Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)
Vol. XII (2013), 687-715

Torsion points on elliptic curves in Weierstrass form

PHILIPP HABEGGER

Abstract. We prove that there are only finitely many complex numbers a and b with $4a^3 + 27b^2 \neq 0$ such that the three points $(1, *)$, $(2, *)$, and $(3, *)$ are simultaneously torsion points on the elliptic curve defined in Weierstrass form by $y^2 = x^3 + ax + b$. This gives an affirmative answer to a question raised by Masser and Zannier. We thus confirm a special case in two dimensions of the relative Manin-Mumford Conjecture formulated by Pink and Masser-Zannier.

Mathematics Subject Classification (2010): 14H52 (primary); 14G40, 11G05, 11U09 (secondary).

1. Main Result

In pursuit of unlikely intersections, Masser and Zannier [10, 11] proved that there are only finitely many complex $\lambda \neq 0, 1$ such that

$$\left(2, \sqrt{2(2-\lambda)}\right) \quad \text{and} \quad \left(3, \sqrt{6(3-\lambda)}\right) \tag{1.1}$$

are torsion points on the elliptic curve given in Legendre form by $y^2 = x(x-1)(x-\lambda)$.

This result provides evidence for far-reaching conjectures stated by its authors [9, 11] and by Pink [14]. Both conjectures govern the distribution of torsion points on a subvariety of a family of semi-Abelian varieties and may be regarded as a relative version of the Manin-Mumford Conjecture. They deal with unlikely or anomalous intersections emphasized in the earlier work of Zilber [22] for constant semi-Abelian varieties. In Masser and Zannier's result the subvariety is an algebraic curve inside the fibered square of the Legendre family of elliptic curves. By a recent example of Bertrand [3], these conjectures require modification when dealing with families whose fibers are not complete. However, in the current paper we will consider only families of Abelian varieties.

One natural family is the Weierstrass family. The Weierstrass equation $y^2 = x^3 + ax + b$ defines an elliptic curve when a and b are complex parameters that

Received May 5, 2011; accepted in revised form November 22, 2011.

satisfy the inequality $4a^3 + 27b^2 \neq 0$ which rules out singularities. We thus obtain a family of elliptic curves parametrized by a and b. Masser and Zannier [11] asked if a similar finiteness statement as above holds in this context. Because there are two parameters, the conjectures suggest imposing a torsion condition on a third point to expect finiteness.

Our main result gives a positive answer to Masser and Zannier's question and provides the first evidence supporting a relative Manin-Mumford Conjecture over a base of dimension greater than one.

Theorem 1.1. *There are only finitely many complex pairs (a, b) with $4a^3+27b^2 \neq 0$ such that*

$$\left(1, \sqrt{1+a+b}\right), \quad \left(2, \sqrt{8+2a+b}\right), \quad \text{and} \quad \left(3, \sqrt{27+3a+b}\right)$$

are torsion points on the elliptic curve given in Weierstrass form $y^2 = x^3 + ax + b$.

Although the methods we present are as a whole confined to a specific example, some intermediate steps hold in greater generality. It is therefore convenient to work in a more general language. When not stated otherwise, a variety is defined over $\mathbf{C}$. We also identify a variety with the set of its complex points. If a variety X is defined over a field K it is sometimes still useful to write $X(K)$ for the K-rational points on X.

We proceed by reformulating our main result. Let S be the affine algebraic surface

$$\{(a, b) \in \mathbf{A}^2;\ 4a^3 + 27b^2 \neq 0\}; \tag{1.2}$$

it is defined over $\overline{\mathbf{Q}}$, the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. The Weierstrass family of elliptic curves

$$\mathcal{E} = \left\{([x : y : z], (a, b)) \in \mathbf{P}^2 \times S;\ y^2z = x^3 + axz^2 + bz^3\right\}$$

is an Abelian scheme over the two-dimensional base S. Let $\mathcal{E}^3$ be the three-fold fibered power of $\mathcal{E}$ over S and $\pi : \mathcal{E}^3 \to S$ by the structure morphism. We obtain an Abelian scheme over S. A complex point of an Abelian scheme that is torsion in its respective fiber will be called a torsion point.

In this language, our result states that all torsion points on a certain, explicitly given, algebraic surface $X \subset \mathcal{E}^3$ are contained in finitely many fibers of $\mathcal{E}^3 \to S$. This surface, we call it the 123-surface, is the Zariski closure of the affine subset of $\mathcal{E}^3$ where the first coordinate in each copy of $\mathcal{E}$ is fixed to be $1, 2$, and 3, respectively. The restriction of $\mathcal{E}^3 \to S$ to X has finite fibers, so our main result is equivalent to the statement that X contains only finitely many torsion points.

The general conjecture stated by Masser and Zannier [11] in the case of families of Abelian varieties expects the torsion points on our surface to lie on finitely many proper subgroup schemes of $\mathcal{E}^3$. If true, it could at best imply that torsion points do not lie Zariski dense on X. Our Theorem 1.1 however, is unconditional.

Moreover, our finiteness statement is stronger than the conjecture's conclusion. This feature is due to the specific nature of our surface.

Let us consider for the moment a variation of the 123-surface. We claim that there are infinitely many complex $(a, b) \in S$ such that

$$\left(0, \sqrt{b}\right), \quad \left(1, \sqrt{1+a+b}\right), \quad \text{and} \quad \left(-1, \sqrt{-1-a+b}\right) \tag{1.3}$$

are torsion points on the elliptic curve $y^2 = x^3 + ax + b$. Indeed, we find them on $b = 0$. The first point is automatically torsion of order 2. We observe that $y^2 = x^3 + ax$ yields an elliptic curve with complex multiplication and j-invariant 1728. It follows from basic facts on elliptic curves that there are infinitely many $a \in \mathbf{C} \setminus \{0\}$ such that $\left(1, \sqrt{1+a}\right)$ is torsion on $y^2 = x^3 + ax$; we shall prove a related statement in Lemma 3.9. We fix such an a. Then $\left(-1, \sqrt{-1-a}\right)$ is the image of $\left(1, \sqrt{1+a}\right)$ under an automorphism of order 4 of $y^2 = x^3 + ax$. So all three points in (1.3) are torsion. Using a specialization argument one can show that the algebraic surface in $\mathcal{E}^3$ induced by (1.3) is not in a proper subgroup scheme of $\mathcal{E}^3$. Conjecturally, it does not contain a Zariski dense set of torsion points.

