Linear relations in families of powers of elliptic curves

Original

Availability:
This version is available at: 11583/2790218 since: 2020-02-07T15:28:17Z

Publisher:
Mathematical Sciences Publishers

Published
DOI:10.2140/ant.2016.10.195

Terms of use:
openAccess
This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

(Article begins on next page)
Linear relations in families of powers of elliptic curves

Fabrizio Barroero and Laura Capuano
Linear relations in families of powers of elliptic curves

Fabrizio Barroero and Laura Capuano

Motivated by recent work of Masser and Zannier on simultaneous torsion on the Legendre elliptic curve $E_\lambda$ 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 $E_\lambda$ with coordinates in $\overline{\mathbb{Q}(\lambda)}$, there are at most finitely many complex numbers $\lambda_0$ such that the points $P_1(\lambda_0), \ldots, P_n(\lambda_0)$ satisfy two independent relations on $E_{\lambda_0}$. This is a special case of conjectures about unlikely intersections on families of abelian varieties.

1. Introduction

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

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

(1-1)

Masser and Zannier [2010; see also 2008] showed that there are at most finitely many complex numbers $\lambda_0 \neq 0, 1$ such that the two points

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

both have finite order on the elliptic curve $E_{\lambda_0}$. Stoll [2014] recently noted that there is actually no such $\lambda_0$. Later, Masser and Zannier [2012] 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, Zannier [2012] asks if there are finitely many $\lambda_0 \in \mathbb{C}$ such that two independent relations between the points $$(2, \sqrt{2(2 - \lambda_0)}), (3, \sqrt{6(3 - \lambda_0)})$$

and $$(5, \sqrt{20(5 - \lambda_0)})$$

hold on $E_{\lambda_0}$.

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

The authors are supported by the European Research Council, grant number 267273.

MSC2010: primary 11G05; secondary 11G50, 11U09, 14K05.

Keywords: linear relations, elliptic curves, unlikely intersections.
result, analogous to the one in [Masser and Zannier 2012] 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 \(\lambda\) since the corresponding points are identically 2-torsion. Moreover, our method allows us to deal with arbitrarily many points since we consider a curve \(C \subseteq \mathbb{A}^{2n+1}\) with coordinate functions \((x_1, y_1, \ldots, x_n, y_n, \lambda)\), where \(\lambda\) is nonconstant, such that, for every \(j = 1, \ldots, n\), the points \(P_j = (x_j, y_j)\) lie on the elliptic curve \(E_\lambda\). As the point \(c\) varies on the curve \(C\), the specialized points \(P_j(c) = (x_j(c), y_j(c))\) will lie on the specialized elliptic curve \(E_\lambda(c)\). We implicitly exclude the finitely many \(c\) with \(\lambda(c) = 0\) or 1, since in that case \(E_\lambda(c)\) is not an elliptic curve.

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

\[
a_1 P_1 + \cdots + a_n P_n = O,
\]

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

Note that the case \(n = 2\) is covered by the main proposition of [Masser and Zannier 2012] in the more general setting of a curve defined over \(\mathbb{C}\).

Moreover, Rémond and Viada [2003] proved an analogue of Theorem 1.1 for a power of a constant elliptic curve with complex multiplication, 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 [2008] and Galateau [2010]. If \(n = 2\) this is nothing but Raynaud’s theorem [1983], 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 \(E_\lambda\). Indeed, the minimal fields of definition of these three points are disjoint quadratic extensions of \(\mathbb{Q}(\lambda)\), and by conjugating one can see that the points would be identically torsion on \(E_\lambda\). This is not possible, as it can be seen in different ways (see [Zannier 2012, p. 68]). For instance, applying the Lutz–Nagell theorem [Silverman 2009, 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 \(\lambda_0\) such that a point with fixed algebraic abscissa is torsion (see [Zannier 2012, Notes to Chapter 3]). On the other hand,
the values of $\lambda$ such that at least one relation holds are “sparse”, as follows from [Masser 1989b]. Actually, a well-known theorem of Silverman [1983] 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 [Zannier 2012]. In particular, there are at most finitely many $\lambda_0$ yielding one relation in a given number field or of bounded degree over $\mathbb{Q}$.

Our proof follows the general strategy introduced in [Pila and Zannier 2008] and used in [Masser and Zannier 2008; 2010; 2012]. 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 $E_\lambda$. If we consider the coefficients $u_j, v_j$ as functions of $\lambda$ and restrict them to a compact set, we obtain a subanalytic surface $S$ in $\mathbb{R}^{2n}$. The points of $C$ 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 the case $n = 2$, one faces the simpler problem of counting rational points with bounded denominator in $S$. For this, a previous result of Pila [2004] suffices together with the fact that the surface is “sufficiently” transcendental. In the general case we adapt ideas of Pila (see [Capuano et al. 2016, Appendix]) to obtain an upper bound of order $T^\epsilon$ for the number of points of $S$ lying on subspaces of the special form mentioned above and integral 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 $C$, using a result of Bertrand [1990], we are able to show that there are no such semialgebraic curve segments.

