LINEAR RELATIONS IN FAMILIES OF POWERS OF ELLIPTIC CURVES

FABRIZIO BARROERO AND LAURA CAPUANO

Abstract. Motivated by recent work of Masser and Zannier on simultaneous torsion on the Legendre elliptic curve E_λ of equation $Y^2 = X(X-1)(X-\lambda)$, we prove that, given n linearly independent points $P_1(\lambda), \ldots, P_n(\lambda)$ on E_λ with coordinates in $\overline{\mathbb{Q}(\lambda)}$, there are at most finitely many complex numbers λ_0 such that the points $P_1(\lambda_0), \ldots, P_n(\lambda_0)$ satisfy two independent relations on E_{λ_0}. This is a special case of conjectures about Unlikely Intersections on families of abelian varieties.

1. Introduction

Let n be an integer with $n \geq 2$ and let E_λ denote the elliptic curve in the Legendre form defined by

$$(1.1) \qquad Y^2 = X(X-1)(X-\lambda).$$

In [MZ10] (see also [MZ08]), Masser and Zannier showed that there are at most finitely many complex numbers $\lambda_0 \neq 0, 1$ such that the two points

$$\left(2, \sqrt{2(2-\lambda_0)}\right), \quad \left(3, \sqrt{6(3-\lambda_0)}\right),$$

both have finite order on the elliptic curve E_{λ_0}. Stoll [Sto14] recently noted that there is actually no such λ_0. Later, in [MZ12] Masser and Zannier proved that one can replace 2 and 3 with any two distinct complex numbers ($\neq 0, 1$) or even choose distinct X-coordinates ($\neq \lambda$) defined over an algebraic closure of $\mathbb{C}(\lambda)$.

In his book [Zan12], Zannier asks if there are finitely many $\lambda_0 \in \mathbb{C}$ such that two independent relations between the points $\left(2, \sqrt{2(2-\lambda_0)}\right)$, $\left(3, \sqrt{6(3-\lambda_0)}\right)$ and $\left(5, \sqrt{20(5-\lambda_0)}\right)$ hold on E_{λ_0}.

In this article we prove that this question has a positive answer, as Zannier expected in view of very general conjectures. We actually prove a more general result, analogous to the one in [MZ12] but, at the moment, we are only able to replace 2, 3 and 5 with any three pairwise distinct algebraic numbers, or choose X-coordinates defined over an algebraic closure of $\mathbb{Q}(\lambda)$, with the obvious exceptions 0, 1 and λ because the corresponding points are identically 2-torsion. Moreover, our method allows us to deal with arbitrarily many points since we consider a curve $\mathcal{C} \subseteq \mathbb{A}^{2n+1}$ with coordinate functions $(x_1, y_1, \ldots, x_n, y_n, \lambda)$, λ non-constant, such that for every $j = 1, \ldots, n$, the points $P_j = (x_j, y_j)$ lie on the elliptic curve E_λ. As the point $\boldsymbol{c}$ varies on the curve $\mathcal{C}$, the specialized points $P_j(\boldsymbol{c}) = (x_j(\boldsymbol{c}), y_j(\boldsymbol{c}))$ will be lying on the specialized elliptic curve $E_{\lambda(\boldsymbol{c})}$. We implicitly exclude the finitely many $\boldsymbol{c}$ with $\lambda(\boldsymbol{c}) = 0$ or 1, since in that case $E_{\lambda(\boldsymbol{c})}$ is not an elliptic curve.

We are now ready to state the main result of the article.

Theorem 1.1. *Let $\mathcal{C} \subseteq \mathbb{A}^{2n+1}$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ with coordinate functions $(x_1, y_1, \ldots, x_n, y_n, \lambda)$, λ non-constant, such that, for every $j = 1, \ldots, n$, the points $P_j = (x_j, y_j)$ lie on E_λ and there are no integers $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero, such that*

$$(1.2) \qquad\qquad a_1 P_1 + \cdots + a_n P_n = O,$$

identically on $\mathcal{C}$. Then there are at most finitely many $\mathbf{c} \in \mathcal{C}$ such that the points $P_1(\mathbf{c}), \ldots, P_n(\mathbf{c})$ satisfy two independent relations on $E_{\lambda(\mathbf{c})}$.

Note that the case $n = 2$ is covered by the main proposition of [MZ12] in the more general setting of a curve defined over $\mathbb{C}$.

Moreover, in [RV03] Rémond and Viada proved an analogue of Theorem 1.1 for a power of a constant elliptic curve with CM, where one must allow the coefficients $a_1, \ldots, a_n$ in (1.2) to lie in the larger endomorphism ring. For the general case of powers of a constant elliptic curve, the result follows from works of Viada [Via08] and Galateau [Gal10]. If $n = 2$ this is nothing but Raynaud's Theorem [Ray83], also known as the Manin-Mumford Conjecture.

We already mentioned the example of the three points with fixed abscissas 2, 3 and 5. It is easy to see that this will follow from Theorem 1.1 once we show that there is no identical relation between the three points on the generic curve E_λ. Indeed, the minimal fields of definition of these three points are disjoint quadratic extensions of $\overline{\mathbb{Q}}(\lambda)$, and by conjugating one can see that the points would be identically torsion on E_λ. This is not possible, as it can be seen in different ways (see [Zan12], p. 68). For instance, applying the Lutz-Nagell Theorem ([Sil09], Corollary 7.2), one can show that the point of abscissa 2 is not torsion on E_6.

One may ask if finiteness holds if we impose only one relation. This is not the case. Indeed, there are infinitely many λ_0 such that a point with fixed algebraic abscissa is torsion (see Notes to Chapter 3 in [Zan12]). On the other hand, the values of λ such that at least one relation holds are "sparse", as follows from work of Masser [Mas89b]. Actually, a well-known theorem of Silverman [Sil83] implies that the absolute Weil height of such values is bounded. A direct effective proof of this can be found in Masser's Appendix C of [Zan12]. In particular, there are at most finitely many λ_0 yielding one relation in a given number field or of bounded degree over $\mathbb{Q}$.

Our proof follows the general strategy introduced by Pila and Zannier in [PZ08] and used by Masser and Zannier in various articles [MZ08], [MZ10] and [MZ12]. In particular, we consider the elliptic logarithms $z_1, \ldots, z_n$ of $P_1, \ldots, P_n$ and the equations

$$z_j = u_j f + v_j g,$$

for $j = 1, \ldots, n$, where f and g are suitably chosen basis elements of the period lattice of E_λ. If we consider the coefficients u_j, v_j as functions of λ and restrict them to a compact set, we obtain a subanalytic surface S in $\mathbb{R}^{2n}$. The points of $\mathcal{C}$ that yield two independent relations on the elliptic curve will correspond to points of S lying on linear varieties defined by equations of some special form and with integer coefficients. In case $n = 2$, one faces the simpler problem of counting rational points with bounded denominator in S. For this, a previous result of Pila [Pil04] suffices together with the fact that the surface is "sufficiently" transcendental. In the general case we adapted ideas of Pila building on previous work of him [Pil11] and used by the second author in her Ph.D. thesis [Cap14] (see also [CMPZ14]), and obtained an upper bound of order T^ϵ for the number of points of S lying on subspaces of the special form mentioned

above and rational coefficients of absolute value at most T, provided S does not contain a semialgebraic curve segment. Under the hypothesis that no identical relation holds on $\mathcal{C}$, using a result of Bertrand [Ber90], we are able to show that there are no such semialgebraic curve segments.

Now, to conclude the proof, we use works of Masser [Mas88], [Mas89a] and David [Dav97] and exploit the boundedness of the height to show that the number of points of S considered above is of order at least T^δ for some $\delta > 0$. Comparing the two estimates leads to an upper bound for T and thus for the coefficients of the two relations, concluding the proof.

With methods similar to ours, in the works [Cap14] and [CMPZ14], mentioned above, the authors prove a toric analogue of Theorem 1.1, giving an alternative proof of a result appeared in [BMZ99] and later generalized by Maurin in [Mau08] (see also [BMZ08]).

In the paper, we will denote by $\gamma_1, \gamma_2, \ldots$ some positive constants. The indexes are reset at the end of each section.

2. The Zilber-Pink Conjectures

In this section we see how our Theorem relates to the so-called Zilber-Pink Conjectures on Unlikely Intersections.

First, let us examine the objects we are investigating from the point of view of dimensions. We consider our elliptic curve E_λ as an elliptic scheme over $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. Our ambient space is then the fiber power of n copies of this elliptic scheme and has dimension $n + 1$. Now, for any choice of linearly independent vectors $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{Z}^n$, imposing the two corresponding conditions yields an $(n - 1)$-fold. Therefore, the intersection of a curve and an $(n - 1)$-fold in a space of dimension $n + 1$ is indeed unlikely to be non-empty and one expects finiteness for varying integer vectors.