Let us briefly recap the proof of Theorem 1.1. It splits up into two parts. In the first half, laid out in Section 2, we work in the Legendre family of elliptic curves

$$\mathcal{E}_L = \left\{([x : y : z], \lambda) \in \mathbf{P}^2 \times Y(2); \;\; y^2 z = x(x-z)(x-\lambda z)\right\}$$

where $Y(2) = \mathbf{P}^1 \setminus \{0, 1, \infty\}$. The three-fold fibered power of $\mathcal{E}_L \to Y(2)$ is denoted by $\mathcal{E}_L^3$. Working in the Legendre family has the advantage that the base is one dimensional.

Any elliptic curve over $\mathbf{C}$ is isomorphic to an elliptic curve in Legendre form. Using a base change argument we can construct a new algebraic surface in $\mathcal{E}_L^3$ using the 123-surface. The study of torsion points on the 123-surface will be carried out by studying torsion points on this new surface.

The first part of the proof makes no use of the special form of the 123-surface. So all partial results will be formulated for an arbitrary irreducible algebraic surface X_L in $\mathcal{E}_L^3$.

On any elliptic curve, or more generally, on any Abelian scheme we use $[N]$ to denote the multiplication by $N \in \mathbf{Z}$ morphism. In Proposition 2.1, we prove that X_L contains only finitely many torsion points outside the so-called torsion anomalous locus of X_L. Informally, this is the union of all positive dimension subvarieties of X_L on which an excessive number of independent integral relations

$$[\alpha](P_1) + [\beta](P_2) + [\gamma](P_3) = 0 \quad \text{where} \quad (P_1, P_2, P_3, \lambda) \in X_L \quad \text{and} \quad \alpha, \beta, \gamma \in \mathbf{Z} \tag{1.4}$$

hold identically. A precise definition is provided in Section 2.

To prove Proposition 2.1 we follow the basic strategy originally proposed by Zannier. It involves estimating from above and below the number of rational points

on certain sufficiently tame sets. This strategy already appeared in the proof of Masser and Zannier's result mentioned further up. It was also used in a new proof of the Manin-Mumford Conjecture by Pila and Zannier [13].

An elliptic logarithm of a torsion point on an elliptic curve has rational coefficients with respect to a chosen period lattice basis. The conjugate of any torsion point again leads to a rational point. This observation together with estimates for the Galois orbit of a torsion point yields the required lower bounds for rational points. Masser and Zannier required an upper bound, proved by Pila, for the number of rational points with fixed denominator on compact subanalytic surfaces.

Additional difficulties arise in our situation since X_L is an algebraic surface as opposed to the algebraic curve connected with (1.1). For example, a crucial height inequality used by Masser and Zannier which depends on work of Silverman has only recently been extended to higher dimension [6] by the author.

Algebraic independence statements for certain transcendental functions related to elliptic logarithms played an important role in Masser and Zannier's result regarding (1.1) and even more so in their generalization to curves [9]. These cannot be applied directly to the higher dimensional case; and neither can Bertrand's more general results [2]. We overcome this difficulty using two tools. First, we use a bound of David [5] on the number of torsion points defined over a number field on an elliptic curve. The quality of his bound is indispensable in our method. It enables us to choose a "wandering curve" in X_L containing sufficiently many conjugates of a given torsion point. We can then apply results from the one dimensional case to this curve. Second, we replace Pila's counting result by the powerful theorem of Pila and Wilkie [12] formulated in the versatile language of o-minimal structures. This additional generality is required to treat the real 4 dimensional sets which arise naturally in our problem. The Pila-Wilkie Theorem is uniform over definable families, a feature which is needed to control the wandering curve constructed above.

A brief recollection of the theory of o-minimal structures is presented in Subsection 2.1. Using David's result we will find an abundance of rational points coming from elliptic logarithms on one fiber of a definable family. Enough actually, to successfully compete with the upper bound coming from the Pila-Wilkie Theorem.

In the second half of the proof, detailed in Section 3, we return to the Weierstrass family, the natural setting of our main result. The obstruction to obtaining finiteness in the first half was the torsion anomalous locus of X_L. There is also an analogous locus for algebraic surfaces in $\mathcal{E}^3$. The goal of the second half is to get hold of this locus for the 123-surface. In fact, Proposition 3.2 tells us that it is empty. We briefly indicate the general idea of the argument.

Typically, an anomalous subvariety is an irreducible algebraic curve $C \subset X$ on which two independent relations as in (1.4) hold. We can specialize to any point in the image of C under $\mathcal{E}^3 \to S$. This yields three points on an elliptic curve over $\mathbf{C}$ which are connected by two independent relations. In this situation it seems difficult to directly extract information from the fact that the first affine coordinates of these three points are $1, 2$, and 3. Roughly speaking, we will specialize to a point on the boundary of a compactification of S. Let us consider the morphism

$C \to \pi(C)$ coming from the restriction to C of $\pi : \mathcal{E}^3 \to S$. Passing to the generic fiber yields a point on the cube of an elliptic curve defined over the function field of $\pi(C)$. Let us assume, for now, that this elliptic curve has a place of split multiplicative reduction. We use the Tate uniformization which relates the group structure of an elliptic curve and the multiplicative group of a field. This will allow us to translate the excessive number of integral relations into a completely explicit multiplicative relation involving algebraic numbers derived from 1, 2, and 3. It is then a simple matter to show that this multiplicative relation is untenable. From this we will deduce that the generic fiber of $C \to \pi(C)$ must have good reduction everywhere. Therefore, all fibers share a common j-invariant. From this severe restriction it will not be difficult to derive a contradiction using the particular nature of the 123-surface.

We make heavy use of the special nature of our surface in the second half. What happens if one replaces 1, 2, 3 by another triple of algebraic numbers? We have seen that finiteness need not hold even if the triple consists of pairwise distinct integers. In an unpublished manuscript the author described a necessary condition on the triple to ensure a finiteness statement as in Theorem 1.1. For example, the first three primes 2, 3, 5 also yield a finiteness result as in our main result.

The author is very grateful to David Masser and Umberto Zannier for the numerous conversations, especially productive in Pisa, July 2010. He also thanks the latter for the invitation to Pisa and the Scuola Normale Superiore for its hospitality and financial support. The author was also supported by SNSF project number 124737.

2. Torsion points outside the torsion anomalous locus

We will work with an irreducible closed algebraic surface X in $\mathcal{E}_L^3$. The 123-surface will not appear in the current section. So no ambiguity can occur if we avoid the more cumbersome notation X_L from the introduction and use π to denote the projection $\mathcal{E}_L \to Y(2)$. We do keep the subscript in $\mathcal{E}_L$ to emphasize that we are in the Legendre family.