Now, we use [Masser 1988; 1989a; David 1997] and exploit the boundedness of the height to show that the number of points of $S$ considered above is of order at least $T^\delta$ 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 similar methods, a toric analogue of Theorem 1.1 was proved in [Capuano 2014] and [Capuano et al. 2016], giving an alternative proof of a result appearing in [Bombieri et al. 1999] and generalized in [Maurin 2008] (see also [Bombieri et al. 2008]).

We will use $\gamma_1, \gamma_2, \ldots$ to denote positive constants. The indices 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 $E_\lambda$ 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 nonempty and one expects finiteness for varying integer vectors.

Our result fits in the framework of very general conjectures formulated by Zilber [2002] and Bombieri, Masser and Zannier [Bombieri et al. 2007] in the toric case and by Pink [2005] in a more general setting, also known as the Zilber–Pink conjectures.

In a series of papers by Masser and Zannier [2010; 2012; 2014; 2015], the authors 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 nonsimple case. On the other hand, Pink’s conjecture concerns families of semiabelian varieties. However, Bertrand [2011] found a counterexample to this, for a suitable nonsplit 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 [Bertrand et al. 2016], 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 [2013].

Let $S$ be an irreducible and nonsingular quasiprojective 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 $G \times_S G$ under the addition morphism and the image of the zero section $S \to \mathcal{A}$, and is mapped to itself by the inversion morphism. 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 [Hartshorne 1977, Chapter III, Proposition 9.7]).

**Theorem 2.1.** Let $\mathcal{A}$ be as above and let $\mathcal{A}^{(2)}$ be the union of the flat subgroup schemes of $\mathcal{A}$ with codimension at least 2. Let $C$ be a curve in $\mathcal{A}$ defined over $\overline{\mathbb{Q}}$ and suppose $\pi(C)$ dominates $S$. Then $C \cap \mathcal{A}^{(2)}$ 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 [Habegger 2013].

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

$$a(P_1, \ldots, P_n) = a_1P_1 + \cdots + a_nP_n.$$ 

We identify the elements of $\mathbb{Z}^n$ with the morphisms they define. The fibered product $a_1 \times_S \cdots \times_S a_r$, for $a_1, \ldots, a_r \in \mathbb{Z}^n$, defines a morphism $A \to B$ over $S$ where $B$ is the $r$-fold fibered power of $E$. The kernel of $a$, denoted by $\ker a$, indicates the fibered product of $a : A \to B$ with the zero section $S \to B$. We consider it as a closed subscheme of $A$.

**Lemma 2.2.** Let $G$ be a codimension-$r$ flat subgroup scheme of $A$ with $1 \leq r \leq n$. Then there exist independent $a_1, \ldots, a_r \in \mathbb{Z}^n$ such that $G \subseteq \ker(a_1 \times_S \cdots \times_S a_r)$. Moreover, $\ker(a_1 \times_S \cdots \times_S a_r)$ is a flat subgroup scheme of $A$ of codimension $r$.

**Proof.** This follows from Lemma 2.5 of [Habegger 2013] and its proof. \qed

Consider the Legendre family defined by (1-1). This gives an example of an elliptic scheme, which we call $E_L$, over the modular curve $Y(2) = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. We write $A_L$ for the $n$-fold fibered power of $E_L$.

**Lemma 2.3** [Habegger 2013, Lemma 5.4]. Let $A$ be as above. After possibly replacing $S$ by a Zariski open, nonempty subset, there exists an irreducible, nonsingular, quasiprojective curve $S'$ defined over $\overline{\mathbb{Q}}$ such that we have a commutative diagram

$$
\begin{array}{ccc}
A & \xleftarrow{f} & A' \\
\pi \downarrow & & \downarrow e \\
S & \xleftarrow{l} & S' \\
\end{array}
\quad
\begin{array}{ccc}
& & \quad \pi_L \\
& & S' \xrightarrow{\lambda} Y(2)
\end{array}
$$

where $l$ is finite, $\lambda$ is quasifinite, $A'$ is the abelian scheme $A \times_S S'$, $f$ is finite and flat and $e$ is quasifinite and flat. Moreover, the restriction of $f$ and $e$ to any fiber of $A' \to S'$ is an isomorphism of abelian varieties.

**Lemma 2.4.** If $G$ is a flat subgroup scheme of $A$, then $e(f^{-1}(G))$ is a flat subgroup scheme of $A_L$ of the same dimension. Moreover, let $X$ be a subvariety of $A$ dominating $S$ and not contained in a proper flat subgroup scheme of $A$, let $X''$ be an irreducible component of $f^{-1}(X)$ and let $X'$ be the Zariski closure of $e(X'')$ in $A_L$. Then $X'$ has the same dimension as $X$, dominates $Y(2)$ and is not contained in a proper flat subgroup scheme of $A_L$.