Our result fits in the framework of very general conjectures formulated by Zilber [Zil02] and Bombieri, Masser and Zannier [BMZ07] in the toric case and by Pink [Pin05] in a more general setting, also known as the Zilber-Pink Conjectures.

In a series of papers [MZ10], [MZ12], [MZ14a] and [MZ14b] Masser and Zannier proved a variant of Pink's conjecture in the case of a curve in an abelian surface scheme over $\overline{\mathbb{Q}}$, and over $\mathbb{C}$ in the non-simple case. On the other hand, Pink's conjecture concerns families of semiabelian varieties. However, in 2011 Bertrand [Ber11] found a counterexample to this, for a suitable non-split extension of a CM elliptic constant family $E_0 \times B$ (over a curve B) by $\mathbb{G}_m$. This situation is rather "special"; in fact, as it is shown in [BMPZ11], the possible presence of the so called "Ribet Sections" is the only obstruction to the validity of the conjecture in the case of semiabelian surface schemes.

Now, let us see how our Theorem 1.1 implies a statement in the spirit of the conjectures mentioned above. In particular, we translate our result in the language of schemes, borrowing some terminology and results from a work of Habegger [Hab13].

Let S be an irreducible and non-singular quasi-projective curve defined over $\overline{\mathbb{Q}}$ and let $\mathcal{E} \to S$ be an elliptic scheme over S, i.e. a group scheme whose fibers are elliptic curves. Let $n \geq 2$. We define $\mathcal{A}$ to be the n-fold fibered power $\mathcal{E} \times_S \cdots \times_S \mathcal{E}$ with the structural morphism $\pi : \mathcal{A} \to S$.

We suppose that $\mathcal{E}$ is not isotrivial. In other words, $\mathcal{E} \to S$ cannot become a constant family after a finite étale base change.

A subgroup scheme G of $\mathcal{A}$ is a closed subvariety, possibly reducible, which contains the image of the zero section $S \to \mathcal{A}$, is mapped to itself by the inversion morphism and such that the image of $G \times_S G$ under the addition morphism is in G. A subgroup scheme G is called flat if $\pi_{|G} : G \to S$ is flat, i.e., all irreducible components of G dominate the base curve S (see [Har77], Proposition III 9.7).

We can now state the following theorem.

Theorem 2.1. *Let $\mathcal{A}$ be as above and let $\mathcal{A}^{\{2\}}$ be the union of its flat subgroup schemes of codimension at least 2. Let $\mathcal{C}$ be a curve in $\mathcal{A}$ defined over $\overline{\mathbb{Q}}$ and suppose $\pi(\mathcal{C})$ dominates S. Then $\mathcal{C} \cap \mathcal{A}^{\{2\}}$ is contained in a finite union of flat subgroup schemes of positive codimension.*

In order to prove that this theorem is a consequence of Theorem 1.1, we need some notation and facts from [Hab13].

For every $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ we have a morphism $\boldsymbol{a} : \mathcal{A} \to \mathcal{E}$ defined by

$$\boldsymbol{a}(P_1, \ldots, P_n) = a_1 P_1 + \cdots + a_n P_n.$$

We identify the elements of $\mathbb{Z}^n$ with the morphisms they define. The fibered product $\alpha = \boldsymbol{a}_1 \times_S \cdots \times_S \boldsymbol{a}_r$, for $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r \in \mathbb{Z}^n$ defines a morphism $\mathcal{A} \to \mathcal{B}$ over S where $\mathcal{B}$ is the r-fold fibered power of $\mathcal{E}$. The kernel of α, $\ker \alpha$ indicates the fibered product of $\alpha : \mathcal{A} \to \mathcal{B}$ with the zero section $S \to \mathcal{B}$. We consider it as a closed subscheme of $\mathcal{A}$.

Lemma 2.2. *Let G be a codimension r flat subgroup scheme of $\mathcal{A}$ with $1 \leq r \leq n$. Then, there exist independent $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r \in \mathbb{Z}^n$ such that $G \subseteq \ker(\boldsymbol{a}_1 \times_S \cdots \times_S \boldsymbol{a}_r)$. Moreover, $\ker(\boldsymbol{a}_1 \times_S \cdots \times_S \boldsymbol{a}_r)$ is a flat subgroup scheme of $\mathcal{A}$ of codimension r.*

Proof. This follows from Lemma 2.5 of [Hab13] and its proof. $\qquad\square$

Consider now the Legendre family with equation (1.1). As said before, this gives an example of an elliptic scheme, which we call $\mathcal{E}_L$, over the modular curve $Y(2) = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. We write $\mathcal{A}_L$ for the n-fold fibered power of $\mathcal{E}_L$.

Lemma 2.3 ([Hab13], Lemma 5.4). *Let $\mathcal{A}$ be as above. After possibly replacing S by a Zariski open, non-empty subset there exists an irreducible, non-singular quasi-projective curve S' defined over $\overline{\mathbb{Q}}$ such that the following is a commutative diagram*

$$
\begin{array}{ccccc}
\mathcal{A} & \xleftarrow{\ f\ } & \mathcal{A}' & \xrightarrow{\ e\ } & \mathcal{A}_L \\
\pi \downarrow & & \downarrow & & \downarrow \pi_L \\
S & \xleftarrow[\ l\ ]{} & S' & \xrightarrow[\ \lambda\ ]{} & Y(2)
\end{array}
$$

where l is finite, λ is quasi-finite, $\mathcal{A}'$ is the abelian scheme $\mathcal{A} \times_S S'$, f is finite and flat and e is quasi-finite and flat. Moreover, the restriction of f and e to any fiber of $\mathcal{A}' \to S'$ is an isomorphism of abelian varieties.

We will also need the following technical lemma.

Lemma 2.4. *If G is a flat subgroup scheme of $\mathcal{A}$ then $e\left(f^{-1}(G)\right)$ is a flat subgroup scheme of $\mathcal{A}_L$ of the same dimension. Moreover, let X be a subvariety of $\mathcal{A}$ dominating S and not*

contained is a proper flat subgroup scheme of $\mathcal{A}$, X'' an irreducible component of $f^{-1}(X)$ and X' the Zariski closure of $e(X'')$ in $\mathcal{A}_L$. Then X' has the same dimension of X, dominates $Y(2)$ and is not contained in a proper flat subgroup scheme of $\mathcal{A}_L$.

Proof. This follows from the proof of Lemma 5.5 of [Hab13]. □

Proof of Theorem 2.1. First, we can assume that $\mathcal{C}$ is not contained in a flat subgroup scheme of $\mathcal{A}$ of positive codimension. Therefore, it is enough to prove that $\mathcal{C} \cap \bigcup G$ is finite where the union is taken over all flat subgroup schemes of $\mathcal{A}$ of codimension at least 2.

Consider the Zariski closure $\mathcal{C}'$ of $e(\mathcal{C}'')$ for a component $\mathcal{C}''$ of $f^{-1}(\mathcal{C})$. By Lemma 2.4, $\mathcal{C}'$ is a curve in $\mathcal{A}_L$ dominating $Y(2)$ and not contained in a proper flat subgroup scheme.

Now, since e is quasi-finite, if $e\left(f^{-1}\left(\mathcal{C} \cap \mathcal{A}^{\{2\}}\right)\right)$ is finite then $\mathcal{C} \cap \mathcal{A}^{\{2\}}$ is finite and by Lemma 2.4 we have

$$e\left(f^{-1}\left(\mathcal{C} \cap \mathcal{A}^{\{2\}}\right)\right) \subseteq e\left(f^{-1}(\mathcal{C})\right) \cap \mathcal{A}_L^{\{2\}}.$$

Therefore, we can reduce to proving our claim for the Legendre family and for $\mathcal{C}'$.

By Lemma 2.2, each flat subgroup scheme of codimension at least 2 of $\mathcal{A}_L$ is contained in $\ker(\boldsymbol{a}_1 \times_{Y(2)} \boldsymbol{a}_2)$ for some independent $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{Z}^n$. Therefore, it is enough to show that $\mathcal{C}' \cap \bigcup \ker(\boldsymbol{a}_1 \times_{Y(2)} \boldsymbol{a}_2)$ is finite, where the union is taken over all pairs of independent $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{Z}^n$. The claim follows applying our Theorem 1.1 since $\mathcal{C}'$ is not contained in a proper flat subgroup scheme. □

3. O-MINIMAL STRUCTURES AND A RESULT OF PILA

In this section we introduce the notion of o-minimal structure, recall some definitions and properties we will need later and state a result of Pila from [Pil11]. For the basic properties of o-minimal structures we refer to [Dri98] and [DM96].

