline{\mathbb{Q}}) : \text{there exists an algebraic subgroup } H \text{ of } G \text{ of codimension } \geq 2 \text{ such that } \sigma_P(\gamma) \in H_\gamma\} \tag{3.1}$$

is infinite, then P lies in a proper algebraic subgroup of G, i.e., $\mathbb{Z} \cdot P$ is not Zariski-dense in G.

Proof For any finite cover $\mathcal{C}' \to \mathcal{C}$, we have a semiabelian scheme $\mathcal{G}' = \mathcal{G} \times_{\mathcal{C}} \mathcal{C}'$ over $\mathcal{C}'$ whose generic fiber is the base-change $G_{\overline{\mathbb{Q}}(\mathcal{C}')}$ of G. The section σ_P extends to $\sigma'_P : \mathcal{C}' \to \mathcal{G}'$. Now, the set (3.1) is infinite if and only if the same set with $\mathcal{C}'$ and σ'_P in place of $\mathcal{C}$ and σ_P is infinite. Therefore, we are allowed to assume that all semiabelian subvarieties and endomorphisms of G are defined over $\overline{\mathbb{Q}}$.

As our statement is invariant under isogenies, we may moreover assume that $G = \prod_{i=1}^{d} A_i^{e_i}$ for nonnegative integers $d, e_1, \ldots, e_d$ where the A_i are pairwise nonisogenous simple abelian varieties or $\mathbb{G}_m$. As we are considering algebraic subgroups of G of codimension ≥ 2, we may restrict ourselves to the cases and corresponding results listed below and obtain our claim.

(1) $G = \mathbb{G}_m^n$: [39] (see also [12,13,16]).
(2) $G = A$ an isoconstant abelian variety: [27] after previous partial results [18,23,42, 44,49].
(3) $G = A$ a nonisoconstant abelian variety: [6] and the earlier [4,5].
(4) G an isoconstant semiabelian variety: [8] (see also [7,9]).
(5) $G = E^n \times \mathbb{G}_m^l$ for a nonisoconstant elliptic curve E: [5]. □

The following theorem is usually considered as a relative version of the Manin-Mumford conjecture. Indeed, if G is isoconstant, then this is implied by the usual Manin-Mumford, proved by Laurent [30], Raynaud [43] and Hindry [28] for $\mathbb{G}_m^n$, abelian varieties and semiabelian varieties respectively. Recently Masser and Zannier have investigated the relative case for abelian varieties in a series of papers [33–38]. All these works imply the following theorem, which is also implied by Theorem 3.1. We state it separately because

in same cases one does not need to use the full strength of the above theorem but a relative Manin-Mumford statement is enough (see Remark 3.4).

Theorem 3.2 *Let $\mathcal{C}$ be a nonsingular projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{G} \to \mathcal{C}$ a group scheme defined over $\overline{\mathbb{Q}}$ and denote by G its generic fiber. Suppose that G be a split semi-abelian variety over $\overline{\mathbb{Q}}(\mathcal{C})$ of dimension at least 2, and let $P \in G(\overline{\mathbb{Q}}(\mathcal{C}))$ and σ_P be the corresponding section. If there are infinitely many $\gamma \in \mathcal{C}(\overline{\mathbb{Q}})$ such that $\sigma_P(\gamma)$ is torsion in G_γ, then P lies in a proper algebraic subgroup of G, in particular $\mathbb{Z} \cdot P$ is not Zariski-dense in G.*

We will now apply Theorems 3.1 and 3.2 to prove that the following result will allow us to control the support of the divisors we are studying.

Theorem 3.3 *Let $\mathcal{C}$ be a nonsingular projective curve defined over $\overline{\mathbb{Q}}$, let $\mathcal{G} \to \mathcal{C}$ a group scheme defined over $\overline{\mathbb{Q}}$ and denote by G its generic fiber. Suppose that G is a split semiabelian variety over $\overline{\mathbb{Q}}(\mathcal{C})$, and let $P, Q \in G(\overline{\mathbb{Q}}(\mathcal{C}))$. If the set*

$$\bigcup_{n \geq 1} \{\gamma \in \mathcal{C}(\overline{\mathbb{Q}}) : \sigma_{nP}(\gamma) = \sigma_Q(\gamma)\} \tag{3.2}$$

is infinite then at least one of the following holds:

(1) *$nP = Q$ for some integer n, or*
(2) *there exists a finite cover $\mathcal{C}' \to \mathcal{C}$ and an isogeny $\alpha : G_{\overline{\mathbb{Q}}(\mathcal{C}')} \to G_1 \times G_2$ such that $\mathbb{Z} \cdot \pi_1(P)$ is Zariski dense in G_1, $\pi_2(P) = \pi_2(Q) = O_{G_2}$ and $\dim(G_1) = 1$, where π_i is the composition of α with the projection on G_i.*

Proof We assume (3.2) is infinite and (1) is false. We want to prove that (2) holds.

For any finite cover $\mathcal{C}' \to \mathcal{C}$ we have a semiabelian scheme $\mathcal{G}' = \mathcal{G} \times_{\mathcal{C}} \mathcal{C}'$ over $\mathcal{C}'$ whose generic fiber is the base-change $G_{\overline{\mathbb{Q}}(\mathcal{C}')}$ of G. The sections σ_{nP} and σ_Q extend to sections $\sigma'_{nP}, \sigma'_Q : \mathcal{C}' \to \mathcal{G}'$. Now, clearly (3.2) is finite if and only if $\bigcup_{n \geq 1} \{\gamma \in \mathcal{C}'(\overline{\mathbb{Q}}) : \sigma'_{nP}(\gamma) = \sigma'_Q(\gamma)\}$ is finite. We may and will replace $\mathcal{C}$ by $\mathcal{C}'$ tacitly and assume that the morphisms of algebraic groups we are considering are defined over $\overline{\mathbb{Q}}(\mathcal{C})$.