For $\lambda \in Y(2)$ the fiber $(\mathcal{E}_L)_\lambda = \pi^{-1}(\lambda)$ is taken as an elliptic curve given in Legendre form. We identify the three-fold fibered power $\mathcal{E}_L^3$ of $\mathcal{E}_L \to Y(2)$ with

$$\mathcal{E}_L^3 = \big\{(P_1, P_2, P_3, \lambda) \in (\mathbf{P}^2)^3 \times Y(2);\ \ P_1, P_2, P_3 \in (\mathcal{E}_L)_\lambda\big\}.$$

By abuse of notation we also use π for the projection $\mathcal{E}_L^3 \to Y(2)$ and write $(\mathcal{E}_L^3)_\lambda = \pi^{-1}(\lambda) \subset \mathcal{E}_L^3$. Recall that $(P_1, P_2, P_3, \lambda) \in \mathcal{E}_L^3$ is called torsion if P_1, P_2, and P_3 are torsion points of $(\mathcal{E}_L)_\lambda$.

Any $\chi = (\alpha, \beta, \gamma) \in \mathbf{Z}^3$ determines a Zariski closed set $G_\chi \subset \mathcal{E}_L^3$ through the integral relation

$$[\alpha](P_1) + [\beta](P_2) + [\gamma](P_3) = 0.$$

An irreducible closed subvariety A of X is called a *torsion anomalous subvariety* of X

(i) if $\dim A = 1$ and two independent integral relations hold on A,
(ii) or if $\dim A = 2$ and one non-trivial integral relation holds on A,
(iii) or if $\dim A \geq 1$ and A is an irreducible component of an algebraic subgroup of $(\mathcal{E}_L^3)_\lambda$ for some $\lambda \in Y(2)$ such that $(\mathcal{E}_L)_\lambda$ has complex multiplication.

The torsion anomalous locus of X is $\bigcup_A A$, here A runs over all torsion anomalous subvarieties of X. We write X^{ta} for the *complement* of the torsion anomalous locus in X.

An irreducible closed subvariety $A \subset \mathcal{E}_L^3$ which dominates $Y(2)$ is called a *component of a flat subgroup scheme* of $\mathcal{E}_L$

(i) if $\dim A = 1$ and three independent integral relations hold on A,
(ii) or if $\dim A = 2$ and two independent integral relation hold on A,
(iii) or if $\dim A = 3$ and one independent integral relation holds on A,
(iv) or if $A = \mathcal{E}_L^3$.

We write $X^\star$ for $X \smallsetminus \bigcup_A A$, here A runs over all components of flat subgroup schemes of $\mathcal{E}_L$ contained completely in X. We have $X^{\mathrm{ta}} \subset X^\star$.

The definition of $X^\star$ coincides with the complex points of the corresponding definition given in [6]. Indeed, see Lemma 2.5 in this reference.

The purpose of this section is to prove that there are only finitely many points outside the torsion anomalous locus of X.

Proposition 2.1. *Let $X \subset \mathcal{E}_L^3$ be an irreducible closed algebraic surface defined over $\overline{\mathbf{Q}}$ which dominates $Y(2)$.*

(i) *There are at most finitely many torsion points in X^{ta}.*
(ii) *The set*

$$\{\pi(P);\ P \in X^\star \text{ is torsion and } (\mathcal{E}_L)_{\pi(P)} \text{ has complex multiplication}\}$$

is finite.

It is conceivable that the union in the definition of $X \smallsetminus X^{\mathrm{ta}}$ or $X \smallsetminus X^\star$ is over infinitely many A. So we have no reason to expect that X^{ta} or $X^\star$ is Zariski open. However, $X^\star$ is known to be Zariski open by [6, Theorem 1.3(i)]. In a later section we will address the problem of describing X^{ta} for an algebraic surface derived from the 123-surface. In this particular situation, X^{ta} will be Zariski open.

The author believes that X^{ta} is Zariski open for all surfaces. More precisely, he expects X to contain only finitely many torsion anomalous subvarieties that are not strictly contained in another torsion anomalous subvariety of X.

Let us assume for the moment that this finiteness statement holds for X. Let us also assume that no non-trivial integral relation holds identically on X and that X dominates $Y(2)$. In this case we sketch how Proposition 2.1 implies a uniform

Manin-Mumford-type statement in a family of Abelian varieties. Indeed, we may regard X as a family of curves $\{X_\lambda = X \cap \pi^{-1}(\lambda)\}$ parametrized by $\lambda \in Y(2)$. Up-to finitely many exceptions, controlled by the proposition, any torsion point on a member of this family lies on one of finitely many anomalous subvariety as in cases (i) and (iii) of the definition. So any torsion point on X satisfies two independent relations coming from a fixed finite set. If we are in case (i) then these relations are integral; in case (iii) they have coefficients in the endomorphism ring of an elliptic curve with complex multiplication. It is not difficult to deduce that X_λ contains a positive dimensional irreducible component of an algebraic subgroup for at most finitely many λ. For all other λ two independent relations as above intersect X_λ in a finite set whose cardinality can be bounded from above independently of λ using Bézout's Theorem. We conclude that after omitting finitely many λ there is a uniform upper bound for the number of torsion points on X_λ.

In the remainder of this section we will assume that X is as in the proposition. So it dominates $Y(2)$ and we may fix a number field $F \subset \overline{\mathbf{Q}}$ over which it is defined.

We will work with real parameters $B \geq 1$ and $\delta \in (0, 1]$. Here δ may depend on B and B may depend on the surface X and on F. If not stated otherwise, the symbols $c_1, c_2, \ldots$ will denote positive constants which may depend X, F, δ, and B. During the proof B and δ will be chosen properly.

2.1. o-minimal structures

We provide the definition of an o-minimal structure. For an in-depth treatment of this subject we refer to van den Dries's book [21].

Let $\mathbf{N} = \{1, 2, 3, \ldots\}$. An *o-minimal structure* is a sequence $\mathfrak{S} = (S_1, S_2, \ldots)$ such that if $n, m \in \mathbf{N}$ then S_n is a collection of subsets of $\mathbf{R}^n$ with the following properties.

(i) The intersection of two sets in S_n is in S_n and the complement of a set in S_n is in S_n.
(ii) Any real semi-algebraic subset of $\mathbf{R}^n$ is in S_n.
(iii) The Cartesian product of a set in S_n with a set in S_m is in S_{n+m}.
(iv) The image of a set in S_{n+m} under the projection $\mathbf{R}^n \times \mathbf{R}^m \to \mathbf{R}^n$ onto the first n coordinates is in S_n.
(v) A set in S_1 is a finite union of points and open, possibly unbounded, intervals.

The first four properties assert that an o-minimal structure contains enough interesting sets to work with. The fifth property restricts the possible sets in all S_n because these project to $\mathbf{R}$ by (iv).