Definition 3.1. A *structure* is a sequence $\mathcal{S} = (\mathcal{S}_N)$, $N \geq 1$, where each $\mathcal{S}_N$ is a collection of subsets of $\mathbb{R}^N$ such that, for each $N, M \geq 1$:

(1) $\mathcal{S}_N$ is a boolean algebra (under the usual set-theoretic operations);
(2) $\mathcal{S}_N$ contains every semialgebraic subset of $\mathbb{R}^N$;
(3) if $A \in \mathcal{S}_N$ and $B \in \mathcal{S}_M$ then $A \times B \in \mathcal{S}_{N+M}$;
(4) if $A \in \mathcal{S}_{N+M}$ then $\pi(A) \in \mathcal{S}_N$, where $\pi : \mathbb{R}^{N+M} \to \mathbb{R}^N$ is the projection onto the first N coordinates.

If $\mathcal{S}$ is a structure and, in addition,

(5) $\mathcal{S}_1$ consists of all finite union of open intervals and points

then $\mathcal{S}$ is called an *o-minimal structure*.

Given a structure $\mathcal{S}$, we say that $S \subseteq \mathbb{R}^N$ is a *definable* set if $S \in \mathcal{S}_N$.

Let $U \subseteq \mathbb{R}^{N+M}$ and let π_1 and π_2 be the projection maps on the first N and on the last M coordinates, respectively. Now, for $t_0 \in \pi_2(U)$, we set $U_{t_0} = \{x \in \mathbb{R}^N : (x, t_0) \in U\} = \pi_1\left(\pi_2^{-1}(t_0)\right)$ and call U a *family* of subsets of $\mathbb{R}^N$, while U_{t_0} is called the *fiber* of U above t_0. If U is a definable set then we call it a *definable family* and one can see that the fibers U_{t_0} are definable sets too. Let $S \subseteq \mathbb{R}^N$ and $f : S \to \mathbb{R}^M$ be a function. We call f a *definable function* if its graph $\{(x, y) \in S \times \mathbb{R}^M : y = f(x)\}$ is a definable set. It is not hard to see that images and preimages of definable sets via definable functions are still definable.

There are many examples of o-minimal structures, see [DM96]. In this article we are interested in the structure of *globally subanalytic sets*, usually denoted by $\mathbb{R}_{an}$. We are not going to pause on details about this structure because it is enough for us to know that if $D \subseteq \mathbb{R}^N$ is a compact definable set, I is an open neighborhood of D and $f : I \to \mathbb{R}^M$ is an analytic function then $f(D)$ is definable in $\mathbb{R}_{an}$.

We now fix an o-minimal structure $\mathcal{S}$. Many important properties of o-minimal structures follow from the *cell decomposition Theorem* ([DM96], 4.2). One of these is the fact that definable families have a uniform bound on the number of connected components of the fibers.

Proposition 3.2 ([DM96], 4.4)**.** *Let U be a definable family. There exists a positive integer γ such that each fiber of U has at most γ connected components.*

Now, let $S \subseteq \mathbb{R}^N$ be a non-empty definable set and let e be a non-negative integer. The set of *regular points* of dimension e, denoted by $\mathrm{reg}_e(S)$, is the set of points $x \in S$ such that there is an open neighborhood I of x with $S \cap I$ a C^1 (embedded) submanifold of $\mathbb{R}^N$ of dimension e. The *dimension* of S is the maximum e such that S has a regular point of dimension e. Note that, if S has dimension e then $S \setminus \mathrm{reg}_e(S)$ has dimension $\le e - 1$.

Definition 3.3. A *definable block* of dimension e in $\mathbb{R}^N$ is a connected definable set B of dimension e contained in some semialgebraic set A of dimension e such that every point of B is a regular point of dimension e in B and A. Dimension zero is allowed: a point is a definable block. Moreover, a *definable block family* is a definable family whose non-empty fibers are all definable blocks.

We now need to define the height of a rational point. The height used by Pila in [Pil11] is not the usual projective Weil height, but a coordinatewise affine height. If a/b is a rational number written in lowest terms, then $H(a/b) = \max(|a|, |b|)$ and, for an N-tuple $(\alpha_1, \ldots, \alpha_N) \in \mathbb{Q}^N$, we set $H(\alpha_1, \ldots, \alpha_N) = \max H(\alpha_i)$. For a subset Z of $\mathbb{R}^N$ and a positive real number T we define

$$(3.1) \qquad Z(\mathbb{Q}, T) = \left\{ (\alpha_1, \ldots, \alpha_N) \in Z \cap \mathbb{Q}^N : H(\alpha_1, \ldots, \alpha_N) \le T \right\}.$$

The following theorem is a special case of Theorem 3.6 of [Pil11] (see also [Pil09]). Here, if f and g are real functions of T, the notation $f(T) \ll_{Z,\epsilon} g(T)$ means that there exists a constant γ, depending on Z and ϵ, such that $f(T) \le \gamma g(T)$ for T large enough.

Theorem 3.4 (Pila, [Pil11])**.** *Let $Z \subseteq \mathbb{R}^N \times \mathbb{R}^M$ be a definable family, and $\epsilon > 0$. There exist $J = J(Z, \epsilon) \in \mathbb{N}$ and a collection of definable block families $B^{(j)} \subseteq \mathbb{R}^N \times (\mathbb{R}^M \times \mathbb{R}^{M_j})$, for $j = 1, \ldots, J$, such that*

(1) each point in each fiber of $B^{(j)}$ is regular of dimension e_j;
(2) for each $(t, u) \in \mathbb{R}^M \times \mathbb{R}^{M_j}$, the fiber $B^{(j)}_{(t,u)} \subseteq Z_t$;
(3) for every $t \in \pi_2(Z)$, $Z_t(\mathbb{Q}, T)$ is contained in the union of $\ll_{Z,\epsilon} T^\epsilon$ definable blocks, each a fiber of one of the $B^{(j)}$.

4. Points lying on rational linear varieties

Let $n \ge 2$ be an integer and let $\ell_1, \ldots, \ell_n, f, g$ be holomorphic functions on a connected neighborhood I of some closed disc $D \subseteq \mathbb{C}$. Suppose that

$$(4.1) \qquad \ell_1, \ldots, \ell_n \text{ are algebraically independent over } \mathbb{C}(f, g) \text{ on } D,$$

and $f(\lambda)$ and $g(\lambda)$ are $\mathbb{R}$-linearly independent for every $\lambda \in D$.

For some positive real T, denote by $D(T)$ the set of $\lambda \in D$ such that

$$(4.2) \qquad \begin{cases} a_1 \ell_1(\lambda) + \cdots + a_n \ell_n(\lambda) = a_{n+1} f(\lambda) + a_{n+2} g(\lambda) \\ b_1 \ell_1(\lambda) + \cdots + b_n \ell_n(\lambda) = b_{n+1} f(\lambda) + b_{n+2} g(\lambda) \end{cases}$$

for some linearly independent vectors $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in (\mathbb{Z} \cap [-T, T])^n$ and some a_{n+1}, $a_{n+2}, b_{n+1}, b_{n+2} \in \mathbb{Z}$.

The following proposition gives the desired upper bound mentioned in the introduction. We postpone its proof until the end of this section after developing some auxiliary tools.

Proposition 4.1. *Under the above hypotheses, for every $\epsilon > 0$, $|D(T)| \ll_\epsilon T^\epsilon$.*

Define
$$\Delta = f\overline{g} - \overline{f}g,$$

which does not vanish on D, since $f(\lambda)$ and $g(\lambda)$ are $\mathbb{R}$-linearly independent for every $\lambda \in D$. Moreover, let

$$u_j = \frac{\ell_j \overline{g} - \overline{\ell_j} g}{\Delta}, \quad v_j = -\frac{\ell_j \overline{f} - \overline{\ell_j} f}{\Delta}.$$

One can easily check that these are real-valued and, furthermore, we have

$$\ell_j = u_j f + v_j g.$$

If we view D and I as a subsets of $\mathbb{R}^2$, then u_j and v_j are real analytic functions on I.

Define

$$\Theta : D \to \mathbb{R}^{2n}$$

$$\lambda \mapsto (u_1(\lambda), v_1(\lambda), \ldots, u_n(\lambda), v_n(\lambda))$$

and set $S = \Theta(D)$. This is a definable set in $\mathbb{R}_{\mathrm{an}}$. In what follows, $(u_1, v_1, \ldots, u_n, v_n)$ will just indicate coordinates in $\mathbb{R}^{2n}$.