By considering the Zariski-closure of $\mathbb{Z} \cdot P$ we may always find an isogeny $\alpha : G \to G_1 \times G_2$ such that $\mathbb{Z} \cdot \pi_1(P)$ is Zariski dense in G_1 and $\pi_2(P) = O_{G_2}$.

Now, possibly extending $\overline{\mathbb{Q}}(\mathcal{C})$ again we have an isogeny $\beta : G_1 \to H_1 \times \cdots \times H_r$ where the H_j are geometrically simple factors (geometrically simple abelian varieties or $\mathbb{G}_m$). As before, we may assume that they are all defined over $\overline{\mathbb{Q}}(\mathcal{C})$.

We may also spread out and obtain semiabelian schemes $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \ldots, \mathcal{H}_r$ over $\mathcal{C}$ whose generic fibers are $G_1, G_2, H_1, \ldots, H_r$ respectively, and morphisms $\mathcal{G} \to \mathcal{G}_1 \times_{\mathcal{C}} \mathcal{G}_2$ and $\mathcal{G}_1 \to \mathcal{H}_1 \times_{\mathcal{C}} \cdots \times_{\mathcal{C}} \mathcal{H}_r$ over $\mathcal{C}$.

We let G_γ be the fiber of $\mathcal{G}$ above $\gamma \in \mathcal{C}$, and we use the same notation for the G_i and the H_j and for the morphisms between them.

Now, since $\pi_2(P) = O_{G_2}$ and (3.2) is infinite, we must have that $\pi_2(Q) = O_{G_2}$. Also, we clearly have that, if $\bigcup_{n \geq 1} \{\gamma \in \mathcal{C}(\overline{\mathbb{Q}}) : (\pi_1)_\gamma(\sigma_{nP}(\gamma)) = (\pi_1)_\gamma(\sigma_Q(\gamma))\}$ is finite, then (3.2) is finite. We may then assume $G = G_1$ and $\mathbb{Z} \cdot P$ is Zariski-dense in G.

Now, we note that we may assume $G = H_1 \times \cdots \times H_r$. Indeed, the isogeny β preserves the 2 conditions above and (3.2) is infinite if and only if $\bigcup_{n \geq 1} \{\gamma \in \mathcal{C}(\overline{\mathbb{Q}}) : (\beta)_\gamma(\sigma_{nP}(\gamma)) = (\beta)_\gamma(\sigma_Q(\gamma))\}$ is infinite.

Since we are not in case (1), there exists a sequence $(\gamma_m)_{m\in\mathbb{N}}$ of distinct points of $\mathcal{C}(\overline{\mathbb{Q}})$ and a sequence of integers $(n_m)_{m\in\mathbb{N}}$ with $|n_m| \to \infty$ such that $\sigma_{n_m P}(\gamma_m) = \sigma_Q(\gamma_m)$.

If we are not in case (2), then we have a factor H of G, that is either

(i) geometrically simple with $\dim(H) \geq 2$, or
(ii) a product of two one dimensional semiabelian varieties.

Let $p : G \to H$ be the projection. If we show that there is an $n \in \mathbb{N}$ with $np(P) = p(Q)$ then we are done. Indeed, we have two relations

$$p_{\gamma_m}(\sigma_{n_m P}(\gamma_m)) = p_{\gamma_m}(\sigma_Q(\gamma_m)) \quad \text{and} \quad p_{\gamma_m}(\sigma_{nP}(\gamma_m)) = p_{\gamma_m}(\sigma_Q(\gamma_m))$$

which, as $|n_m| \to \infty$, are independent for m large enough. This implies that $p_{\gamma_m}(\sigma_P(\gamma_m))$ is torsion for infinitely many γ_m. By Theorem 3.2, this contradicts the fact that $\mathbb{Z} \cdot P$ is Zariski-dense in G.

If we are in case (i), then we can just apply Theorem 8.5 of [6] to get our sought relation. We can then assume that we are in case (ii), hence we can write $H = H_1 \times H_2$ and let $p_j : G \to H_j$ be the projection. We may also assume, arguing as above, that any isogeny between H_1 and H_2 is defined over $\overline{\mathbb{Q}}(\mathcal{C})$, as well as any endomorphism of H_1 and H_2.

Now, to conclude, one could simply imitate the proof of Theorem A-1 of [6] and invoke the right unlikely intersection result. We include the proof anyway for the reader's convenience.

We let $P_j = p_j(P)$ and $Q_j = p_j(Q)$. We will moreover write $P_j(\gamma)$ for $p_j(\sigma_P(\gamma))$, and similarly $Q_j(\gamma) = p_j(\sigma_Q(\gamma))$.