**Proof.** This follows from the proof of Lemma 5.5 of [Habegger 2013]. \qed
Proof of Theorem 2.1. First, we can assume that \(C\) is not contained in a flat subgroup scheme of \(A\) of positive codimension. Therefore, it is enough to prove that \(C \cap \bigcup \mathcal{G}\) is finite where the union is taken over all flat subgroup schemes of \(A\) of codimension at least 2.

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

Now, since \(e\) is quasifinite, if \(e(f^{-1}(C \cap A^{[2]}))\) is finite then \(C \cap A^{[2]}\) is finite and by Lemma 2.4 we have
\[
e(f^{-1}(C \cap A^{[2]})) \subseteq e(f^{-1}(C)) \cap A_L^{[2]}.
\]
Therefore, we can reduce to proving our claim for the Legendre family and for \(C'\).

By Lemma 2.2, each flat subgroup scheme of codimension at least 2 of \(A_L\) is contained in \(\ker(a_1 \times Y(2) a_2)\) for some independent \(a_1, a_2 \in \mathbb{Z}^n\). Therefore, it is enough to show that \(C' \cap \bigcup \ker(a_1 \times Y(2) a_2)\) is finite, where the union is taken over all pairs of independent \(a_1, a_2 \in \mathbb{Z}^n\). The claim follows by applying Theorem 1.1 since \(C'\) is not contained in a proper flat subgroup scheme. \(\blacksquare\)

3. O-minimal structures and a result of Pila

In this section we introduce the notion of an o-minimal structure, recall some definitions and properties we will need later and state a result from [Pila 2011]. For the basic properties of o-minimal structures we refer to [van den Dries 1998] and [van den Dries and Miller 1996].

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

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

If \(S\) is a structure and, in addition,

5. \(S_1\) consists of all finite union of open intervals and points,

then \(S\) is called an *o-minimal structure*.

Given a structure \(S\), we say that \(S \subseteq \mathbb{R}^N\) is a *definable* set if \(S \in S_N\).

Let \(U \subseteq \mathbb{R}^{N+M}\) and let \(\pi_1\) and \(\pi_2\) be the projection maps on the first \(N\) and on the last \(M\) coordinates, respectively. Now, for \(t_0 \in \pi_2(U)\), we define \(U_{t_0} = \{x \in \mathbb{R}^N : (x, t_0) \in U\} = \pi_1(\pi_2^{-1}(t_0))\) 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 let $f : S \to \mathbb{R}^M$ 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 [van den Dries and Miller 1996]. In this article we are interested in the structure of globally subanalytic sets, usually denoted by $\mathbb{R}_{\text{an}}$. We will not dwell 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 $\mathbb{R}_{\text{an}}$.

We now fix an o-minimal structure $S$. Many important properties of o-minimal structures follow from the cell decomposition theorem [van den Dries and Miller 1996, 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** [van den Dries and Miller 1996, 4.4]. Let $U$ be a definable family. There exists a positive integer $\gamma$ such that each fiber of $U$ has at most $\gamma$ connected components.

Now, let $S \subseteq \mathbb{R}^N$ be a nonempty definable set and let $e$ be a nonnegative integer. The set of regular points of dimension $e$, denoted by $\text{reg}_e(S)$, is the set of points $x \in S$ such that there is an open neighborhood $I$ of $x$ for which $S \cap I$ is 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 $S \setminus \text{reg}_e(S)$ has dimension $\leq e - 1$.

**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 nonempty fibers are all definable blocks.

We now need to define the height of a rational point. The height used in [Pila 2011] 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

$$Z(\mathbb{Q}, T) = \{(\alpha_1, \ldots, \alpha_N) \in Z \cap \mathbb{Q}^N : H(\alpha_1, \ldots, \alpha_N) \leq T\}. \quad (3-1)$$

The following theorem is a special case of [Pila 2011, Theorem 3.6] (see also [Pila 2009]). 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 $\gamma$, depending on $Z$ and $\epsilon$, such that $f(T) \leq \gamma g(T)$ for $T$ large enough.
Theorem 3.4 [Pila 2011]. Let \( Z \subseteq \mathbb{R}^N \times \mathbb{R}^M \) be a definable family, and let \( \epsilon > 0 \). Then there exist a \( J = J(Z, \epsilon) \in \mathbb{N} \) and a collection of definable block families \( B^{(j)}(Z, \epsilon) \subseteq \mathbb{R}^N \times (\mathbb{R}^M \times \mathbb{R}^M)^j \), for \( j = 1, \ldots, J \), such that

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

4. Points lying on rational linear varieties

Let \( n \geq 2 \) 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

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

and that \( f(\lambda) \) 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

\[
\begin{align*}
    a_1 \ell_1(\lambda) + \cdots + a_n \ell_n(\lambda) &= a_{n+1} f(\lambda) + a_{n+2} g(\lambda), \\
    b_1 \ell_1(\lambda) + \cdots + b_n \ell_n(\lambda) &= b_{n+1} f(\lambda) + b_{n+2} g(\lambda),
\end{align*}
\]

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 \( \epsilon > 0 \), we have \( |D(T)| \ll \epsilon T^\epsilon \).