For $T > 0$, we call $S(T)$ the set of points of S of coordinates $(u_1, v_1, \ldots, u_n, v_n)$ such that there exist linearly independent vectors $(a_1, \ldots, a_{n+2}), (b_1, \ldots, b_{n+2}) \in \mathbb{Q}^{n+2}$ of height at most T with

$$(4.3) \qquad \begin{cases} a_1 u_1 + \cdots + a_n u_n = a_{n+1} \\ a_1 v_1 + \cdots + a_n v_n = a_{n+2} \\ b_1 u_1 + \cdots + b_n u_n = b_{n+1} \\ b_1 v_1 + \cdots + b_n v_n = b_{n+2}. \end{cases}$$

We will need the following lemma.

Lemma 4.2. *For every choice of $a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2} \in \mathbb{R}$ (not only rationals), not all zero, the subset of S for which (4.3) holds is finite.*

Proof. By contradiction suppose that the subset of S of points satisfying (4.3) for some choice of coefficients is infinite. This would imply that there exists an infinite set $E \subseteq D$ on which, for instance, if at least one of the $a_j \neq 0$, for every $\lambda \in E$,

$$a_1 \ell_1(\lambda) + \cdots + a_n \ell_n(\lambda) = a_{n+1} f(\lambda) + a_{n+2} g(\lambda).$$

Since this relation holds on a set with an accumulation point, it must hold on the whole D (see Ch. III, Theorem 1.2 (ii) of [Lan85]), contradicting the hypothesis (4.1). $\qquad\square$

The following proposition is the main tool to prove Proposition 4.1.

Proposition 4.3. *For every $\epsilon > 0$ we have*

$$|S(T)| \ll_\epsilon T^\epsilon.$$

Proof. We are counting points of S that lie on linear varieties of $\mathbb{R}^{2n}$ defined by systems of the form (4.3).

Let us consider the set $W \subset \mathbb{R}^{4n+4}$ defined as

$$W = \left\{ (u_1, v_1, \ldots, u_n, v_n, a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2}) \in S \times \mathbb{R}^{2n+4} : \right.$$
$$\left. \text{with (4.3) and } (a_1, \ldots, a_{n+2}) \text{ and } (b_1, \ldots, b_{n+2}) \text{ are linearly independent} \right\},$$

which is a definable set. Denote by π_1 the projection on S and by π_2 the projection on the last $2n + 4$ coordinates. Given a point L of $\pi_2(W)$, we write $\tau(L)$ for the set of points of S that lie on the affine subspace corresponding to L, i.e., $\tau(L) = \pi_1\left(\pi_2^{-1}(L)\right)$. In other words, if we consider W as a family of subsets of $\mathbb{R}^{2n}$, $\tau(L)$ is just the fiber W_L. This is a definable subset of S and we have that it must be zero-dimensional by Lemma 4.2. By Proposition 3.2, there exists a positive integer γ_1 such that $|\tau(L)| \leq \gamma_1$, for every $L \in \pi_2(W)$. Moreover, for $V \subseteq \pi_2(W)$, we write $\tau(V)$ for $\pi_1\left(\pi_2^{-1}(V)\right)$.

Now, let us call $\widehat{W} = \pi_2(W) \subseteq \mathbb{R}^{2n+4}$. Recall the definition in (3.1) and note that $S(T) \subseteq \tau\left(\widehat{W}(\mathbb{Q}, T)\right)$. By Theorem 3.4, there is a finite number of definable block families such that, for every ϵ_1, $\widehat{W}(\mathbb{Q}, T)$ is contained in the union of $\ll_{W,\epsilon_1} T^{\epsilon_1}$ definable blocks, each a fiber of one of these families. We have that $S(T) \subseteq \bigcup_B \tau(B)$ where the union is taken over the $\ll_{W,\epsilon_1} T^{\epsilon_1}$ definable blocks mentioned above.

Let us fix a definable block family U with fibers $U_t \subseteq \widehat{W}$. We claim that, for every ϵ_2, each fiber U_t of U gives rise to $\ll_{U,\epsilon_2} T^{\epsilon_2}$ points on $S(T)$, i.e., that $|\tau(U_t) \cap S(T)| \ll_{U,\epsilon_2} T^{\epsilon_2}$ for every fiber U_t. Once we proved this, the claim of the proposition follows easily after fixing ϵ_1 and ϵ_2 with $\epsilon_1 \epsilon_2 = \epsilon$, e.g., $\epsilon_1 = \epsilon_2 = \sqrt{\epsilon}$.

We proceed by induction on the dimension e of the fibers of U. By Lemma 4.2, the claim is true for $e = 0$.

Suppose now $e > 0$. We denote by $B_\eta(L)$ the Euclidean ball centered in L of radius η, and define, for $m = 1, \ldots, \gamma_1$,

$$V^{(m)} = \left\{ (L, t) \in U : \exists \eta > 0, \exists A_1, \ldots, A_m \in S : \forall L' \in B_\eta(L) \cap U_t, \tau(L') = \{A_1, \ldots, A_m\} \right\}.$$

These are definable families and so is $V := \bigcup_{m=1}^{\gamma_1} V^{(m)}$ as it is a finite union of definable sets. Hence, by Proposition 3.2, there exists γ_2 such that all fibers V_t have at most γ_2 connected components. It is clear that, for each L in the same connected component, $\tau(L)$ consists of the same set of not more than γ_1 points; therefore, each fiber V_t of V gives rise to at most $\gamma_1 \gamma_2$ points of $S(T)$, i.e., $|S(T) \cap \tau(V_t)| \leq \gamma_1 \gamma_2$.

Now we want to prove that all the fibers of $Z = U \setminus V$ have dimension $< e$. Suppose not and let L be an e-regular point of a fiber Z_t. Then, after fixing a ball $B_\eta(L)$ with connected $B_\eta(L) \cap U_t \subseteq Z_t$, we set $\{A_1, \ldots, A_m\} = \bigcap_{L' \in B_\eta(L) \cap Z_t} \tau(L')$, i.e., the set of points of S that lie on all subspaces in $B_\eta(L) \cap Z_t$. By definition of Z, $\tau^{-1}\left(\{A_1, \ldots, A_m\}\right) \cap B_\eta(L) \cap Z_t$ must be of dimension $< e$, therefore there exist $L_0 \in B_\eta(L) \cap Z_t$ and η_0 such that for every $L' \in B_{\eta_0}(L_0) \cap Z_t$, $\tau(L') \supsetneq \{A_1, \ldots, A_m\}$. Thus, we can define $f : B_{\eta_0}(L_0) \cap Z_t \to S$ that associates to L' a point

in $\tau(L')$ different from $A_1, \ldots, A_m$. This is a definable function and, taking η_0 small enough (and possibly choosing a different L_0), we can also suppose that it is differentiable ([DM96], C.2 Lemma).

Now, assume the derivative of f is zero in all directions. Then, f is constant and there exists a point $A_{m+1} \in \tau(L')$ for all $L' \in B_{\eta_0}(L_0) \cap Z_t$. We repeat this procedure of finding a point, a ball and a function like above and continue until this function has non-zero derivative in some direction. This procedure must stop because otherwise we would have a point L' with $|\tau(L')| > \gamma_1$, contradicting the above considerations.

We can therefore suppose that there are $L_0 \in B_\eta(L) \cap Z_t$ and η_0 such that f is differentiable on $B_{\eta_0}(L_0) \cap Z_t$ and with non zero-derivative in some direction. Now, recall that L_0 is an e-regular point of U_t and, by definition of definable block, of a semialgebraic set that contains it. Therefore, $B_{\eta_0}(L_0) \cap U_t = B_{\eta_0}(L_0) \cap Z_t$ is semialgebraic. Thus, if we intersect it with a suitable linear variety, we get an algebraic curve segment C in $B_{\eta_0}(L_0) \cap Z_t$, passing through L_0 in the direction for which the derivative of f is non-zero. The function f is non-constant on C. Consider $C' = f(C) \times C$. By definition of f, C' is a real-analytic curve segment in W. Moreover, let us define $D' = \Theta^{-1}(f(C))$. As f is not constant on C, D' is an infinite subset of D.

Now, on D' the coordinate functions $a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2}$ satisfy $2n + 3$ independent algebraic relations with coefficients in $\mathbb{C}$ and, combining the relations of (4.3), we have also

$$\begin{cases} a_1\ell_1 + \cdots + a_n\ell_n = a_{n+1}f + a_{n+2}g \\ b_1\ell_1 + \cdots + b_n\ell_n = b_{n+1}f + b_{n+2}g. \end{cases}$$

Each of these two is independent of the previous $2n + 3$ relations and they are independent of each other because we imposed $(a_1, \ldots, a_{n+2})$ and $(b_1, \ldots, b_{n+2})$ to be linearly independent. Therefore, as the $3n + 4$ functions $a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2}, \ell_1, \ldots, \ell_n$ satisfy $2n + 5$ independent algebraic relations with coefficients in $\mathbb{C}[f, g]$ on the infinite set D', they continue to do so on I. Therefore, if $F := \mathbb{C}(f, g)$,

$$\mathrm{tr.deg}_F F(\ell_1, \ldots, \ell_n) < n.$$

This contradicts the hypothesis (4.1).