We have

$$n_m P_1(\gamma_m) = Q_1(\gamma_m), \tag{3.3}$$

and

$$n_m P_2(\gamma_m) = Q_2(\gamma_m). \tag{3.4}$$

Suppose first that H_1 and H_2 are not isogenous. Then, by Theorem 3.1, (P_1, Q_1, P_2, Q_2) lies in a proper algebraic subgroup of $H_1^2 \times H_2^2$. We may assume by symmetry that there are $a_1, b_1 \in \mathrm{End}(H_1)$ such that $a_1 P_1 = b_1 Q_1$. Note that $b_1 = 0$ would contradict the fact that $\mathbb{Z} \cdot P$ is Zariski-dense in G. This relation, together with (3.3), implies that $P_1(\gamma_m)$ is torsion for m large enough. Since P_1 cannot be identically torsion, Theorem 3.1 gives us $a_2 P_2 = b_2 Q_2$ for some $a_2, b_2 \in \mathrm{End}(H_2)$ with $b_2 \neq 0$ as before. If we combine this with (3.4) we have that $P_2(\gamma_m)$ is torsion for m large enough. We get a contradiction by applying Theorem 3.2.

We are then left to deal with the case in which H_1 and H_2 are isogenous. This is similar to what we have just done in the nonisogenous case but a bit more involved. We may assume $H_1 = H_2 =: H$.

This time Theorem 3.1 gives $a_1, a_2, b_1, b_2 \in \mathrm{End}(H)$, not all zero such that

$$a_1 P_1 + a_2 P_2 = b_1 Q_1 + b_2 Q_2. \tag{3.5}$$

As before, b_1, b_2 cannot be both zero since otherwise this would contradict the fact that $\mathbb{Z} \cdot P$ is Zariski-dense in G. Therefore, we may assume $b_1 \neq 0$. Then, combining (3.3) and (3.5) we have that $P_1(\gamma_m), P_2(\gamma_m)$ and $Q_2(\gamma_m)$ satisfy nontrivial dependence relations for m large enough. As the coefficient in front of $P_2(\gamma_m)$ is independent of γ_m, this relation is

independent of (3.4). Thus, by Theorem 3.1, we have

$$c_1P_1 + c_2P_2 = d_2Q_2, \tag{3.6}$$

for $c_1, c_2, d_2 \in \mathrm{End}(H)$, not all zero, and we may assume $d_2 \neq 0$ as before. Combining (3.4) and (3.6), we have

$$c_1P_1(\gamma_m) = (d_2n_m - c_2)P_2(\gamma_m). \tag{3.7}$$

This, together with (3.3), gives

$$e_1P_1 + e_2P_2 = f_1Q_1,$$

for some $e_1, e_2, f_1 \in \mathrm{End}(H)$ with $f_1 \neq 0$. Combining this with (3.3) again we obtain

$$(e_1 - f_1n_m)P_1(\gamma_m) = e_2P_2(\gamma_m). \tag{3.8}$$

Now, (3.7) and (3.8) cannot be independent relations because of Theorem 3.1. Therefore,

$$c_1e_2 = (e_1 - f_1n_m)(d_2n_m - c_2)$$

that, since $f_1d_2 \neq 0$, gives a nontrivial quadratic equation for n_m independent of m. This is impossible because $|n_m| \to \infty$. □

Remark 3.4 One can see that, in the case $Q = O$ (or more generally Q is torsion) there is no need to invoke Theorem 3.1 but only Theorem 3.2 in the proof of Theorem 3.3.

4 Bounding the multiplicity

In this section we prove that the order of the divisors D_{nP} and $D_{nP,Q}$ at points of their support is bounded independently of n.

The first case generalizes an argument given by Silverman in the case of elliptic curves.

Lemma 4.1 (cfr. [45, Lemma 4 and Remark 2]) *Let G be a connected algebraic group defined over the function field $\overline{\mathbb{Q}}(\mathcal{C})$ of a nonsingular projective curve $\mathcal{C}$, let $\mathcal{G}$ be a model of G over $\mathcal{C}$ and let $\mathcal{O}$ be the image of the section of $\mathcal{G}$ corresponding to the identity element of G. Let P be a nontorsion point of G and let D_P be the divisor on $\mathcal{C}$ defined according to Definition 2.1. Let γ be a point of $\mathcal{C}$. Then,*

(1) *if* $\mathrm{ord}_\gamma D_P \geq 1$ *then*

$$\mathrm{ord}_\gamma D_{nP} = \mathrm{ord}_\gamma D_P \qquad \text{for all } n \neq 0;$$

(2) *there is an integer $m = m(\mathcal{G}, P, \gamma)$ so that*

$$\mathrm{ord}_\gamma D_{nP} \in \{0, m\} \qquad \text{for all } n \neq 0,$$

in particular $\mathrm{ord}_\gamma D_{nP}$ *is bounded independently of n.*

Proof The proof is analogous to [45, Lemma 4]. If we denote by $\mu_r : \mathcal{G} \to \mathcal{G}$ the multiplication by r map, then the subscheme $\mu_r^*\mathcal{O}$ is the union of $\mathcal{O}$ and the set T_r of nonzero r-torsion sections of $\mathcal{G}$. Since G is a connected algebraic group in characteristic zero, $\mathcal{G}$ is divisible which implies that μ_r is étale in a neighborhood of the identity element $\mathcal{O}_\gamma$ of $\mathcal{G}_\gamma$ hence $\mathcal{O} \cap T_r = \emptyset$. This implies that

$$\mathrm{ord}_\gamma D_{nP} = \mathrm{ord}_\gamma D_P,$$

proving (1).