Define

\[ \Delta = f \bar{g} - \bar{f} g, \]

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

\[ u_j = \frac{\ell_j \bar{g} - \bar{\ell}_j g}{\Delta}, \quad v_j = -\frac{\ell_j \bar{f} - \bar{\ell}_j f}{\Delta}. \]

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

\[ \Theta : D \to \mathbb{R}^{2n}, \quad \lambda \mapsto (u_1(\lambda), v_1(\lambda), \ldots, u_n(\lambda), v_n(\lambda)), \]
and set \( S = \Theta(D) \). This is a definable set in \( \mathbb{R}^\text{an} \). 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

\[
\begin{align*}
    a_1 u_1 + \cdots + a_n u_n &= a_{n+1}, \\
    a_1 v_1 + \cdots + a_n v_n &= a_{n+2}, \\
    b_1 u_1 + \cdots + b_n u_n &= b_{n+1}, \\
    b_1 v_1 + \cdots + b_n v_n &= b_{n+2}.
\end{align*}
\]

(4-3)

**Lemma 4.2.** For every choice of \( a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2} \in \mathbb{R} \), 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. We can suppose that at least one \( a_j \) is nonzero. This would imply that there exists an infinite set \( E \subseteq D \) on which, 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 all of \( D \) (see [Lang 1985, Chapter III, Theorem 1.2(ii)]), contradicting hypothesis (4-1). \( \Box \)

The following proposition is the main tool used 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 \( W \subseteq \mathbb{R}^{4n+4} \) defined as

\[
W = \{ (u_1, v_1, \ldots, u_n, v_n, a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2}) \in S \times \mathbb{R}^{2n+4} : (4-3) \text{ holds and } (a_1, \ldots, a_{n+2}), (b_1, \ldots, b_{n+2}) \text{ are linearly independent} \},
\]

which is a definable set. Denote by \( \pi_1 \) the projection on \( S \) and by \( \pi_2 \) 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., \( \tau(L) = \pi_1(\pi_2^{-1}(L)) \). In other words, if we consider \( W \) as a family of subsets of \( \mathbb{R}^{2n} \), then \( \tau(L) \) is just the fiber \( W_L \). This is a definable subset of \( S \) and it must be zero-dimensional by Lemma 4.2. By Proposition 3.2, there exists a positive integer \( \gamma \) such that \( |\tau(L)| \leq \gamma \), for every \( L \in \pi_2(W) \). If \( V \subseteq \pi_2(W) \), we write \( \tau(V) \) for \( \pi_1(\pi_2^{-1}(V)) \).

Now, let us set \( \hat{W} = \pi_2(W) \subseteq \mathbb{R}^{2n+4} \). Recall the definition in (3-1) and note that \( S(T) \subseteq \tau(\hat{W}(\mathbb{Q}, T)) \). By Theorem 3.4, there is a finite number of definable
block families such that, for every $\epsilon_1$, the set $\hat{W}(\mathbb{Q}, T)$ 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 $U_t \subseteq \hat{W}$. We claim that, for every $\epsilon_2$, 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 prove this, the claim of the proposition follows easily after fixing $\epsilon_1$ and $\epsilon_2$ 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 $\eta$ and define, for $m = 1, \ldots, \gamma_1$,

$$V^{(m)} = \{(L, t) \in U : \text{there exist an } \eta > 0 \text{ and } A_1, \ldots, A_m \in S \text{ such that, for all } L' \in B_{\eta}(L) \cap U_t, \text{ we have } \tau(L') = \{A_1, \ldots, A_m\}\}.$$ 

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 a $\gamma_2$ such that all fibers $V_t$ have at most $\gamma_2$ 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 $\gamma_1$ 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 $Z_t$. We fix a ball $B_{\eta}(L)$ such that $B_{\eta}(L) \cap U_t$ is connected and contained in $Z_t$. We set $\{A_1, \ldots, A_m\}$ equal to $\bigcap_{L' \in B_{\eta}(L) \cap Z_t} \tau(L')$, i.e., the set of points of $S$ that lie on all subspaces in $B_{\eta}(L) \cap Z_t$. By definition of $Z$, we know $\tau^{-1}(\{A_1, \ldots, A_m\}) \cap B_{\eta}(L) \cap Z_t$ must be of dimension $< e$; therefore, there exist an $L_0 \in B_{\eta}(L) \cap Z_t$ and an $\eta_0$ such that, for every $L' \in B_{\eta}(L_0) \cap Z_t$, we have $\tau(L') \supseteq \{A_1, \ldots, A_m\}$. Thus, we can define a function $f : B_{\eta_0}(L_0) \cap Z_t \to S$ that associates to $L'$ a point in $\tau(L')$ different from $A_1, \ldots, A_m$. This is a definable function and, taking $\eta_0$ small enough (and possibly choosing a different $L_0$), we can also suppose that it is differentiable [van den Dries and Miller 1996, 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 nonzero 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 an $L_0 \in B_{\eta}(L) \cap Z_t$ and an $\eta_0$ such that $f$ is differentiable on $B_{\eta_0}(L_0) \cap Z_t$ and has nonzero 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, $B_{n0}(L_0) \cap U_t = B_{n0}(L_0) \cap Z_t$ is semialgebraic. Thus, if we intersect it with a suitable linear variety, we get an algebraic curve segment $C$ in $B_{n0}(L_0) \cap Z_t$, passing through $L_0$ in the direction for which the derivative of $f$ is nonzero. The function $f$ is nonconstant on $C$. Consider $C' = f(C) \times C$. By definition of $f$, we know $C'$ is a real-analytic curve segment in $W$. Moreover, let us define $D' = \Theta^{-1}(f(C))$. As $f$ is not constant on $C$, we know $D'$ 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