We have just proved that there cannot be any e-regular point on any fiber of Z. We apply Pila's result (Theorem 3.4) again on Z. There is a finite number of definable block families such that, for each ϵ_3 and for each fiber Z_t, $Z_t(\mathbb{Q}, T)$ is contained in the union of $\ll_{Z,\epsilon_3} T^{\epsilon_3}$ definable blocks, each a fiber of one of these families. The fibers of these families must have dimension $< e$, therefore our inductive hypothesis implies that if U' is one of them, then, for every ϵ_4, $|\tau(U'_{t'}) \cap S(T)| \ll_{U',\epsilon_4} T^{\epsilon_4}$, for every fiber $U'_{t'}$ of U'. This means that, after choosing $\epsilon_3 = \epsilon_4 = \sqrt{\epsilon_2}$, for each fiber Z_t, we have $|\tau(Z_t) \cap S(T)| \ll_{Z,\epsilon_2} T^{\epsilon_2}$. Now recall that we had $U_t = V_t \cup Z_t$ and that V_t gives rise to at most $\gamma_1\gamma_2$ points of $S(T)$. This proves our claim and the proposition. $\square$

Remark. We would like to point out that this last proposition can be deduced from recent work of Habegger and Pila, in particular Corollary 7.2 of [HP14].

We are now ready to prove Proposition 4.1.

Proof of Proposition 4.1. Since f and g are linearly independent, if $\lambda \in D$ satisfies (4.2) then (4.3) holds for $\Theta(\lambda)$. Now, since D is a compact subset of $\mathbb{R}^2$, each $\ell_j(D)$ is bounded and therefore, if $\ell_1(\lambda), \ldots, \ell_n(\lambda), f(\lambda), g(\lambda)$ satisfy (4.2), then $|a_{n+1}|, |a_{n+2}|, |b_{n+1}|, |b_{n+2}|$ are bounded in terms of $|a_1|, \ldots, |a_n|, |b_1|, \ldots, |b_n|$ and thus of T. Therefore, $\Theta(\lambda) \in S(\gamma_3 T)$ for some γ_3 independent of T. Now, using Proposition 3.2 and Lemma 4.2, we see that there exists a γ_4 such that, for any choice of $a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2}$, there are at most γ_4 elements λ in D such that $\ell_1(\lambda), \ldots, \ell_n(\lambda), f(\lambda), g(\lambda)$ satisfy (4.2). Thus $|D(T)| \ll |S(\gamma_3 T)|$ and the claim follows from Proposition 4.3. $\qquad\square$

5. Periods and elliptic logarithms

In this section we introduce the functions which we will apply Proposition 4.1 to. We follow [MZ12].

It is well known that there is an analytic isomorphism between $E_\lambda(\mathbb{C})$ and $\mathbb{C}/L_\lambda$, where L_λ is a rank 2 lattice in $\mathbb{C}$. Consider the hypergeometric function

$$F(t) = F\left(\frac{1}{2}, \frac{1}{2}, 1; t\right) = \sum_{m=0}^{\infty} \frac{(2m)!^2}{2^{4m} m!^4} t^m,$$

and let

(5.1) $f(t) = \pi F(t), \quad \text{and} \quad g(t) = \pi i F(1 - t).$

Moreover, we define

$$\Lambda = \{t \in \mathbb{C} : |t| < 1, |1 - t| < 1\}.$$

The functions f and g are well-defined and analytic in Λ, as functions of t. Moreover, they are well-defined as functions of $\boldsymbol{c}$ in $\lambda^{-1}(\Lambda) \subset \mathcal{C}(\mathbb{C})$.

By (6.1) Theorem, p. 179, of [Hus87], $f(\lambda)$ and $g(\lambda)$ are basis elements of the period lattice L_λ of E_λ with respect to $\frac{dX}{2Y}$. Therefore, if $\exp_\lambda$ is the associated exponential map from $\mathbb{C}$ to $E_\lambda(\mathbb{C})$, we have

$$\exp_\lambda(f(\lambda)) = \exp_\lambda(g(\lambda)) = O,$$

where O denotes the origin in E_λ. Let $P_j = (x_j, y_j)$, where x_j, y_j are coordinate functions in $\mathbb{C}(\mathcal{C})$. We can suppose that, for every j, $x_j \neq 0, 1, \lambda$ identically, otherwise the corresponding P_j would be identically 2-torsion, contradicting the hypothesis of Theorem 1.1.

Now, we want to define suitable functions $z_j(\boldsymbol{c})$ such that $\exp_{\lambda(\boldsymbol{c})}(z_j(\boldsymbol{c})) = P_j(\boldsymbol{c})$; in other words, we want z_j to be the elliptic logarithm of P_j.

Let $\widehat{\mathcal{C}}$ be the subset of points $\boldsymbol{c} \in \mathcal{C}$ such that $\lambda(\boldsymbol{c}), x_j(\boldsymbol{c}) \neq 0, 1, \infty$, $x_j(\boldsymbol{c}) \neq \lambda(\boldsymbol{c})$ for every $j = 1, \ldots, n$ and $\boldsymbol{c}$ is not a singular point or a point on which the differential of λ vanishes.

Note that, in this way, we excluded finitely many $\boldsymbol{c} \in \mathcal{C}$, and these are algebraic points of $\mathcal{C}$. Moreover, on $\widehat{\mathcal{C}}$, the coordinate function λ has everywhere a local inverse.

We now follow the construction of [MZ12], p. 459. Fix a point $\boldsymbol{c}_* \in \widehat{\mathcal{C}}$ and choose a path in the x_j-plane from $x_j(\boldsymbol{c}_*)$ to ∞ and not passing through $0, 1$ and $\lambda(\boldsymbol{c}_*)$. We also fix a determination of $Y = \sqrt{X(X - 1)(X - \lambda(\boldsymbol{c}_*))}$ equal to $y_j(\boldsymbol{c}_*)$ at $X = x_j(\boldsymbol{c}_*)$. Therefore, the path corresponds to a path on the elliptic curve $E_{\lambda(\boldsymbol{c}_*)}$ from the point $P_j(\boldsymbol{c}_*)$ to the origin O. Hence we can define $z_j(\boldsymbol{c}_*)$ as the integral

$$z_j(\boldsymbol{c}_*) = \int_{x_j(\boldsymbol{c}_*)}^{\infty} \frac{dX}{2\sqrt{X(X - 1)(X - \lambda(\boldsymbol{c}_*))}}.$$

We can extend it to a $\boldsymbol{c}$ close to $\boldsymbol{c}_*$ by

$$z_j(\boldsymbol{c}) = \int_{x_j(\boldsymbol{c}_*)}^{\infty} \frac{dX}{2\sqrt{X(X-1)(X-\lambda(\boldsymbol{c}))}} + \int_{x_j(\boldsymbol{c}_*)}^{x_j(\boldsymbol{c})} \frac{dX}{2\sqrt{X(X-1)(X-\lambda(\boldsymbol{c}))}}.$$

In fact, in the first integral on the right we use the same path fixed before and the integrand is determined by continuity from the previously chosen determination of Y. Hence, this term is an analytic function in $\lambda(\boldsymbol{c})$. For the second term, we can take any local path from $x_j(\boldsymbol{c}_*)$ to $x_j(\boldsymbol{c})$. We can extend the integrand as a double power series in $\lambda(\boldsymbol{c}) - \lambda(\boldsymbol{c}_*)$ and in $X - x_j(\boldsymbol{c}_*)$; the result will be a double power series in $\lambda(\boldsymbol{c}) - \lambda(\boldsymbol{c}_*)$ and $x_j(\boldsymbol{c}) - x_j(\boldsymbol{c}_*)$. Notice that we have at any rate $\exp_{\lambda(\boldsymbol{c})}(z_j(\boldsymbol{c})) = P_j(\boldsymbol{c})$ for every $j = 1, \ldots, n$.

In this way, fixing a $\boldsymbol{c}_* \in \lambda^{-1}(\Lambda) \cap \widehat{\mathcal{C}}$, the functions $z_1, \ldots, z_n$ are well defined on a small neighborhood N_* on $\mathcal{C}$. Moreover, if we take N_* small enough, we can see them as analytic functions of λ on $\lambda^{-1}(N_*)$.

We will need the following transcendence result.