To prove (2) we can assume that there exist at least two multiples n_1P and n_2P such that $\operatorname{ord}_\gamma D_{n_iP} \geq 1$ for $i = 1, 2$, otherwise there is nothing to prove. Then (1) implies

$$\operatorname{ord}_\gamma D_{n_1P} = \operatorname{ord}_\gamma D_{n_1n_2P} = \operatorname{ord}_\gamma D_{n_2P} =: m.$$

This implies that for every $n \neq 0$ either $\operatorname{ord}_\gamma D_{nP} = 0$ or $\operatorname{ord}_\gamma D_{nP} = \operatorname{ord}_\gamma D_{n_1P} = m$ as wanted. □

The second statement we obtain is the analogous bound for divisors of the form $D_{nP,Q}$. This was obtained in [25] for products of elliptic curves; however, we use a completely different argument to deduce the bound for split semiabelian varieties of the form $A \times \mathbb{G}_m^\ell$.

Proposition 4.2 *Let A be an abelian variety over $\overline{\mathbb{Q}}(\mathcal{C})$ and let $G = A \times \mathbb{G}_m^\ell$ for some $\ell \geq 0$. Let P, Q be two points of G such that $Q \neq nP$ for every $n \geq 1$. For every $n \geq 1$ let $D_{nP,Q}$ be the divisor on $\mathcal{C}$ defined according to Definition 2.1. Then, there exists an integer $m = m(G, P, Q, \gamma)$ such that $\operatorname{ord}_\gamma D_{nP,Q} \leq m$ for every $n \geq 1$.*

In order to prove Proposition 4.2, we first deal with the case of abelian schemes. In this case we can characterize the order of the divisor at a point γ in terms of the Betti map, following [19, Lemma 2.7].

The Betti map has been a central tool in the study of Diophantine problems, and recently its rank has been investigated by several authors, see for example [1,22,24] and references therein. We will begin by recalling basic facts about the Betti map.

Given a point P in a complex abelian variety A of dimension g, its abelian logarithm can be expressed as a linear combination of the periods of A with real coefficients, usually called the *Betti coordinates* of P. In the case of an abelian scheme $\mathcal{A} \to \mathcal{C}$ and a section $\sigma_P : \mathcal{C} \to \mathcal{A}$, these coordinates become a system of multivalued real-analytic functions.

More precisely, since $\mathcal{C}$ is smooth, by a result of Raynaud the abelian scheme $\pi : \mathcal{A} \to \mathcal{C}$ carries a principal polarization and has a level $\ell \geq 3$ structure. By [22, Proposition 2.1], for every $c_0 \in \mathcal{C}^{an}(\mathbb{C})$ there exist a connected open neighborhood Δ of c_0 and a real-analytic map $b_\Delta : \mathcal{A}_\Delta := \pi^{-1}(\Delta) \to (\mathbb{R}/\mathbb{Z})^{2g}$ which is fiberwise a group isomorphism.

Explicitly, if Δ is simply connected, for each $c \in \Delta$ one can define a basis of the period lattice at each fiber, $\rho_1(c), \dots, \rho_{2g}(c)$, as holomorphic functions of c. In the identification $\mathcal{A}_c = \pi^{-1}(c)$ with $\mathbb{C}^g/\Lambda_c$, where Λ_c is the lattice generated by the periods at c, each $x \in \mathcal{A}_c(\mathbb{C})$ is the class of

$$b_1(x)\rho_1(c) + \cdots + b_{2g}(x)\rho_{2g}(c)$$

for some real numbers $b_1(x), \dots, b_{2g}(x)$. Then $b_\Delta(x)$ is in the class of the $2g$-tuple $(b_1(x), \dots, b_{2g}(x))$ modulo $\mathbb{Z}^{2g}$. If $\sigma_P : \mathcal{C} \to \mathcal{A}$ is a section, the composition $\beta_P := b_\Delta \circ \sigma_P|_\Delta$, given in coordinates by

$$\begin{aligned} \beta_P : \Delta &\longrightarrow (\mathbb{R}/\mathbb{Z})^{2g} \\ c &\longmapsto \big(\beta_{1,P}(c), \dots, \beta_{2g,P}(c)\big), \end{aligned}$$

is called the *Betti map associated to* σ_P, with respect to the neighborhood Δ.

We denote by $m_{\beta_P}(\gamma)$ the multiplicity of β_P at the point γ. In the following lemma we show that $m_{\beta_P}(\gamma)$ coincides with $\operatorname{ord}_\gamma D_P$ in an abelian scheme.

Lemma 4.3 *Let $\sigma_P : \mathcal{C} \to \mathcal{A}$ be a nontorsion section of an abelian scheme $\mathcal{A}$ and let $\gamma \in \mathcal{C}$ such that $\sigma_P(\gamma) = \mathcal{O}(\gamma)$ in $\mathcal{A}_\gamma$. Then, the order* $\operatorname{ord}_\gamma D_P$ *equals $m_{\beta_P}(\gamma)$.*

Proof The statement is local, so we can assume that, in a small neighborhood of $\gamma = 0$, the sections σ_P and the zero section $\mathcal{O}$ are locally given respectively by

$$\sigma_P : t \mapsto (f_1(t), \dots, f_g(t), t) \qquad \mathcal{O} : t \mapsto (0, \dots, 0, t),$$

where $f_j(t)$ are complex analytic functions for every $j = 1, \dots, g$. In this setting, the order m of D_P at 0 is given by

$$m := \operatorname{ord}_0 D_P = \min \left\{ i : \frac{d^{(i)} f_j}{dt}(0) \neq 0 \text{ for some } j = 1, \dots, g \right\}.$$

Similarly the multiplicity of the Betti map is given by

$$m_{\beta_P} = m_{\beta_P}(0) = \min \left\{ i : \frac{d^{(i)} \beta_{j,P}}{dx^{(i)}}(0) \neq 0, \text{ for some } j = 1, \dots, g \right\}. \tag{4.1}$$

We note that, in our setting, both minima are strictly positive since $\sigma_P(0) = \mathcal{O}(0) = (0, \dots, 0)$.