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

Each of these two relations is independent of the previous $2n + 3$ relations, and they are independent of each other because $(a_1, \ldots, a_{n+2})$ and $(b_1, \ldots, b_{n+2})$ are required 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 $F := \mathbb{C}(f, g)$,

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

This contradicts 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 $\epsilon_3$ and for each fiber $Z_t$, the set $Z_t(\mathbb{Q}, T)$ 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 $\epsilon_4 > 0$, we have $|\tau(U'_t) \cap S(T)| \ll_{U', \epsilon_3} T^{\epsilon_4}$ 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 have $U_t = V_t \cup Z_t$ and that $V_t$ gives rise to at most $\gamma_1 \gamma_2$ points of $S(T)$. This proves our claim and the proposition. □

**Remark.** We would like to point out that this last proposition can be deduced from recent work of Habegger and Pila [2014, Corollary 7.2].

**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 $\gamma_3$ independent of $T$. Now, using Proposition 3.2 and Lemma 4.2, we see that there exists a $\gamma_4$ such that, for
any choice of $a_1, \ldots, a_{n+2}, b_1, \ldots, b_{n+2}$, there are at most $\gamma_4$ elements $\lambda$ 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.

\section{Periods and elliptic logarithms}

In this section we introduce the functions to which we will apply Proposition 4.1. We follow [Masser and Zannier 2012].

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

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

and let

$$f(t) = \pi F(t) \quad \text{and} \quad g(t) = \pi i F(1 - t). \quad (5-1)$$

Define

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

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

By [Husemöller 1987, Chapter 9, (6.1) Theorem, p. 179], $f(\lambda)$ and $g(\lambda)$ are basis elements of the period lattice $L_\lambda$ of $E_\lambda$ with respect to $dX/(2Y)$. 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 $E_\lambda$. Let $P_j = (x_j, y_j)$, where $x_j, y_j$ are coordinate functions in $\mathbb{C}(\mathbb{C})$. We can suppose, for every $j$, that $x_j \neq 0, 1, \lambda$ 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 $z_j(c)$ such that $\exp_{\lambda(c)}(z_j(c)) = P_j(c)$; in other words, we want $z_j$ to be the elliptic logarithm of $P_j$.

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

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

We now follow the construction of [Masser and Zannier 2012, p. 459]. Fix a point $c_\ast \in \hat{C}$ and choose a path in the $x_j$-plane from $x_j(c_\ast)$ to $\infty$ and not passing through 0, 1 and $\lambda(c_\ast)$. We also fix a determination of $Y = \sqrt{X(X-1)(X-\lambda(c_\ast))}$ that is equal to $y_j(c_\ast)$ at $X = x_j(c_\ast)$. Therefore, the path corresponds to a path on
the elliptic curve $E_{\lambda(c)}$ from the point $P_j(c)$ to the origin $O$. Hence we can define $z_j(c)$ as the integral

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

We can extend it to a $c$ close to $c_\ast$ by

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

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 $\lambda(c)$. For the second term, we can take any local path from $x_j(c_\ast)$ to $x_j(c)$. We can extend the integrand as a double power series in $\lambda(c) - \lambda(c_\ast)$ and in $X - x_j(c_\ast)$; the result will be a double power series in $\lambda(c) - \lambda(c_\ast)$ and $x_j(c) - x_j(c_\ast)$. Notice that we have, at any rate, $\exp_{\lambda(c)}(z_j(c)) = P_j(c)$ for every $j = 1, \ldots, n$.

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

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 $N_\ast$.

**Proof.** The functions $z_1, \ldots, z_n, f, g$ are analytic functions of $\lambda$, linearly independent over $\mathbb{C}$. Indeed, a relation $a_1z_1 + \cdots + a_nz_n = a_{n+1}f + a_{n+2}g$, with integer coefficients, would map via $\exp_{\lambda}$ to a relation of the form (1-2) on $N_\ast$, and therefore on all of $\hat{C}$, which cannot hold by the hypothesis of the theorem. Moreover, if $\wp_\lambda$ is the Weierstrass $\wp$-function associated to $L_\lambda$, the $\wp_\lambda(z_j)$ are algebraic functions of $\lambda$ because $\wp_\lambda(z_j) = x_j - \frac{1}{2}(\lambda + 1)$ (see [Masser and Zannier 2010, (3.8), p. 1683]). Therefore, the hypotheses of [Bertrand 1990, Théorème 5, p. 136] 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 $\hat{C}$.