Lemma 5.1. *The functions $z_1, \ldots, z_n$ are algebraically independent over $\mathbb{C}(f, g)$ on N_*.*

Proof. The $z_1, \ldots, z_n, f, g$ are analytic functions of λ, linearly independent over $\mathbb{Z}$. Indeed, a relation $a_1 z_1 + \cdots + a_n z_n = a_{n+1} f + a_{n+2} g$, with integer coefficients, would map via $\exp_\lambda$ to a relation of the form (1.2) on N_*, and therefore on the whole $\mathcal{C}$, which cannot hold by the hypothesis of the Theorem. Moreover, if $\wp_\lambda$ is the Weierstrass $\wp$-function associated to L_λ, the $\wp_\lambda(z_i)$ are algebraic functions of λ because $\wp_\lambda(z_j) = x_j - \frac{1}{3}(\lambda + 1)$ (see (3.8) on p. 7 of [MZ08]). Therefore, the hypotheses of Théorème 5 on p. 136 of [Ber90] are satisfied and we can apply it to get the claim. $\square$

We would like now to extend our functions $f, g, z_1, \ldots, z_n$ on $\widehat{\mathcal{C}}$.

If $\boldsymbol{c} \in \widehat{\mathcal{C}}$, one can continue f and g to a neighborhood $N_{\boldsymbol{c}}$ of $\boldsymbol{c}$. In fact, if we choose $\boldsymbol{c} \in \widehat{\mathcal{C}}$ and a path from $\boldsymbol{c}_*$ to $\boldsymbol{c}$ lying in $\widehat{\mathcal{C}}$, we can easily continue f and g along the path using (5.1).

To continue z_j from a point $\boldsymbol{c}_*$ to a $\boldsymbol{c}$ in $\widehat{\mathcal{C}}$, it is sufficient to verify that, if N_1 and N_2 are two open small subsets in $\widehat{\mathcal{C}}$, with $N_1 \cap N_2$ connected, and z_j has analytic definitions z_j' on N_1 and z_j'' on N_2, then it has an analytic definition on the union $N_1 \cup N_2$. But we saw that $\exp_\lambda(z_j) = P_j$ for every $j = 1, \ldots, n$, hence on $N_1 \cap N_2$ we have $\exp_\lambda(z_j') = \exp_\lambda(z_j'')$. This means that there exist rational integers u, v with $z_j'' = z_j' + uf + vg$ on this intersection, and they must be constant there. Hence it is enough to change z_j'' to $z_j'' - uf - vg$ on N_2.

Using the same path, it is now clear that we can continue the function $(f, g, z_1, \ldots, z_n)$ from a small neighborhood of $\boldsymbol{c}_*$ to a small neighborhood $N_{\boldsymbol{c}} \subseteq \widehat{\mathcal{C}}$ of $\boldsymbol{c}$, and the obtained function $(f^{\boldsymbol{c}}, g^{\boldsymbol{c}}, z_1^{\boldsymbol{c}}, \ldots, z_n^{\boldsymbol{c}})$ is analytic on $N_{\boldsymbol{c}}$. Moreover, the functions preserve the algebraic independence, as the following lemma shows.

Lemma 5.2. *The functions $z_1^{\boldsymbol{c}}, \ldots, z_n^{\boldsymbol{c}}$ are algebraically independent over $\mathbb{C}(f^{\boldsymbol{c}}, g^{\boldsymbol{c}})$ on $N_{\boldsymbol{c}}$.*

Proof. Any algebraic relation can be continued to a neighborhood N_* of some $\boldsymbol{c}_* \in \lambda^{-1}(\Lambda)$, contradicting Lemma 5.1. $\square$

Furthermore, the lattice L_λ is still generated by $f^{\boldsymbol{c}}$ and $g^{\boldsymbol{c}}$ on $N_{\boldsymbol{c}}$, see Lemma 6.1 of [MZ12] or Lemma 4.1 of [MZ10].

Now fix $\boldsymbol{c} \in \mathcal{C}$ and $N_{\boldsymbol{c}} \subseteq \widehat{\mathcal{C}}$. Since we are avoiding singular points and points on which the differential of λ vanishes, λ gives an analytic isomorphism $\lambda : N_{\boldsymbol{c}} \to \lambda(N_{\boldsymbol{c}})$. Then, we can view $z_1^{\boldsymbol{c}}, \ldots, z_n^{\boldsymbol{c}}, f^{\boldsymbol{c}}, g^{\boldsymbol{c}}$ as analytic functions on $\lambda(N_{\boldsymbol{c}})$.

6. Linear relations on a fixed curve

In this section we prove a general fact about linear relations on elliptic curves.

For a point $(\alpha_1, \ldots, \alpha_N) \in \overline{\mathbb{Q}}^N$, the absolute logarithmic Weil height $h(\alpha_1, \ldots, \alpha_N)$ is defined by

$$h(\alpha_1, \ldots, \alpha_N) = \frac{1}{[\mathbb{Q}(\alpha_1, \ldots, \alpha_N) : \mathbb{Q}]} \sum_v \log \max\{1, |\alpha_1|_v, \ldots, |\alpha_N|_v\},$$

where v runs over a suitably normalized set of valuations of $\mathbb{Q}(\alpha_1, \ldots, \alpha_N)$.

Let α be an algebraic number and consider the Legendre curve $E = E_\alpha$ defined by the equation $Y^2 = X(X-1)(X-\alpha)$. Moreover, let $P_1, \ldots, P_n$ be linearly dependent points on E, defined over some finite extension K of $\mathbb{Q}(\alpha)$ of degree $\kappa = [K : \mathbb{Q}]$. Suppose that $P_1, \ldots, P_n$ have Néron-Tate height $\widehat{h}$ at most q (for the definition of Néron-Tate height, see for example p. 255 of [Mas88]). In case the $P_1, \ldots, P_n$ are all torsion, i.e., $\widehat{h}(P_j) = 0$ for all j, we set $q = 1$. We define

$$L(P_1, \ldots, P_n) = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n : a_1 P_1 + \cdots + a_n P_n = O\}.$$

This is a sublattice of $\mathbb{Z}^n$ of some positive rank r. We want to show that $L(P_1, \ldots, P_n)$ has a set of generators with small max norm $|\boldsymbol{a}| = \max\{|a_1|, \ldots, |a_n|\}$.

Lemma 6.1. *Under the above hypotheses, there are generators $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ of $L(P_1, \ldots, P_n)$ with*

$$|\boldsymbol{a}_i| \leq \gamma_1 \kappa^{\gamma_2} (h(\alpha) + 1)^{2n} q^{\frac{1}{2}(n-1)},$$

for some positive constants γ_1, γ_2 depending only on n.

Proof. The Weierstrass form $\widetilde{E} = \widetilde{E}_\alpha$ of $E = E_\alpha$ has equation

$$\widetilde{Y}^2 = 4\widetilde{X}^3 - g_2 \widetilde{X} - g_3,$$

where $g_2 = \frac{4}{3}(\alpha^2 - \alpha + 1)$ and $g_3 = \frac{4}{27}(\alpha - 2)(\alpha + 1)(2\alpha - 1)$ (see (3.7) of [MZ10]). The isomorphism ϕ from E to $\widetilde{E}$ is given by

$$\widetilde{X} = X - \frac{1}{3}(\alpha + 1), \quad \widetilde{Y} = 2Y.$$

Now, $\widetilde{E}$ is clearly defined over $\mathbb{Q}(\alpha)$ and any linear relation $a_1 P_1 + \cdots + a_n P_n = O$ on E carries on to $\widetilde{E}$ and vice versa. Moreover, the $Q_i = \phi(P_i)$ will have coordinates in K and the same Néron-Tate height of the P_i, hence also bounded by q.

First, suppose that at least one of the points has infinite order. By Theorem E of [Mas88], if $Q_1, \ldots, Q_n$ are linearly dependent points on $\widetilde{E}(K)$, of Néron-Tate height at most $q \geq \eta$, then $L(Q_1, \ldots, Q_n)$ is generated by vectors with max norm at most

$$n^{n-1} \omega \left(\frac{q}{\eta}\right)^{\frac{1}{2}(n-1)},$$

where $\omega = \left|\widetilde{E}_{\text{tors}}(K)\right|$ and $\eta = \inf \widehat{h}(P)$, for $P \in \widetilde{E}(K) \setminus \widetilde{E}_{\text{tors}}(K)$. We need to bound ω and η. The constants $\gamma_3, \ldots, \gamma_9$ are absolute constants.