We call a subset of $\mathbf{R}^n$ *definable in* $\mathfrak{S}$ if it lies in S_n. If $X \subset \mathbf{R}^n$ then we call a function $f : X \to \mathbf{R}^m$ definable in $\mathfrak{S}$ if its graph, a subset of $\mathbf{R}^n \times \mathbf{R}^m$, lies in S_{n+m}. Domain and image of a function that is definable in $\mathfrak{S}$ are definable in $\mathfrak{S}$.

A subset Z of $\mathbf{R}^n \times \mathbf{R}^m$ that is definable in $\mathfrak{S}$ is sometimes called a family definable in $\mathfrak{S}$. We do this to emphasizes that Z can be seen as a collection of subsets of $\mathbf{R}^n$ parametrized by $\mathbf{R}^m$. Concretely, for $y \in \mathbf{R}^m$ we let Z_y denote the projection of $Z \cap (\mathbf{R}^n \times \{y\})$ to $\mathbf{R}^n$. Then Z_y is definable in $\mathfrak{S}$.

To formulate the result of Pila and Wilkie mentioned in the introduction, we shall define the exponential Weil height on the rational numbers by setting $H(p/q) = \max\{|p|, q\}$ for coprime integers p and q with $q \geq 1$. In higher dimension we set $H(\xi_1, \dots, \xi_n) = \max\{H(\xi_1), \dots, H(\xi_n)\}$ for $(\xi_1, \dots, \xi_n) \in \mathbf{Q}^n$. Let $X \subset \mathbf{R}^n$ be any subset for the moment. The counting function associated to X is

$$N(X, T) = \#\{\xi \in X \cap \mathbf{Q}^n;\ H(\xi) \leq T\} \quad \text{for} \quad T \geq 1;$$

there are only finitely many points in $\mathbf{Q}^n$ of bounded height, so the cardinality is finite.

We define $X^{\mathrm{alg}} \subset X$ to be the union of all connected, positive dimensional real semi-algebraic sets contained in X.

Theorem 2.2 (Pila-Wilkie [12]). *Let $Z \subset \mathbf{R}^n \times \mathbf{R}^m$ be a family definable in an o-minimal structure and let $\epsilon > 0$. There is a constant $c > 0$ depending on Z and ϵ such that if $y \in \mathbf{R}^m$, then*

$$N(Y \smallsetminus Y^{\mathrm{alg}}, T) \leq cT^{\epsilon} \quad \textit{for all} \quad T \geq 1$$

where $Y = Z_y$.

By the Tarski-Seidenberg Theorem, the collection of all real semi-algebraic sets satisfies (iv) in the definition of an o-minimal structure. From this it is not difficult to show that the real semi-algebraic sets define an o-minimal structure. But this structure is not large enough for our needs. Luckily, a variety of larger o-minimal structures are known. For example, van den Dries [20] reinterpreted a result of Gabrielov as stating that the so-called finitely subanalytic sets form an o-minimal structure $\mathbf{R}_{\mathrm{an}}$. We will not give the definition of such sets here. It suffices to remark that the restriction to $[-1, 1]^n$ of a real valued analytic function on a neighborhood of $[-1, 1]^n$ is definable in $\mathbf{R}_{\mathrm{an}}$. This will be enough functions for our application.

For the remainder of this section we will call sets, functions, and families *definable* if they are definable in $\mathbf{R}_{\mathrm{an}}$.

We could not find a reference for the following, possibly well-known, statement. Therefore, we provide its short proof which is valid in any o-minimal structure.

Lemma 2.3. *Let $X \subset \mathbf{R}^n$ be a definable set and let $f : X \to \mathbf{R}^m$ be a definable function. There are definable sets $X_0, \dots, X_M \subset \mathbf{R}^n$ with $X = X_0 \cup X_1 \cup \cdots \cup X_M$ such that $f|_{X_1}, \dots, f|_{X_M}$ are injective and such that the fibers of $f|_{X_0}$ contain no isolated points. Here $X_0 = \emptyset$ and $M = 0$ are possible.*

Proof. We first prove the lemma when f has finite fibers. Then the fibers have cardinality bounded from above uniformly by [21, Corollary 3.6, page 60]. Say c is the maximal cardinality attained. We may suppose $c \geq 2$. By Definable Choice, Proposition 1.2, page 93 *ibid.*, there is a definable function $g : f(X) \to \mathbf{R}^n$ with $f(g(y)) = y$ for all $y \in f(X)$. The sets $g(f(X))$ and $X \smallsetminus g(f(X))$ are definable.

Now the definable function $f|_{g(f(X))}$ is injective and the fibers of the definable function $f|_{X\setminus g(f(X))}$ have cardinality at most $c-1$. The current case of the lemma follows by induction on c.

In the general case we observe that

$$X_0 = \{x \in X;\ x \text{ not isolated in } f^{-1}(f(x))\}$$

is a definable set by the Cell Decomposition Theorem, *cf.* page 52 *ibid.* We note that X_0 contains no isolated points. The function f restricted to its complement in X has discrete fibers. Again by Corollary 3.6, page 60 *ibid.* these fibers are finite. This enables us to reduce to the situation above. □

2.2. A definable family

In the current subsection, any reference to a topology on X or $\mathcal{E}_L^3$ will refer to the Euclidean topology if not stated otherwise.

In a neighborhood of $1/2 \in Y(2) = \mathbf{C}\setminus\{0, 1\}$ we may describe a period lattice basis of the fiber of $\mathcal{E}_L$ using Gauss's hypergeometric function, *cf.* [8, Chapter 9]. This period lattice basis can be continued analytically along any path in $Y(2)$. We fix a path from any point in $\mathcal{E}_L^3$ to the zero element of $(\mathcal{E}_L^3)_{1/2}$. We continue the periods along the path induced in $Y(2)$.

Any $P \in \mathcal{E}_L^3$ has a neighborhood V_P in $\mathcal{E}_L^3$ on which we may choose holomorphic elliptic logarithms

$$z_{P1}, z_{P2}, z_{P3} : V_P \to \mathbf{C}.$$

We may also fix holomorphic functions $f_P, g_P : V_P \to \mathbf{C}$ whose values determine a basis of the period lattice of the corresponding fiber.

The values of f_P and g_P are $\mathbf{R}$-linearly independent. We can express z_{Pk} in terms of f_P and g_P using real analytic functions $\xi_{P1}, \ldots, \xi_{P6} : V_P \to \mathbf{R}$, *i.e.*

$$z_{P1} = \xi_{P1} f_P + \xi_{P2} g_P, \quad z_{P2} = \xi_{P3} f_P + \xi_{P4} g_P, \quad \text{and} \quad z_{P3} = \xi_{P5} f_P + \xi_{P6} g_P.$$

We write $\theta_P : V_P \to \mathbf{R}^6$ for the real analytic function

$$Q \mapsto (\xi_{P1}(Q), \ldots, \xi_{P6}(Q)).$$

It provides coordinates of an elliptic logarithm of Q in terms of the period lattice basis given by $f_P(Q)$ and $g_P(Q)$.