Let $\tilde{\sigma}_P$ be an abelian logarithm of σ_P, which locally in a neighborhood U of $\gamma = 0$ is given by

$$\tilde{\sigma}_P(u) = \left(\int_{\mathcal{O}(u) \to \sigma_P(u)} \omega_1, \dots, \int_{\mathcal{O}(u) \to \sigma_P(u)} \omega_g \right), \tag{4.2}$$

where $\omega_1, \dots, \omega_g$ are a basis of $\Omega^1_{\mathcal{A}/\mathcal{C}}$ and we are integrating on some choice of path from $\mathcal{O}(u)$ to $\sigma_P(u)$. In our setting, the sheaf of one forms of $\mathcal{A}$ is locally generated by $dx_1, \dots, dx_g$, where the $x_1, \dots, x_g$ are local parameters. Therefore we can express locally each ω_i as the sum

$$\sum_{j=1}^{g} s_{i,j}(x_1, \dots, x_g) dx_j,$$

where the $s_{i,j}$ are power series in $x_1, \dots, x_g$ and the determinant of the $g \times g$ matrix $S(x_1, \dots, x_g) := (s_{i,j}(x_1, \dots, x_g))$ does not vanish when evaluated in $\underline{0}$. Notice that a path from $\mathcal{O}(u)$ to $\sigma_P(u)$ on $\mathcal{A}_u$ corresponds, via the local parameters, to a path in $\mathbb{C}^g$ from $\underline{0}$ to $\underline{f}(u) := (f_1(u), \dots, f_g(u))$. Then, a similar argument as in [19, Lemma 2.7] allows one to prove that $\|\tilde{\sigma}_P(u)\| \sim \|u\|^m$. Indeed, computing the integrals defining $\tilde{\sigma}_P(u)$ in (4.2) using the power series expansions of the s_{ij}, one has that

$$\|\tilde{\sigma}_P(u)\| = \left\| S(\underline{0}) \cdot \underline{f}(u)^t \right\| + O(\|\underline{f}(u)\|^2),$$

which implies that

$$\|\underline{f}(u)\| \ll \|\tilde{\sigma}_P(u)\| \ll \|\underline{f}(u)\|.$$

Moreover, since the $f_j(t)$ are complex analytic functions and u is in a neighborhood of 0, one has that $\|\underline{f}(u)\| \sim \|u\|^m$, giving $\|\tilde{\sigma}_P(u)\| \sim \|u\|^m$ as wanted.

On the other hand, by the same argument as in the end of [19, Lemma 2.7], and the definition of the Betti map, we have that

$$\|\tilde{\sigma}_P(u)\| \sim \| \left(\beta_{1,P}(u), \dots, \beta_{2g,P}(u) \right) \|.$$

Since the β_i are real analytic we have that

$$\| \left(\beta_{1,P}(u), \dots, \beta_{2g,P}(u)\right) \| \sim \|u\|^{m_{\beta_P}}.$$

Combining the last two estimates with the fact that $\|\tilde{\sigma}_P(u)\| \sim \|u\|^m$, we obtain $m = m_{\beta_P}$, as wanted. □

Using the relation with the Betti map we can give a uniform bound for the order of a divisor of the form $D_{nP,Q}$ at a point γ in its support in the case of abelian schemes.

Lemma 4.4 *Let σ_P, σ_Q be two sections of an abelian scheme $\mathcal{A} \to \mathcal{C}$ defined over $\overline{\mathbb{Q}}$ corresponding to points $P, Q \in A(\overline{\mathbb{Q}}(\mathcal{C}))$, such that $nP \neq Q$ for every $n \in \mathbb{Z}$, and let $\gamma \in \mathcal{C}$. Then, there exists $m = m(\mathcal{A}, P, Q, \gamma)$ such that* $\operatorname{ord}_\gamma D_{nP,Q} \leq m$ *for every $n \geq 1$.*

Proof We can assume $Q \neq O$ since otherwise the conclusion follows by Lemma 4.1. Furthermore, if there is at most one n such that $\operatorname{ord}_\gamma D_{nP,Q} \geq 1$, then there is nothing to prove, so we will assume there exists more than one n satisfying this inequality. This implies that $\sigma_Q(\gamma)$ is a torsion point and therefore there exists a positive integer a such that $\sigma_{aQ}(\gamma) = \sigma_{anP}(\gamma) = \mathcal{O}(\gamma)$. Note that, by Lemmas 4.1 and 4.3, we have that $m_{\beta_{a(nP-Q)}}(\gamma) = m_{\beta_{nP-Q}}(\gamma)$.