If $c \in \hat{C}$, one can continue $f$ and $g$ to a neighborhood $N_c$ of $c$. In fact, if we choose $c \in \hat{C}$ and a path from $c_\ast$ to $c$ lying in $\hat{C}$, we can easily continue $f$ and $g$ along the path using (5-1).

To continue $z_j$ from a point $c_\ast$ to a $c$ in $\hat{C}$, it is sufficient to verify that if $N_1$ and $N_2$ are two open small subsets in $\hat{C}$, with $N_1 \cap N_2$ connected, and if $z_j$ has analytic definitions $z_j'$ on $N_1$ and $z_j''$ on $N_2$, then $z_j$ 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 clear that we can continue the function \((f, g, z_1, \ldots, z_n)\) from a small neighborhood of \( c_\ast \) to a small neighborhood \( N_c \subseteq \hat{\mathcal{C}} \) of \( c \), and that the obtained function \((f^c, g^c, z_1^c, \ldots, z_n^c)\) is analytic on \( N_c \). Moreover, the functions preserve algebraic independence, as the following lemma shows.

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

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

Furthermore, the lattice \( L_\lambda \) is still generated by \( f^c \) and \( g^c \) on \( N_c \); see Lemma 6.1 of [Masser and Zannier 2012] or Lemma 4.1 of [Masser and Zannier 2010].

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

### 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 is defined by

\[
h(\alpha_1, \ldots, \alpha_N) = \frac{1}{[\overline{\mathbb{Q}}(\alpha_1, \ldots, \alpha_N) : \mathbb{Q}]} \sum \log \max \{1, |\alpha_1|^v, \ldots, |\alpha_N|^v\},
\]

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

Let \( \alpha \) be an algebraic number and consider the Legendre curve \( E = E_\alpha \) defined by the equation \( Y^2 = X(X - 1)(X - \alpha) \). 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 \( \hat{h} \) at most \( q \) (for the definition of Néron–Tate height, see for example [Masser 1988, p. 255]). In case the \( P_1, \ldots, P_n \) are all torsion, i.e., \( \hat{h}(P_j) = 0 \) for all \( j \), we set \( q = 1 \). We define

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

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 \( |a| = \max(|a_1|, \ldots, |a_n|) \).

**Lemma 6.1.** Under the above hypotheses, there are generators \( a_1, \ldots, a_r \) of \( L(P_1, \ldots, P_n) \) with

\[
|a_i| \leq \gamma_1 \kappa^{\gamma_2} (h(\alpha) + 1)^{2n} \kappa^{\frac{1}{2}(n-1)},
\]

for some positive constants \( \gamma_1, \gamma_2 \) depending only on \( n \).
Proof. The Weierstrass form $\tilde{E} = \tilde{E}_\alpha$ of $E = E_\alpha$ has equation

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

where $g_2 = \frac{4}{3}(\alpha^2 - \alpha + 1)$ and $g_3 = \frac{4}{27}(\alpha - 2)(\alpha + 1)(2\alpha - 1)$ (see [Masser and Zannier 2010, (3.7), p. 1683]). The isomorphism $\phi$ from $E$ to $\tilde{E}$ is given by

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

Now, $\tilde{E}$ 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 $\tilde{E}$ and vice versa. Moreover, the $Q_i = \phi(P_i)$ will have coordinates in $K$ and the same Néron–Tate height of the $P_i$, and hence $\hat{h}(Q_i) \leq q$.

First, suppose that at least one of the points has infinite order. By Theorem E of [Masser 1988], if $Q_1, \ldots, Q_n$ are linearly dependent points on $\tilde{E}(K)$ 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

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

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

For the first we use Théorème 1.2(i) of [David 1997]: choosing any archimedean $v$ and noting that, by David’s definition, $h_v(\tilde{E}) \geq \sqrt{3}^2$, one has

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

where $h = \max\{1, h(j_{\tilde{E}})\}$. Now, $j_{\tilde{E}} = 2^8(\alpha^2 - \alpha + 1)^3/(\alpha^2(\alpha - 1)^2)$ (see for instance [Husemoller 1987], p. 83). Therefore, $h \leq \gamma_4(h(\alpha) + 1)$ and

$$\omega \leq \gamma_5(h(\alpha) + 1)^2.$$  \hspace{1cm} (6-1)

For the lower bound on $\eta$, we use a result of Masser [1989a, Corollary 1]. In Masser’s bound a constant depending on $\kappa$ appears in the denominator. However, going through the proof one can see that this constant is polynomial in $\kappa$, as noted on [David 1997, p. 109]. Therefore,

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

where $w = \max\{1, h(g_2), h(g_3)\}$. As $g_2$ and $g_3$ are polynomials in $\alpha$, we have $w \leq \gamma_9(h(\alpha) + 1)$. 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 $\gamma_1$, $\gamma_2$ depending only on $n$. 
If all the points are torsion points, it is clear that one can take $|a_i| \leq \omega$ and use (6-1).