After shrinking V_P we may suppose that it is contained in an affine subset of $\mathcal{E}_L^3$. This has the effect that if $X' \subset \mathcal{E}_L^3$ is Zariski closed then $X' \cap V_P$ can be described as the set of common zeros of finitely many polynomials restricted to V_P.

We note that $\mathcal{E}_L^3$ is an 8-dimension real analytic manifold. After shrinking V_P there is a real bianalytic map $\vartheta_P : (-2, 2)^8 \to V_P$ taking 0 to P. We define

$$U_P = X \cap \vartheta_P([-1, 1]^8) \subset V_P.$$

Then U_P is compact since $\vartheta_P([-1,1]^8)$ is compact. It is also a neighborhood of P in X.

The compact set

$$\Lambda_\delta = \{z \in \mathbf{C};\ \delta \le |z| \le \delta^{-1} \quad \text{and} \quad |1-z| \ge \delta\}$$

is contained in $Y(2)$. The pre-image $\pi|_X^{-1}(\Lambda_\delta) = X \cap \big((\mathbf{P}^2)^3 \times \Lambda_\delta\big)$ is also compact. This set is covered by all neighborhoods U_P with $P \in \pi|_X^{-1}(\Lambda_\delta)$. So there is a positive integer c_1 and $P_1, \dots, P_{c_1} \in \pi|_X^{-1}(\Lambda_\delta)$ with $U_{P_1} \cup \dots \cup U_{P_{c_1}} \supset \pi|_X^{-1}(\Lambda_\delta)$.

In the following, we drop the P and write $U_i, V_i, \theta_i, \vartheta_i$ for $U_{P_i}, V_{P_i}, \theta_{P_i}, \vartheta_{P_i}$, respectively.

Let $|\cdot|$ denote the maximum norm on $\mathbf{R}^n$.

Lemma 2.4. *Let $1 \le i \le c_1$. There are sets $U_{i0}, \dots, U_{iM_i}$ with $U_i = U_{i0} \cup \dots \cup U_{iM_i}$ such that the following properties hold.*

(i) *The functions $\theta_i|_{U_{i1}}, \dots, \theta_i|_{U_{iM_i}}$ are injective and the fibers of $\theta_i|_{U_{i0}}$ contain no isolated points.*
(ii) *If $X' \subset \mathcal{E}_L^3$ is Zariski closed, then $\theta_i(X' \cap U_{ij}) \subset \mathbf{R}^6$ is definable for all $0 \le j \le M_i$.*
(iii) *There is c_2 with $|\xi| \le c_2$ if $\xi \in \theta_i(U_i)$.*

Proof. By construction, $X \cap V_i$ is the zero set in V_i of functions that are polynomial on V_i. So each pre-image $\vartheta_i^{-1}(U_i) = \vartheta_i^{-1}(X \cap V_i) \cap [-1,1]^8$ is the set of common zeros of finitely many real analytic functions on $(-2,2)^8$ restricted to $[-1,1]^8$. Therefore, it is definable in our o-minimal structure $\mathbf{R}_{\mathrm{an}}$.

Observe that $\theta_i \circ \vartheta_i$ is real analytic on $(-2,2)^8$. Its restriction to $\vartheta_i^{-1}(U_i)$ is thus definable. We apply Lemma 2.3 to $\theta_i \circ \vartheta_i|_{\vartheta_i^{-1}(U_i)}$ and obtain $M+1$ definable subsets of $\vartheta_i^{-1}(U_i)$. Taking their images under ϑ_i gives $U_{i0}, U_{i1}, \dots, U_{iM_i}$ with $U_i = U_{i0} \cup \dots \cup U_{iM_i}$. The statement of Lemma 2.3 and the fact that ϑ_i is injective and continuous is what is needed for (i).

Let X' be as in part (ii). As before, $\vartheta_i^{-1}(X' \cap V_i) \cap [-1,1]^8$ is a definable set and therefore so is $\vartheta_i^{-1}(U_{ij}) \cap \vartheta_i^{-1}(X' \cap V_i) \cap [-1,1]^8 = \vartheta_i^{-1}(X' \cap U_{ij})$. Its image $\theta_i(X' \cap U_{ij})$ under the definable function $\theta_i \circ \vartheta_i|_{[-1,1]^8}$ is definable. This shows (ii).

Part (iii) follows since U_i is compact and θ_i is continuous. □

In order to avoid double indices we rename U_{ij} as U_i by increasing, if necessary, the constant c_1. Of course, we also adjust the θ_i accordingly. For example, in this new notation claim (i) of the preceding lemma states that $\theta_i|_{U_i}$ is either injective or has fibers without isolated points.

We define

$$W_i = \theta_i(U_i) \subset \mathbf{R}^6.$$

This is a definable set by part (ii) of the lemma above applied to $X \supset U_i$.

The image of a torsion point of order N in U_i lies in $\frac{1}{N}\mathbf{Z}^6 \cap W_i$. For this reason we are interested in the distribution of rational points on W_i. Below, we will find many such rational points on a fiber of

$$\begin{aligned} Z_i = &\{(\xi_1, \dots, \xi_6, \alpha, \beta, \gamma, \psi, \omega) \in W_i \times \mathbf{R}^5; \\ &\alpha\xi_1 + \beta\xi_3 + \gamma\xi_5 = \psi \quad \text{and} \quad \alpha\xi_2 + \beta\xi_4 + \gamma\xi_6 = \omega\} \subset \mathbf{R}^6 \times \mathbf{R}^5 \end{aligned} \tag{2.1}$$

considered as a family parametrized by $\mathbf{R}^5$. We note that the Z_i are definable because their definition involve only definable sets and the basic algebraic operations.

The next lemma is the theorem of Pila and Wilkie adapted to our situation.

Lemma 2.5. *There exists a positive constant c_3, depending on the usual data, such that if $1 \le i \le c_1$ and $y \in \mathbf{R}^5$, then*

$$N(Y \setminus Y^{\text{alg}}, T) \le c_3 T^{1/12} \quad \textit{for all} \quad T \ge 1$$

where $Y = (Z_i)_y$.

Proof. This follows from Theorem 2.2 adapted to our situation. □

As we will see below, it is critical that this estimate is uniform in the parameter y. We work with the exponent $1/12$ for expository reasons; the Theorem of Pila-Wilkie provides any positive ϵ at the cost of increasing c_3.