From the local definition of the multiplicity of the Betti map in (4.1) and the fact that

$$\beta_{P_1+P_2} = \beta_{P_1} + \beta_{P_2},$$

we get that

$$m_{\beta_{nP-Q}}(\gamma) = m_{\beta_{a(nP-Q)}}(\gamma) \geq \min\{m_{\beta_{anP}}(\gamma), m_{\beta_{aQ}}(\gamma)\}. \tag{4.3}$$

On the other hand, there exists at most one n such that (4.3) is not an equality (namely, when the value of n makes the linear combination of the corresponding derivatives vanish at γ). This implies that there exists a constant $m' = m'(\mathcal{A}, P, Q, \gamma)$ independent of n such that

$$m_{\beta_{nP-Q}}(\gamma) \leq \min\{m_{\beta_{anP}}(\gamma), m_{\beta_{aQ}}(\gamma)\} + m'. \tag{4.4}$$

Now, by Lemma 4.3, we know that the multiplicities of the Betti map equal the orders of the corresponding divisors, thus we obtain from (4.4) that

$$\operatorname{ord}_\gamma D_{nP,Q} \leq \min\{\operatorname{ord}_\gamma D_{anP}, \operatorname{ord}_\gamma D_{aQ}\} + m'.$$

To conclude, we apply Lemma 4.1 to bound $\operatorname{ord}_\gamma D_{anP}$ independently of n and we note that both $\operatorname{ord}_\gamma D_{aQ}$ and m' do not depend on n, thus finishing the proof. □

The same strategy would allow to show that the order of D_{nP-Q} can be characterized in terms of the Betti map also in the multiplicative group. In this case, however, we can obtain directly that the order is bounded independently of the integer n.

Lemma 4.5 *Let P, Q be two points in $\mathbb{G}_m^\ell$ such that Q is nontorsion and $Q \neq nP$ for every $n \geq 1$. Let σ_P, σ_Q be the corresponding sections over $\mathbb{G}_m^\ell \times \mathcal{C}$. Then, there exists an integer $m = m(P, Q, \gamma)$ such that* $\operatorname{ord}_\gamma D_{nP,Q} \leq m$ *for every $n \geq 1$.*

Proof Since the statement is local we can assume, as in Lemma 4.3, that the section σ_{nP-Q} is given locally as

$$\sigma_{nP-Q} : t \mapsto (h_1(t), \dots, h_\ell(t), t),$$

where the h_j are rational functions. Then, the order satisfies

$$\operatorname{ord}_\gamma D_{nP-Q} = \min_i \left\{ \frac{d^{(i)}h_j}{dt}(\gamma) \neq 0 \text{ for some } j = 1\dots,\ell \right\}.$$

In particular, we can bound $\operatorname{ord}_\gamma D_{nP-Q}$ in terms of the minimal order of the derivative of h_j that, for a fixed j, does not vanish at γ. This shows that we can reduce to the case in which $\ell = 1$ so that we are considering the problem for $\mathbb{G}_m$. In this case,

$$h_1(t) = \frac{a^n(t)d(t) - b^n(t)c(t)}{b^n(t)c(t)},$$

where $a(t)$, $b(t)$ and $c(t)$, $d(t)$ are pairs of coprime polynomials with $P = a(t)/b(t)$ and $Q = c(t)/d(t)$ (recall that the operation of the group in this case is multiplication). Therefore, it is enough to bound the multiplicities of the zeros of the numerator of h_1. We claim that we can conclude by applying a result of Ostafe [40, Lemma 2.9]. In order to see this, we notice that, by the coprimality assumption, the multiplicities of the common zeros of $a^n d$ and $b^n c$ are bounded independently of n. Hence we can factor them out and reduce to bound the multiplicities of $a'^n(t)d'(t) - b'^n(t)c'(t)$, where $a'd'$ and $b'c'$ have no common zeros; in particular, they satisfy the hypotheses of [40, Lemma 2.9] as wanted. □

Combining Lemmas 4.4 and 4.5 we can now prove Proposition 4.2.

Proof Given the split semiabelian scheme $\mathcal{G} = \mathcal{A} \times \mathbb{G}_m^\ell \to \mathcal{C}$ we denote by π_1 and π_2 the projections from $\mathcal{G}$ to $\mathcal{A}$ and $\mathbb{G}_m^\ell$ respectively. Given $D_{nP,Q}$, we denote by $D^{\mathcal{A}}_{nP,Q}$ the divisor corresponding to the sections $\pi_1 \circ \sigma_P$ and $\pi_1 \circ \sigma_Q$ in the abelian scheme $\mathcal{A} \to \mathcal{C}$. Similarly, we denote by $D^{\mathbb{G}_m^\ell}_{nP,Q}$ the divisor corresponding to the sections $\pi_2 \circ \sigma_P$ and $\pi_2 \circ \sigma_Q$ in $\mathbb{G}_m^\ell \times \mathcal{C}$.

By the definition of $\operatorname{ord}_\gamma D_{nP,Q}$ and the fact that $\mathcal{G} = \mathcal{A} \times \mathbb{G}_m^\ell$, we see that

$$\operatorname{ord}_\gamma D_{nP,Q} \leq \min\{\operatorname{ord}_\gamma D^{\mathcal{A}}_{nP,Q}, \operatorname{ord}_\gamma D^{\mathbb{G}_m^\ell}_{nP,Q}\}.$$

Then the conclusion follows combining Lemmas 4.4 and 4.5. □

5 Proofs of Theorems 1.3 and 1.6

We begin by proving Theorem 1.6, which also implies part (i) of Theorem 1.3.

First, recall that $\gamma \in \operatorname{supp} D_{nP,Q}$ if and only if $\sigma_{nP}(\gamma) = \sigma_Q(\gamma)$. By Theorem 3.3, we have that

$$\mathcal{S} := \bigcup_{n\geq 1} \operatorname{supp} D_{nP,Q}$$

is a finite set. Moreover, by Proposition 4.2, if $\operatorname{ord}_\gamma D_{nP,Q} \geq 1$, then the order is bounded independently of n. For every $\gamma \in \mathcal{S}$ we put $m_\gamma := \max_{n\geq 1} \operatorname{ord}_\gamma D_{nP,Q}$. Then,

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

is the desired divisor.