7. Bounded height

In this section we see that the height of the points on the curve $C$ 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 $C$ is defined. Suppose also that the finitely many points we excluded from $C$ to get $\hat{C}$, 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 $C'$ be the set of points of $\hat{C}$ such that $P_1, \ldots, P_n$ satisfy two independent relations on the specialized curve and let $c_0 \in C'$. Since $C$ is defined over $\mathbb{Q}$, the $x_j(c_0)$ and $\lambda(c_0)$ must be algebraic, unless the $P_j$ are identically linearly dependent, which we excluded by hypothesis. Then by Silverman’s specialization theorem [1983] (see also of [Zannier 2012, Appendix C]) there exists a $\gamma_1 > 0$ such that

$$h(\lambda(c_0)) \leq \gamma_1.$$ (7-1)

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

$$\Lambda_\delta = \{t \in \mathbb{C} : |t| \leq 1/\delta, |t - \lambda(c)| \geq \delta \text{ for all } c \in \mathbb{C} \setminus \hat{C} \}.$$

**Lemma 7.1.** There is a positive $\delta$ such that there are at least $\frac{1}{2}[k(\lambda(c_0)) : k]$ different $k$-embeddings $\sigma$ of $k(\lambda(c_0))$ in $\mathbb{C}$ such that $\sigma(\lambda(c_0))$ lies in $\Lambda_\delta$ for all $c_0 \in C'$.

**Proof.** See Lemma 8.2 of [Masser and Zannier 2012].

**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 [2004], 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 $\gamma_2, \gamma_3$ such that, for every $c_0 \in C'$ and every $j = 1, \ldots, n$, we have

$$\hat{h}(P_j(c_0)) \leq \gamma_2,$$

and the $P_j(c_0)$ are defined over some number field $K \supseteq k(\lambda(c_0))$ with

$$[K : \mathbb{Q}] \leq \gamma_3[k(\lambda(c_0)) : k].$$

**Proof.** Recall that each $x_j(c_0)$ is a root of $f_j(X, \lambda(c_0))$. This already implies the second statement. Now, we have $h(P_j(c_0)) \leq \gamma_4(h(\lambda(c_0)) + 1)$ and, using the work of Zimmer [1976], we have $\hat{h}(P_j(c_0)) \leq h(P_j(c_0)) + \gamma_5(h(\lambda(c_0)) + 1)$. The first claim now follows from (7-1).
We want to show that there are at most finitely many \( c \) on the curve such that \( P_1(c), \ldots, P_n(c) \) satisfy two linearly independent relations on \( E_\lambda(c) \). By Northcott’s theorem [1949] and (7-1), we only need to bound the degree \( d \) of \( \lambda(c) \) over \( k \).

Let \( c_0 \in \mathcal{C}', \lambda_0 = \lambda(c_0) \) and \( d_0 = [k(\lambda(c_0)) : k] \). First, by Lemma 7.1, we can choose \( \delta \) independent of \( c_0 \), such that \( \lambda_0 \) has at least \( d_0/2 \) conjugates in \( \Lambda_\delta \). Now, since \( \Lambda_\delta \) is compact, it can be covered by \( \gamma_2 \) closed discs \( D_{c_1}, \ldots, D_{c_{\gamma_2}} \subseteq \lambda(\mathcal{C}) \), where \( D_{c_i} \) is centered in \( \lambda(c_i) \), for some \( c_i \in \mathcal{C} \).

We can suppose that the closed disc \( D_{c_1} \) contains at least \( d_0/(2\gamma_2) \) conjugates \( \lambda_0^\sigma \). Now, each such conjugate comes from a \( c_0^\sigma \in \mathcal{N}_{c_1} \) and the corresponding points \( P_1(c_0^\sigma), \ldots, P_n(c_0^\sigma) \) satisfy the same linear relations. So there are linearly independent \((a_1, \ldots, a_n), (b_1, \ldots, b_n)\) such that

\[
a_1 P_1(c_0^\sigma) + \cdots + a_n P_n(c_0^\sigma) = b_1 P_1(c_0^\sigma) + \cdots + b_n P_n(c_0^\sigma) = 0 \quad (8-1)
\]
on \( E_\lambda(c_0^\sigma) \).