2.3. The Galois orbit of a torsion point

Let E be an elliptic curve defined over a number field K. It is well-known that the group of torsion points $E(K)_{\text{tors}}$ of $E(K)$ is finite. By a deep result of Merel its cardinality $\#E(K)_{\text{tors}}$ is bounded from above solely in terms of $[K : \mathbf{Q}]$. In particular, the bound does not depend on the height of E. Our method allows us to assume that the height of E is bounded. So the deep uniformity aspect in Merel's work will not play a role here. On the other hand, our argument is quite sensitive in the dependency in $[K : \mathbf{Q}]$ of the bound for $\#E(K)_{\text{tors}}$.

The following result of David is essentially best possible with regard to the degree for an unrestricted elliptic curve.

For a definition and basic properties of the absolute logarithmic Weil height h, or just height for short, we refer to Chapter 1.5 in Bombieri and Gubler's book [4].

Theorem 2.6 (David [5]). *There exists a positive absolute constant c_4 with the following property. Let E be an elliptic curve defined over a number field K and let $h_0 \ge 1$ be a bound for the height of the j-invariant of E. Then*

$$\#E(K)_{\text{tors}} \le c_4 h_0 [K : \mathbf{Q}] \log(3[K : \mathbf{Q}]).$$

Proof. This follows from [5, Théorème 1.2(i)]. Indeed, torsion points have Néron-Tate height zero. □

Our approach works as long as one has a bound of the form $\#E(K)_{\text{tors}} \le c(h_0)[K : \mathbf{Q}]^\kappa$ with fixed $\kappa < 3/2$ and where $c(h_0)$ is allowed to depend on h_0.

2.4. Torsion points on X

Throughout this subsection we work with a fixed torsion point $P=(P_1, P_2, P_3, \lambda)\in X(\overline{\mathbf{Q}})$. We will additionally assume

$$h(\lambda) \leq B;$$

here B is the parameter introduced in beginning of this section. It will be fixed at a later point in the proof and may depend on X but not on P. We recall that $\delta, c_1, c_2, \ldots$ may depend on B; but they shall not depend on P.

Let N be the order of P. For brevity, say $K = F(P) \subset \overline{\mathbf{Q}}$ and $D = [K : F]$. We remark $\lambda \in K \smallsetminus \{0, 1\}$. We write Σ for the set of embeddings $\sigma : K \to \mathbf{C}$ that restrict to the identity on F. Then $\#\Sigma = D$.

Lemma 2.7. *There exist a positive absolute constant c_8 and $\chi \in \mathbf{Z}^3 \smallsetminus \{0\}$ with*

$$\max\{N, |\chi|^3\} \leq c_8 D \log(3D)$$

such that $P \in G_\chi$.

Proof. The three torsion points P_1, P_2, P_3 generate a finite subgroup Γ of $(\mathcal{E}_L)_\lambda(K)_{\mathrm{tors}}$. Being a finite subgroup of an elliptic curve, Γ is isomorphic to $(\mathbf{Z}/N'\mathbf{Z}) \times (\mathbf{Z}/R\mathbf{Z})$ for some positive integers $R|N'$. Since Γ is killed by multiplication by N we find $N'|N$. But we must have $N' = N$ since P has order N.

Finding $\chi = (\alpha, \beta, \gamma) \in \mathbf{Z}^3 \smallsetminus \{0\}$ with $[\alpha](P_1) + [\beta](P_2) + [\gamma](P_3) = 0$ on $(\mathcal{E}_L)_\lambda$ amounts to finding $(\alpha, \beta, \gamma, *, *) \in \mathbf{Z}^5 \smallsetminus \{0\}$ in the kernel of a certain matrix

$$\begin{bmatrix} * & * & * & N & 0 \\ * & * & * & 0 & R \end{bmatrix} \tag{2.2}$$

where the entries denoted by $*$ are integers; in the first and second row they lie in $[-N/2, N/2]$ and $[-R/2, R/2]$, respectively.

We apply Siegel's Lemma as stated in [4, Corollary 2.9.7]. The height of the system (2.2) is at most $c_5 NR$ with $c_5 > 0$ absolute. Since our system has three independent solutions, there is a solution in $\mathbf{Z}^5 \smallsetminus \{0\}$ with maximum norm at most $c_6(NR)^{1/3}$. Forgetting the last two coordinates gives

$$|\chi| \leq c_6(NR)^{1/3}. \tag{2.3}$$

On the other hand, we have $NR = \#\Gamma \leq \#(\mathcal{E}_L)_\lambda(K)_{\mathrm{tors}}$. David's result from the last section implies $NR \leq c_4 h_0 D \log(3D)$, here h_0 is 1 more than the height of the j-invariant of $(\mathcal{E}_L)_\lambda$. This j-invariant equals

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \tag{2.4}$$

by [19, Proposition III 1.7(b)]. Elementary height inequalities imply that h_0 is bounded in terms of $h(\lambda)$. So h_0 is bounded in terms of B. Hence $NR \leq c_7 D \log(3D)$ and in particular $N \leq c_7 D \log(3D)$. This is the bound for N in the assertion. We find the bound for $|\chi|^3$ by recalling (2.3). □

Any embedding $\sigma \in \Sigma$ determines a torsion point $P^\sigma = \sigma(P) \in X(\overline{\mathbf{Q}})$.

Lemma 2.8. *For $\delta \in (0, 1]$ sufficiently small in terms of B and F there is a positive constant $c_9 \leq 1$ and an index $1 \leq i_0 \leq c_1$ such that for at least $c_9 D$ embeddings $\sigma \in \Sigma$ we have*

$$\pi(P^\sigma) \in \Lambda_\delta \quad \text{and} \quad P^\sigma \in U_{i_0}.$$

Proof. A similar statement was given in [11, Lemma 6.2]. Recall $\lambda = \pi(P) \in K$. Let $\delta \in (0, 1]$ and let us assume $\sigma(\lambda) \notin \Lambda_\delta$ for more than $D/2$ embeddings $\sigma \in \Sigma$. Then one of

$$|\sigma(\lambda)| > \delta^{-1}, \quad |\sigma(\lambda)|^{-1} > \delta^{-1}, \quad |1 - \sigma(\lambda)|^{-1} > \delta^{-1}$$

holds for more than $D/6$ embeddings $\sigma \in \Sigma$.