For the first we use a result of David [Dav97]. By Théorème 1.2 (i) of [Dav97], choosing any archimedean v and noting that, by David's definition, $h_v\left(\widetilde{E}\right) \geq \frac{\sqrt{3}}{2}$, one has

$$\omega \leq \gamma_3(\kappa h + \kappa \log \kappa),$$

where $h = \max\left\{1, h\left(j_{\widetilde{E}}\right)\right\}$. Now, $j_{\widetilde{E}} = 2^8 \frac{(\alpha^2 - \alpha + 1)^3}{\alpha^2(\alpha-1)^2}$ (see for instance [Hus87], p. 83). Therefore, $h \leq \gamma_4(h(\alpha) + 1)$ and we have

(6.1) $$\omega \leq \gamma_5(h(\alpha) + 1)\kappa^2.$$

For the lower bound on η, we use a result of Masser (Corollary 1 of [Mas89a]). In Masser's bound a constant depending on κ appears in the denominator. However, going through the proof one can see that this constant is polynomial in κ, as noted by David on p. 109 of [Dav97]. Therefore,

$$\eta \geq \frac{\gamma_6}{w\kappa^{\gamma_7+3}(w + \log \kappa)^2} \geq \gamma_8 \kappa^{-(\gamma_7+5)} w^{-3},$$

where $w = \max\{1, h(g_2), h(g_3)\}$. As g_2 and g_3 are polynomials in α, $w \leq \gamma_9(h(\alpha) + 1)$. Consequently, $L(Q_1, \ldots, Q_n)$ will have generators of norms at most

$$\gamma_1 \kappa^{\gamma_2}(h(\alpha) + 1)^{2n} q^{\frac{1}{2}(n-1)},$$

with γ_1, γ_2 depending only on n.

In case all the points are torsion points, it is clear that one can take $|\boldsymbol{a}_i| \leq \omega$ and use (6.1). $\qquad \square$

7. BOUNDED HEIGHT

In this section we see that the height of the points on the curve $\mathcal{C}$ for which there is at least one dependence relation is bounded and a few consequences of this fact.

Let k be a number field over which $\mathcal{C}$ is defined. Suppose also the finitely many points we excluded from $\mathcal{C}$ to get $\widehat{\mathcal{C}}$, which are algebraic, are defined over k. Clearly, there are $f_1, \ldots, f_n \in k[T]$ such that $f_j(x_j, \lambda) = 0$ for every j, identically on the curve.

Let $\mathcal{C}'$ be the set of points of $\widehat{\mathcal{C}}$ such that $P_1, \ldots, P_n$ satisfy two independent relations on the specialized curve and let $\boldsymbol{c}_0 \in \mathcal{C}'$. Since $\mathcal{C}$ is defined over $\overline{\mathbb{Q}}$, the $x_j(\boldsymbol{c}_0)$ and $\lambda(\boldsymbol{c}_0)$ must be algebraic, unless the P_j are identically linearly dependent, which we excluded by hypothesis. Then by Silverman's Specialization Theorem [Sil83] (see also Appendix C of [Zan12]) there exists $\gamma_1 > 0$ such that

(7.1) $$h(\lambda(\boldsymbol{c}_0)) \leq \gamma_1.$$

We see now a few consequences of this bound. If $\delta > 0$ is a small real number, let us call

$$\Lambda_\delta = \left\{t \in \mathbb{C} : |t| \leq \frac{1}{\delta}, |t - \lambda(\boldsymbol{c})| \geq \delta \text{ for all } \boldsymbol{c} \in \mathcal{C} \setminus \widehat{\mathcal{C}}\right\}.$$

Lemma 7.1. *There is a positive δ such that there are at least $\frac{1}{2}[k(\lambda(\boldsymbol{c}_0)) : k]$ different k-embeddings σ of $k(\lambda(\boldsymbol{c}_0))$ in $\mathbb{C}$ such that $\sigma(\lambda(\boldsymbol{c}_0))$ lies in Λ_δ for all $\boldsymbol{c}_0 \in \mathcal{C}'$.*

Proof. See Lemma 8.2 of [MZ12]. $\qquad \square$

Remark. We would like to point out that, as suggested by the referee, it might be possible to avoid the restriction to a compact domain and the use of the previous lemma by exploiting the work of Peterzil and Starchenko [PS04], who proved that it is possible to define the Weierstrass $\wp$ function globally in the structure $\mathbb{R}_{\text{an,exp}}$.

Lemma 7.2. *There exist positive constants γ_2, γ_3 such that, for every $\boldsymbol{c}_0 \in \mathcal{C}'$ and every $j = 1, \ldots, n$, we have*

$$\widehat{h}(P_j(\boldsymbol{c}_0)) \leq \gamma_2,$$

and the $P_j(\boldsymbol{c}_0)$ are defined over some number field $K \supseteq k(\lambda(\boldsymbol{c}_0))$ with

$$[K : \mathbb{Q}] \leq \gamma_3 d_0,$$

where $d_0 = [k(\lambda(\boldsymbol{c}_0)) : k]$.

Proof. Recall that each $x_j(\boldsymbol{c}_0)$ is a root of $f_j(X, \lambda(\boldsymbol{c}_0))$. This already implies the second statement. Now, we have $h(P_j(\boldsymbol{c}_0)) \leq \gamma_4(h(\lambda(\boldsymbol{c}_0)) + 1)$ and, using the work of Zimmer [Zim76], we have $\widehat{h}(P_j(\boldsymbol{c}_0)) \leq h(P_j(\boldsymbol{c}_0)) + \gamma_5(h(\lambda(\boldsymbol{c}_0)) + 1)$. The first claim now follows from (7.1). $\square$

8. Proof of Theorem 1.1

We want to show that there are at most finitely many $\boldsymbol{c}$ on the curve such that $P_1(\boldsymbol{c}), \ldots, P_n(\boldsymbol{c})$ satisfy two linear independent relations on $E_{\lambda(\boldsymbol{c})}$. By Northcott's Theorem [Nor49] and (7.1), we only need to bound the degree d of $\lambda(\boldsymbol{c})$ over k.

Let $\boldsymbol{c}_0 \in \mathcal{C}'$, $\lambda_0 = \lambda(\boldsymbol{c}_0)$ and $d_0 = [k(\lambda(\boldsymbol{c}_0)) : k]$. First, by Lemma 7.1, we can choose δ, independent of $\boldsymbol{c}_0$, such that λ_0 has at least $\frac{1}{2}d_0$ conjugates in Λ_δ. Now, since Λ_δ is compact, it can be covered by γ_2 closed discs $D_{\boldsymbol{c}_1}, \ldots, D_{\boldsymbol{c}_{\gamma_2}} \subseteq \lambda(\widehat{\mathcal{C}})$, where $D_{\boldsymbol{c}_i}$ is centered in $\lambda(\boldsymbol{c}_i)$, for some $\boldsymbol{c}_i \in \widehat{\mathcal{C}}$.

We can suppose that the closed disc $D_{\boldsymbol{c}_1}$ contains at least $\frac{1}{2\gamma_2}d_0$ conjugates λ_0^σ. Now, each such conjugate comes from a $\boldsymbol{c}_0^\sigma \in N_{\boldsymbol{c}_1}$ and the corresponding points $P_1(\boldsymbol{c}_0^\sigma), \ldots, P_n(\boldsymbol{c}_0^\sigma)$ satisfy the same linear relations. So there are linearly independent $(a_1, \ldots, a_n), (b_1, \ldots, b_n)$ such that

$$(8.1) \qquad a_1 P_1(\boldsymbol{c}_0^\sigma) + \cdots + a_n P_n(\boldsymbol{c}_0^\sigma) = b_1 P_1(\boldsymbol{c}_0^\sigma) + \cdots + b_n P_n(\boldsymbol{c}_0^\sigma) = O,$$

on $E_\lambda(\boldsymbol{c}_0^\sigma)$.

By Lemma 7.2, $\widehat{h}(P_j(\boldsymbol{c}_0^\sigma)) \leq \gamma_3$ and the points are defined over some finite extension of $k(\lambda(\boldsymbol{c}_0^\sigma))$ of degree at most $\gamma_4 d_0$. Therefore, applying Lemma 6.1 and recalling (7.1), we can suppose that the a_j and b_j are in absolute value less than or equal to $\gamma_5 d_0^{\gamma_6}$.