By Lemma 7.2, \( \hat{h}(P_1(c_0^\sigma)) \) is at most \( \gamma_3 \) and the points are defined over some finite extension of \( k(\lambda(c_0^\sigma)) \) 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 \( \lambda(\mathcal{N}_{c_i}) \supseteq D_{c_i} \), we defined \( f^{\sigma_1}, g^{\sigma_1} \) to be generators of the period lattice \( L_\lambda \) and the elliptic logarithms \( z_1^{\sigma_1}, \ldots, z_n^{\sigma_1} \) such that

\[
\exp_\lambda(z_j^{\sigma_1}(\lambda)) = P_j(\lambda) \quad (8-2)
\]
on \( \lambda(\mathcal{N}_{c_i}) \). We know that \( z_1^{\sigma_1}, \ldots, z_n^{\sigma_1}, f^{\sigma_1}, g^{\sigma_1} \) are holomorphic functions on a neighborhood of \( D_{c_i} \), with \( f^{\sigma_1}(\lambda) \) and \( g^{\sigma_1}(\lambda) \) linearly independent over \( \mathbb{R} \) for every \( \lambda \in D_{c_i} \), and, by Lemma 5.2, that \( z_1^{\sigma_1}, \ldots, z_n^{\sigma_1} \) are algebraically independent over \( \mathbb{C}(f^{\sigma_1}, g^{\sigma_1}) \) on \( D_{c_i} \). Therefore, the hypotheses of Proposition 4.1 are satisfied.

By (8-1) and (8-2), we have

\[
a_1 z_1^{\sigma_1}(\lambda_0^\sigma) + \cdots + a_n z_n^{\sigma_1}(\lambda_0^\sigma) \equiv b_1 z_1^{\sigma_1}(\lambda_0^\sigma) + \cdots + b_n z_n^{\sigma_1}(\lambda_0^\sigma) \equiv 0 \quad (mod L_{\lambda_0^\sigma}).
\]

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

\[
\begin{align*}
& \{a_1 z_1^{\sigma_1}(\lambda_0^\sigma) + \cdots + a_n z_n^{\sigma_1}(\lambda_0^\sigma) = a_{n+1} f^{\sigma_1}(\lambda_0^\sigma) + a_{n+2} g^{\sigma_1}(\lambda_0^\sigma), \\
& b_1 z_1^{\sigma_1}(\lambda_0^\sigma) + \cdots + b_n z_n^{\sigma_1}(\lambda_0^\sigma) = b_{n+1} f^{\sigma_1}(\lambda_0^\sigma) + b_{n+2} g^{\sigma_1}(\lambda_0^\sigma) \}
\end{align*}
\]

Thus all \( \lambda_0^\sigma \in D_{c_i} \) are in \( D_{c_i}(\gamma_5 d_0^{\gamma_6}) \) (recall the definition of \( D(T) \) just above Proposition 4.1).

By Proposition 4.1, we have \(|D_{c_i}(\gamma_5 d_0^{\gamma_6})| \ll_{\epsilon} d_0^{\gamma_6} \). But by our choice of \( D_{c_i} \), we have at least \( d_0/(2\gamma_2) \) points in \( D_{c_i}(\gamma_5 d_0^{\gamma_6}) \). Therefore, if we choose \( \epsilon < 1/\gamma_6 \) we have a contradiction when \( d_0 \) 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 $\lambda(c_0)$, which proves Theorem 1.1.

Acknowledgments

The authors would like to thank Umberto Zannier for his support, Daniel Bertrand, Philipp Habegger, Lars Kühne, Vincenzo Mantova and Harry Schmidt for useful discussions and the referee for very helpful comments that improved this article.

References

Linear relations in families of powers of elliptic curves 213


Communicated by Jonathan Pila
Received 2015-01-29 Revised 2015-10-01 Accepted 2015-11-27

fbarroero@gmail.com Classe di Scienze, Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126 Pisa, Italy

laura.capuano1987@gmail.com Classe di Scienze, Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126 Pisa, Italy
### Table of Contents

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stable sets of primes in number fields</td>
<td>1</td>
</tr>
<tr>
<td>ALEXANDER IVANOV</td>
<td></td>
</tr>
<tr>
<td>Hopf–Galois structures arising from groups with unique subgroup of order $p$</td>
<td>37</td>
</tr>
<tr>
<td>TIMOTHY KOHL</td>
<td></td>
</tr>
<tr>
<td>On tensor factorizations of Hopf algebras</td>
<td>61</td>
</tr>
<tr>
<td>MARC KEILBERG and PETER SCHAUENBURG</td>
<td></td>
</tr>
<tr>
<td>Extension theorems for reductive group schemes</td>
<td>89</td>
</tr>
<tr>
<td>ADRIAN VASIU</td>
<td></td>
</tr>
<tr>
<td>Actions of some pointed Hopf algebras on path algebras of quivers</td>
<td>117</td>
</tr>
<tr>
<td>RYAN KINSER and CHELSEA WALTON</td>
<td></td>
</tr>
<tr>
<td>On the image of the Galois representation associated to a non-CM Hida family</td>
<td>155</td>
</tr>
<tr>
<td>JACLYN LANG</td>
<td></td>
</tr>
<tr>
<td>Linear relations in families of powers of elliptic curves</td>
<td>195</td>
</tr>
<tr>
<td>FABRIZIO BARROERO and LAURA CAPUANO</td>
<td></td>
</tr>
</tbody>
</table>