By elementary height properties we have $h(\lambda^{-1}) = h(\lambda) \leq B$ and $h((1-\lambda)^{-1}) = h(1 - \lambda) \leq h(\lambda) + \log 2 \leq B + \log 2$. The definition of the height as stated on the bottom of [4, page 16] implies

$$\begin{aligned} &h(\lambda) + h(\lambda^{-1}) + h((1 - \lambda)^{-1}) \\ &\geq \frac{1}{[K : \mathbf{Q}]} \sum_{\sigma : K \to \mathbf{C}} \log \left(\max\{1, |\sigma(\lambda)|\} \max\left\{1, \frac{1}{|\sigma(\lambda)|}\right\} \max\left\{1, \frac{1}{|1 - \sigma(\lambda)|}\right\} \right) \end{aligned}$$

here σ runs over all embeddings of K into $\mathbf{C}$. We bound $3B + \log 2 \geq D/(6[K : \mathbf{Q}]) \log(\delta^{-1})$. But $[K : \mathbf{Q}] = D[F : \mathbf{Q}]$, so $\log(\delta^{-1}) \leq 6[F : \mathbf{Q}](3B + \log 2)$.

So if $\delta \in (0, 1]$ is sufficiently small with respect to B and F there are at least $D/2$ embeddings $\sigma \in \Sigma$ satisfying $\sigma(\lambda) = \pi(P^\sigma) \in \Lambda_\delta$. Recall that $\pi|_X^{-1}(\Lambda_\delta)$ is covered by $U_1, \ldots, U_{c_1}$. The lemma follows from the Pigeonhole Principle on taking $c_9 = 1/(2c_1)$. □

We fix δ and i once and for all as in this lemma and let $\Sigma' \subset \Sigma$ denote the subset provided therein. We abbreviate $U = U_{i_0}$, $W = W_{i_0}$, $Z = Z_{i_0}$, and $\theta = \theta_{i_0}$ from Subsection 2.2. The fact that i_0 may depend on P will be harmless.

The conjugates P^σ lie in U for all $\sigma \in \Sigma'$. We denote their images under θ by

$$\xi^\sigma = (\xi_1^\sigma, \ldots, \xi_6^\sigma) = \theta(P^\sigma) \in W.$$

Since P^σ has order N we have $\xi^\sigma \in \frac{1}{N}\mathbf{Z}^6$ for the coordinates in terms of the period lattice basis.

Before we continue, let us recapitulate the current situation and also describe how we will proceed. In total there are D conjugates of P over F. Of these, a fixed positive proportion lies on the set $U \subset X$. So by Lemma 2.7, the number of conjugates on U is at least of order $N/\log N$. The next lemma is crucial. It states that among the embeddings considered above, at least approximately $N^{1/3}/\log N$ yield a ξ^σ in a fixed fiber of the definable family Z constructed around (2.1). We will show that the number of ξ^σ equals the number of conjugates P^σ, at least in the most interesting cases. As we have seen above, the ξ^σ are rational. Their heights turn out to be bounded linearly in terms of N. Consequentially, we will

have found many rational points of bounded height on a fixed fiber of Z. But we have no control over the precise fiber containing these rational points; its existence is derived from the Pigeonhole Principle. This is compensated by the fact that the Pila-Wilkie Theorem is uniform over definable families. We then conclude the existence of a semi-algebraic curve inside a fixed fiber of Z. Such a curve will lead to a torsion anomalous subvariety of X.

Lemma 2.9. *There exist a positive constant c_{12}, a tuple $y = (\alpha, \beta, \gamma, *, *) \in \mathbf{Z}^5$ with $(\alpha, \beta, \gamma) \neq 0$, and a subset $\Sigma'' \subset \Sigma'$ with*

$$\#\Sigma'' \geq c_{12}\frac{N^{1/3}}{\log(3N)} \quad \textit{such that} \quad \xi^\sigma \in Z_y \quad \textit{for all} \quad \sigma \in \Sigma''.$$

Proof. Let $\chi = (\alpha, \beta, \gamma)$ be as in Lemma 2.7. Then $P \in G_\chi$ and even $P^\sigma \in G_\chi$ for all $\sigma \in \Sigma$. For $\sigma \in \Sigma'$, the period coordinates satisfy

$$(\alpha\xi_1^\sigma + \beta\xi_3^\sigma + \gamma\xi_5^\sigma, \alpha\xi_2^\sigma + \beta\xi_4^\sigma + \gamma\xi_6^\sigma) \in \mathbf{Z}^2. \tag{2.5}$$

A simply application of the triangle inequality together with the bound for ξ_j^σ from Lemma 2.4(iii) gives

$$|\alpha\xi_1^\sigma + \beta\xi_3^\sigma + \gamma\xi_5^\sigma| \leq 3c_2|\chi|.$$

The same bound holds for $|\alpha\xi_2^\sigma + \beta\xi_4^\sigma + \gamma\xi_6^\sigma|$. So the number of possibilities for the integral vector (2.5) is at most $(6c_2|\chi| + 1)^2$ as σ runs over Σ'. Using Lemma 2.7, the number of possibilities is at most $c_{10}D^{2/3}\log(3D)^{2/3}$.

We recall $\#\Sigma' \geq c_9 D$. By the Pigeonhole Principle there is a subset $\Sigma'' \subset \Sigma'$ with

$$\#\Sigma'' \geq \frac{c_9 D}{c_{10}D^{2/3}\log(3D)^{2/3}} = c_{11}\left(\frac{D}{\log(3D)^2}\right)^{1/3}$$

such that (2.5) attains the same value for all $\sigma \in \Sigma''$. We use elementary estimates and $N \leq c_8 D\log(3D)$ from Lemma 2.7 to conclude

$$\#\Sigma'' \geq c_{11}\left(\frac{D\log(3D)}{\log(3D)^3}\right)^{1/3} \geq c_{11}\left(\frac{D\log(3D)}{\log(3D\log(3D))^3}\right)^{1/3} \geq c_{12}\frac{N^{1/3}}{\log(3N)}. \qquad \square$$

We recall some notation from [6]. There $\ker[N]$ was defined as the kernel of the multiplication by N morphism $[N] : \mathcal{E}_L^3 \to \mathcal{E}_L^3$.

Next we find a condition which guarantees that the conjugates of P indeed lead to many rational points ξ^σ. The condition is satisfied if for example P is not inside an anomalous subvariety of X.

Lemma 2.10. *Let us assume that $\{P\}$ is an irreducible component of $X \cap \ker[N]$. Then $\theta|_U : U \to \mathbf{R}^6$ is injective and in particular, $\#\{\xi^\sigma;\ \sigma \in \Sigma''\} = \#\Sigma''$.*

Proof. By Lemma 2.4(i) we know that $\theta|_U$ is either injective or has fibers without isolated points. Say we are in the second case and let us fix $\sigma \in \Sigma''$. The fiber of θ containing any P^σ also contains an infinite sequence $(P_k)_{k\in\mathbf{N}}$ with $P_k \in U \smallsetminus \{P^\sigma\}$ converging to P^σ. Since elliptic logarithms of P_k and P^σ have the same coordinates with respect to a period lattice basis we find $P_k \in \ker[N]$. Therefore, $\{P^\sigma\}$ is not an irreducible component of $X \cap \ker[N]$. The same holds true for $\{P\}$ and this contradicts our hypothesis. □

We now apply the Theorem of Pila-Wilkie.