Now, recall that, in Section 5, on $\lambda(N_{\boldsymbol{c}_1}) \supseteq D_{\boldsymbol{c}_1}$ we defined $f^{\boldsymbol{c}_1}, g^{\boldsymbol{c}_1}$ to be generators of the period lattice L_λ and the elliptic logarithms $z_1^{\boldsymbol{c}_1}, \ldots, z_n^{\boldsymbol{c}_1}$ such that

$$(8.2) \qquad \exp_\lambda(z_j^{\boldsymbol{c}_1}(\lambda)) = P_j(\lambda),$$

on $\lambda(N_{\boldsymbol{c}_1})$. We know that $z_1^{\boldsymbol{c}_1}, \ldots, z_n^{\boldsymbol{c}_1}, f^{\boldsymbol{c}_1}, g^{\boldsymbol{c}_1}$ are holomorphic functions on a neighborhood of $D_{\boldsymbol{c}_1}$, with $f^{\boldsymbol{c}_1}(\lambda)$ and $g^{\boldsymbol{c}_1}(\lambda)$ linearly independent over $\mathbb{R}$ for every $\lambda \in D_{\boldsymbol{c}_1}$, and, by Lemma 5.2, $z_1^{\boldsymbol{c}_1}, \ldots, z_n^{\boldsymbol{c}_1}$ are algebraically independent over $\mathbb{C}(f^{\boldsymbol{c}_1}, g^{\boldsymbol{c}_1})$ on $D_{\boldsymbol{c}_1}$. Therefore, the hypotheses of Proposition 4.1 are satisfied.

By (8.1) and (8.2), we have that

$$a_1 z_1^{\boldsymbol{c}_1}(\lambda_0^\sigma) + \cdots + a_n z_n^{\boldsymbol{c}_1}(\lambda_0^\sigma) \equiv b_1 z_1^{\boldsymbol{c}_1}(\lambda_0^\sigma) + \cdots + b_n z_n^{\boldsymbol{c}_1}(\lambda_0^\sigma) \equiv 0 \mod L_{\lambda_0^\sigma}.$$

Therefore, there are $a_{n+1}, a_{n+2}, b_{n+1}, b_{n+2} \in \mathbb{Z}$ such that

$$\begin{cases} a_1 z_1^{\boldsymbol{c}_1}(\lambda_0^\sigma) + \cdots + a_n z_n^{\boldsymbol{c}_1}(\lambda_0^\sigma) = a_{n+1} f^{\boldsymbol{c}_1}(\lambda_0^\sigma) + a_{n+2} g^{\boldsymbol{c}_1}(\lambda_0^\sigma) \\ b_1 z_1^{\boldsymbol{c}_1}(\lambda_0^\sigma) + \cdots + b_n z_n^{\boldsymbol{c}_1}(\lambda_0^\sigma) = b_{n+1} f^{\boldsymbol{c}_1}(\lambda_0^\sigma) + b_{n+2} g^{\boldsymbol{c}_1}(\lambda_0^\sigma). \end{cases}$$

Thus all $\lambda_0^\sigma \in D_{\boldsymbol{c}_1}$ are in $D_{\boldsymbol{c}_1}(\gamma_5 d_0^{\gamma_6})$ (recall the definition of $D(T)$ right above Proposition 4.1).

By Proposition 4.1, we have that $|D_{\boldsymbol{c}_1}(\gamma_5 d_0^{\gamma_6})| \ll_\epsilon d_0^{\gamma_6\epsilon}$. But by our choice of $D_{\boldsymbol{c}_1}$ we had at least $\frac{1}{2\gamma_2}d_0$ points in $D_{\boldsymbol{c}_1}(\gamma_5 d_0^{\gamma_6})$. Therefore, if we choose $\epsilon < \frac{1}{\gamma_6}$ we have a contradiction if d_0 is large enough.

We just deduced that d_0 is bounded and, by (7.1) and Northcott's Theorem, we have finiteness of the possible values of $\lambda(\boldsymbol{c}_0)$, which proves Theorem 1.1.

Acknowledgments

References

[Ber90]   D. Bertrand, *Extensions de D-modules et groupes de Galois différentiels*, *p*-adic analysis (Trento, 1989), Lecture Notes in Math., vol. 1454, Springer, Berlin, 1990, pp. 125–141.

[Ber11]   ———, *Special points and Poincaré bi-extensions; with an Appendix by B. Edixoven*, preprint, ArXiv: 1104.5178v1 (2011), 11 pp.

[BMPZ11] D. Bertrand, D. Masser, A. Pillay, and U. Zannier, *Relative Manin-Mumford for semi-abelian surfaces*, to appear in Proc. Edinb. Math. Soc. (2011), 40 pp.

[BMZ99] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Internat. Math. Res. Notices (1999), no. 20, 1119–1140.

[BMZ07] ———, *Anomalous subvarieties—structure theorems and applications*, Int. Math. Res. Not. IMRN (2007), no. 19, 1–33.

[BMZ08] ———, *Intersecting a plane with algebraic subgroups of multiplicative groups*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **7** (2008), no. 1, 51–80.

[Cap14]   L. Capuano, *Unlikely Intersections and applications to Diophantine Geometry*, Ph.D. thesis, Scuola Normale Superiore, 2014.

[CMPZ14] L. Capuano, D. Masser, J. Pila, and U. Zannier, *Rational points on Grassmannians and unlikely intersections in tori*, submitted (2014).

[Dav97]   S. David, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory **64** (1997), no. 1, 104–129.

[DM96]   L. van den Dries and C. Miller, *Geometric categories and o-minimal structures*, Duke Math. J. **84** (1996), no. 2, 497–540.

[Dri98]   L. van den Dries, *Tame Topology and O-minimal Structures*, London Mathematical Society Lecture Note Series, vol. 248, Cambridge University Press, Cambridge, 1998.

[Gal10]   A. Galateau, *Une minoration du minimum essentiel sur les variétés abéliennes*, Comment. Math. Helv. **85** (2010), no. 4, 775–812.

[Hab13]   P. Habegger, *Special points on fibered powers of elliptic surfaces*, J. Reine Angew. Math. **685** (2013), 143–179.

[Har77]   R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52.

[HP14]   P. Habegger and J. Pila, *O-minimality and certain atypical intersections*, to appear in Ann. Sci. École Norm. Sup. (2014).

[Hus87]   D. Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 1987.

[Lan85]   S. Lang, *Complex Analysis*, second ed., Graduate Texts in Mathematics, vol. 103, Springer-Verlag, New York, 1985.

[Mas88]   D. Masser, *Linear relations on algebraic groups*, New advances in transcendence theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, pp. 248–262.

[Mas89a] D. W. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France **117** (1989), no. 2, 247–265.

[Mas89b] _____, *Specializations of finitely generated subgroups of abelian varieties*, Trans. Amer. Math. Soc. **311** (1989), no. 1, 413–424.

[Mau08] G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. **341** (2008), no. 4, 789–824.

[MZ08] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, C. R. Math. Acad. Sci. Paris **346** (2008), no. 9-10, 491–494.

[MZ10] _____, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), no. 6, 1677–1691.

[MZ12] _____, *Torsion points on families of squares of elliptic curves*, Math. Ann. **352** (2012), no. 2, 453–484.

[MZ14a] _____, *Torsion points on families of products of elliptic curves*, Adv. Math. **259** (2014), 116–133.

[MZ14b] _____, *Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings (with appendix by V. Flynn)*, to appear in J. Eur. Math. Soc. (JEMS) (2014).

[Nor49] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–509.

[Pil04] J. Pila, *Integer points on the dilation of a subanalytic surface*, Q. J. Math. **55** (2004), no. 2, 207–223.

[Pil09] _____, *On the algebraic points of a definable set*, Selecta Math. **15** (2009), 151–170.

[Pil11] _____, *O-minimality and the André-Oort conjecture for $\mathbb{C}^n$*, Ann. of Math. (2) **173** (2011), no. 3, 1779–1840.

[Pin05] R. Pink, *A common generalization of the conjectures of André-Oort, Manin-Mumford and Mordell-Lang*, manuscript dated 17th April (2005).

[PS04] Y. Peterzil and S. Starchenko, *Uniform definability of the Weierstrass $\wp$ functions and generalized tori of dimension one*, Selecta Math. (N.S.) **10** (2004), no. 4, 525–550.

[PZ08] J. Pila and U. Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **19** (2008), no. 2, 149–162.

[Ray83] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), no. 1, 207–233.

[RV03] G. Rémond and E. Viada, *Problème de Mordell-Lang modulo certaines sous-variétés abéliennes*, Int. Math. Res. Not. (2003), no. 35, 1915–1931.

[Sil83] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.

[Sil09] _____, *The Arithmetic of Elliptic Curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Sto14] M. Stoll, *Simultaneous torsion in the Legendre family*, preprint, ArXiv: 1410.7070v1 (2014).

[Via08] E. Viada, *The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve*, Algebra Number Theory **2** (2008), no. 3, 249–298.

[Zan12] U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematics Studies, vol. 181, Princeton University Press, 2012, With appendixes by David Masser.

[Zil02] B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. (2) **65** (2002), no. 1, 27–44.

[Zim76] H. G. Zimmer, *On the difference of the Weil height and the Néron-Tate height*, Math. Z. **147** (1976), no. 1, 35–51.

Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy
E-mail address: `fbarroero@gmail.com`

Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy
E-mail address: `laura.capuano1987@gmail.com`