Let us now prove part (ii) of Theorem 1.3. Recall that $\operatorname{ord}_\gamma D_P \geq 1$ if and only if $\sigma_P(\gamma) = \mathcal{O}(\gamma)$, and in this case by Lemma 4.1 we have that $\operatorname{ord}_\gamma D_{nP} = \operatorname{ord}_\gamma D_P$ for every $n \neq 0$. It can however happen that $\operatorname{ord}_\gamma D_{nP} \geq 1$ but $\operatorname{ord}_\gamma D_P = 0$; we are going to show that this can happen only for few choices of n.

As before, by Theorem 3.3 we have that $\mathcal{S}' = \cup_{n\geq 1} \operatorname{supp} D_{nP}$ is finite. Consider $\gamma \in \mathcal{S}' \setminus \operatorname{supp} D_P$ and let n_γ be the smallest positive integer n such that $\gamma \in \operatorname{supp} D_{nP}$. Now, $\gamma \in \operatorname{supp} D_{nP}$ if and only if n_γ divides n. Moreover, if γ is not in the support of D_P we have that $n_\gamma > 1$. This implies that for every positive integer n not divisible by any of these finitely many n_γ we have that $D_{nP} = D_P$, concluding the proof.

Remark 5.1 It is worth noticing that the statement (ii) of Theorem 1.3 does not hold in general in the setting of Theorem 1.6, i.e. when σ_Q is not identically torsion. Indeed, it may happen that the two sections σ_P and σ_Q intersect at a point $\gamma \in \mathcal{C}(\overline{\mathbb{Q}})$ and $\sigma_P(\gamma)$ is not torsion in $\mathcal{G}_\gamma$. This implies that $\gamma \in \operatorname{supp} D_{P,Q}$ but $\gamma \notin \operatorname{supp} D_{nP,Q}$ for every $n \geq 2$.

Acknowledgements
We thank Julian Demeio for discussing with us the results of [19]. We thank Pietro Corvaja, Ariyan Javanpeykar, Siddarth Mathur, Joe Silverman and Umberto Zannier for comments and discussions. The three authors are partially supported by the PRIN 2022 project 2022HPSNCR: Semiabelian varieties, Galois representations and related Diophantine problems. A.T. is partially supported by the projects PRIN2017: Advances in Moduli Theory and Birational Classification and PRIN2020: Curves, Ricci flat Varieties and their Interactions. The three authors are members of the INDAM group GNSAGA.

Funding Open access funding provided by Università degli Studi Roma Tre within the CRUI-CARE Agreement.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Received: 27 October 2022 Accepted: 15 November 2023 Published online: 23 January 2024

References

1. André, Y., Corvaja, P., Zannier, U.: The Betti map associated to a section of an abelian scheme. Invent. Math. **222**(1), 161–202 (2020)
2. André, Y.: Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire. J. Reine Angew. Math. **505**, 203–208 (1998)
3. Ailon, N., Rudnick, Z.: Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. Acta Arith. **113**(1), 31–38 (2004)
4. Barroero, F., Capuano, L.: Linear relations in families of powers of elliptic curves. Algebra Number Theory **10**(1), 195–214 (2016)
5. Barroero, F., Capuano, L.: Unlikely intersections in products of families of elliptic curves and the multiplicative group. Q. J. Math. **68**(4), 1117–1138 (2017)
6. Barroero, F., Capuano, L.: Unlikely intersections in families of abelian varieties and the polynomial Pell equation. Proc. Lond. Math. Soc. (3) **120**(2), 192–219 (2020)
7. Barroero, F., Capuano, L., Mérai, L., Ostafe, A., Sha, M.: Multiplicative and linear dependence in finite fields and on elliptic curves modulo primes. IMRN **2022**, 16094–16137 (2022)
8. Barroero, F., Kühne, L., Schmidt, H.: Unlikely intersections of curves with algebraic subgroups in semiabelian varieties. Sel. Math. (N.S.) **29**(2), Paper No. 18, 37 (2023)
9. Barroero, F., Sha, M.: Torsion points with multiplicatively dependent coordinates on elliptic curves. Bull. Lond. Math. Soc. **52**(5), 807–815 (2020)
10. Bertrand, D.: Special points and Poincaré bi-extensions, with an Appendix by Bas Edixhoven (2011). arXiv:1104.5178
11. Bertrand, D., Masser, D., Pillay, A., Zannier, U.: Relative Manin–Mumford for semi-Abelian surfaces. Proc. Edinb. Math. Soc. (2) **59**(4), 837–875 (2016)
12. Bombieri, E., Habegger, P., Masser, D., Zannier, U.: A note on Maurin's theorem. Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. **21**(3), 251–260 (2010)
13. Bombieri, E., Masser, D., Zannier, U.: Intersecting a curve with algebraic subgroups of multiplicative groups. Int. Math. Res. Not. (IMRN) **1999**(20), 1119–1140 (1999)
14. Bugeaud, Y., Corvaja, P., Zannier, U.: An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. Math. Z. **243**(1), 79–84 (2003)
15. Campagna, F., Dill, G.A.: Around the support problem for Hilbert class polynomials. Preprint (2022). arXiv:2204.13461
16. Capuano, L., Masser, D., Pila, J., Zannier, U.: Rational points on Grassmannians and unlikely intersections in tori. Bull. Lond. Math. Soc. **48**, 141–154 (2016)
17. Capuano, L., Turchet, A.: Lang–Vojta conjecture over function fields for surfaces dominating $\mathbb{G}_m^2$. Eur. J. Math. **8**(2), 573–610 (2021)
18. Carrizosa, M.: Petits points et multiplication complexe. Int. Math. Res. Not. IMRN **2009**(16), 3016–3097 (2009)
19. Corvaja, P., Demeio, J., Masser, D., Zannier, U.: On the torsion values for sections of an elliptic scheme. J. Reine Angew. Math. **782**, 1–41 (2022)

20. Corvaja, P., Zannier, U.: Some cases of Vojta's conjecture on integral points over function fields. J. Algebraic Geom. **17**, 195–333 (2008)
21. Corvaja, P., Zannier, U.: Algebraic hyperbolicity of ramified covers of $\mathbb{G}_m^2$ (and integral points on affine subsets of $\mathbb{P}_2$). J. Differ. Geom. **93**(3), 355–377 (2013)
22. Dimitrov, V., Gao, Z., Habegger, P.: Uniformity in Mordell–Lang for curves. Ann. Math. **194**(1), 237–298 (2021)
23. Galateau, A.: Une minoration du minimum essentiel sur les variétés abéliennes. Comment. Math. Helv. **85**(4), 775–812 (2010)
24. Gao, Z.: Generic rank of Betti map and unlikely intersections. Compos. Math. **156**(12), 2469–2509 (2020)
25. Ghioca, D., Hsia, L.-C., Tucker, T.: A variant of a theorem by Ailon–Rudnick for elliptic curves. Pac. J. Math. **295**(1), 1–15 (2018)
26. Guo, J., Nguyen K.D., Sun, C.-L., Wang, J.T.-Y.: Vojta's abc Conjecture for algebraic tori and applications over function fields. Preprint (2023)
27. Habegger, P., Pila, J.: O-minimality and certain atypical intersections. Ann. Sci. Éc. Norm. Supér. (4) **49**(4), 813–858 (2016)
28. Hindry, M.: Autour d'une conjecture de Serge Lang. Invent. Math. **94**(3), 575–603 (1988)
29. Lang, S.: Division points on curves. Ann. Mat. Pura Appl. (4) **70**, 229–234 (1965)
30. Laurent, M.: Équations diophantiennes exponentielles. Invent. Math. **78**(2), 299–327 (1984)
31. Levin, A.: Greatest common divisors and Vojta's conjecture for blowups of algebraic tori. Invent. Math. **215**(2), 493–533 (2019)
32. Marché, J., Maurin, G.: Singular intersections of subgroups and character varieties. Math. Ann. **386**(1–2), 713–734 (2023)
33. Masser, D., Zannier, U.: Torsion anomalous points and families of elliptic curves. C. R. Math. Acad. Sci. Paris **346**(9–10), 491–494 (2008)
34. Masser, D., Zannier, U.: Torsion anomalous points and families of elliptic curves. Am. J. Math. **132**(6), 1677–1691 (2010)
35. Masser, D., Zannier, U.: Torsion points on families of squares of elliptic curves. Math. Ann. **352**(2), 453–484 (2012)
36. Masser, D., Zannier, U.: Torsion points on families of products of elliptic curves. Adv. Math. **259**, 116–133 (2014)
37. Masser, D., Zannier, U.: Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings. J. Eur. Math. Soc. (JEMS) **17**(9), 2379–2416 (2015). With an appendix by E. V. Flynn
38. Masser, D., Zannier, U.: Torsion points, Pell's equation, and integration in elementary terms. Acta Math. **225**(2), 227–313 (2020)
39. Maurin, G.: Courbes algébriques et équations multiplicatives. Math. Ann. **341**(4), 789–824 (2008)
40. Ostafe, A.: On some extensions of the Ailon–Rudnick theorem. Monatsh. Math. **181**(2), 451–471 (2016)
41. Pink, R.: A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang. Preprint (2005). https://people.math.ethz.ch/~pink/ftp/AOMMML.pdf
42. Ratazzi, N.: Intersection de courbes et de sous-groupes et problèmes de minoration de dernière hauteur dans les variétés abéliennes C.M. Ann. Inst. Fourier (Grenoble) **58**(5), 1575–1633 (2008)
43. Raynaud, M.: Courbes sur une variété abélienne et points de torsion. Invent. Math. **71**(1), 207–233 (1983)
44. Rémond, G., Viada, E.: Problème de Mordell–Lang modulo certaines sous-variétés abéliennes. IMRN **2003**(35), 1915–1931 (2003)
45. Silverman, J.H.: Common divisors of elliptic divisibility sequences over function fields. Manuscr. Math. **114**(4), 431–446 (2004)
46. Silverman, J.H.: Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. Monatsh. Math. **145**, 333–350 (2005)
47. Turchet, A.: Fibered threefolds and Lang–Vojta's conjecture over function fields. Trans. Am. Math. Soc. **369**(12), 8537–8558 (2017)
48. Ulmer, D., Urzúa, G.: Bounding tangencies of sections on elliptic surfaces. IMRN **2021**(6), 4768–4802 (2021)
49. Viada, E.: The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve. Algebra Number Theory **2**(3), 249–298 (2008)
50. Zannier, U.: Some problems of unlikely intersections in arithmetic and geometry. In: Annals of Mathematics Studies, vol. 181. Princeton University Press, Princeton (2012). With appendixes by D. Masser

Publisher's Note