Lemma 2.11. *Assume P satisfies the hypothesis of Lemma* 2.10 *and suppose N, the order of P, is sufficiently large, i.e. $N \geq c_{15}$. There exist $\chi \in \mathbf{Z}^3 \smallsetminus \{0\}$, an irreducible component $C \subset X \cap G_\chi$, and $\sigma \in \Sigma$ with $P^\sigma \in C$ such that $\theta(C \cap U)$ contains a connected real semi-algebraic curve.*

Proof. Let $y = (\alpha, \beta, \gamma, \psi, \omega) \in \mathbf{Z}^5 \smallsetminus \{0\}$ and Σ'' be as provided by Lemma 2.9. Say $\sigma \in \Sigma''$. Then P^σ is torsion of order N and we have $\xi^\sigma \in \frac{1}{N}\mathbf{Z}^6$. On the other hand, $|\xi^\sigma| \leq c_2$ by Lemma 2.4(iii). Therefore,

$$\xi^\sigma \in \mathbf{Q}^6 \quad \text{and} \quad H(\xi^\sigma) \leq c_{13}N \quad \text{with} \quad c_{13} = \max\{1, c_2\}. \tag{2.6}$$

We set $T = c_{13}N \geq 1$. By Lemma 2.9 we have $\Sigma'' \geq c_{14}T^{1/3-1/6} = c_{14}T^{1/6}$. The number of rational points ξ^σ is thus at least $c_{14}T^{1/6}$ by Lemma 2.10. However, the upper bound from Lemma 2.5 gives

$$N(Z_y \smallsetminus (Z_y)^{\mathrm{alg}}, T) \leq c_3 T^{1/12}.$$

We may assume that $T = c_{13}N$ is sufficiently large to the end that $c_{14}T^{1/6} > c_3T^{1/12}$. Hence there exists $\sigma \in \Sigma''$ with $\xi^\sigma \in (Z_y)^{\mathrm{alg}}$. In other words, there is a connected real semi-algebraic set R in Z_y of positive dimension that contains ξ^σ.

Any $\xi' = (\xi_1, \ldots, \xi_6) \in Z_y$ satisfies

$$\alpha\xi_1 + \beta\xi_3 + \gamma\xi_5 = \psi \quad \text{and} \quad \alpha\xi_2 + \beta\xi_4 + \gamma\xi_6 = \omega.$$

By definition, $Z_y \subset W = \theta(U)$. So there is $Q \in U$ with $\theta(Q) = \xi'$. The linear relations imply $Q \in G_\chi$ with $\chi = (\alpha, \beta, \gamma)$. We conclude $Z_y \subset \theta(U \cap G_\chi)$. Let $X \cap G_\chi = C_1 \cup \cdots \cup C_r$ be the decomposition into irreducible components. So $Z_y \subset \bigcup_k \theta(C_k \cap U)$.

Since Z_y contains a connected real semi-algebraic set of positive dimension that passes through ξ^σ, it is reasonable to expect some $\theta(C_k \cap U)$ to do the same. Let us now prove this fact. By [21, Proposition 3.2, page 100] there is a continuous semi-algebraic function $\gamma : [0, 1] \to Z_y$ with $\gamma(0) = \xi^\sigma$ and $\gamma(1) \neq \gamma(0)$. Each $\theta(C_k \cap U)$ is definable by Lemma 2.4(ii). The pre-images $I_k = \gamma^{-1}(\theta(C_k \cap$

$U)) \subset \mathbf{R}$ are definable and their union is $[0,1]$. Recall that U is compact. So each I_k is closed because $\theta(C_k \cap U) \subset \mathbf{R}^6$ is closed. By property (v) of an o-minimal structure, each I_k is a finite union of closed intervals. So there is k and $t \in (0,1]$ such that I_k has $[0,t]$ as a connected component. We may choose k such that t is maximal. So $\gamma|_{[0,t]}$ maps to $\theta(C \cap U)$ with $C = C_k$; in particular, $\xi^\sigma \in \theta(C \cap U)$. What if $\gamma|_{[0,t]}$ is constant? Then $t < 1$ because $\gamma(1) \neq \gamma(0)$. By a similar argument as above, the interval $[t,1]$ can be covered by pre-images which are themselves finite unions of closed intervals. From this we deduce a contradiction to the maximality of t. So $\gamma|_{[0,t]}$ is non-constant. Its image is a connected real semi-algebraic curve which is completely contained in $\theta(C \cap U)$.

This implies the second assertion of the lemma. It also shows that $\xi^\sigma = \theta(P')$ for some $P' \in C \cap U$. But recall that $\theta|_U$ is injective by Lemma 2.10 and $\theta(P^\sigma) = \xi^\sigma$. Therefore, $P^\sigma = P' \in C$. □

Lemma 2.12. *Let $C \subset \mathcal{E}_L^3$ be an irreducible algebraic curve such that $\theta(U \cap C)$ contains a connected real semi-algebraic curve.*

(i) *If $\pi|_C : C \to Y(2)$ is dominant there exist independent $\chi', \chi'' \in \mathbf{Z}^3$ with $C \subset G_{\chi'} \cap G_{\chi''}$.*
(ii) *If $\pi|_C : C \to Y(2)$ is not dominant, then it is constant and C is the translate of an algebraic subgroup of $(\mathcal{E}_L^3)_{\pi(C)}$.*

Proof. Part (i) follows from Bertrand's [2, Théorème 5] applied to the three possible projections of C onto $\mathcal{E}_L^2$. Alternatively, we can also refer to Masser and Zannier's [9, Appendix A].

Part (ii) is a consequence of Ax's [1, Theorem 3] for a fixed Abelian variety. □

2.5. Proof of Proposition 2.1

We begin by fixing the parameter B used above.

By [6, Theorem 1.3(ii)] there exists $B \geq 1$, depending on X, with $h(\pi(P)) \leq B$ for all torsion points $P \in X^\star \cap X(\overline{\mathbf{Q}})$.

Let $P \in X^\star$ be a torsion point of order N and set $\lambda = \pi(P)$.

The Zariski closed set $\ker[N]$ is equidimensional of dimension 1 by [6, Lemma 2.5]. So $\{P\}$ is an irreducible component of the intersection $X \cap \ker[N]$. We can deduce two things. First, using the fact that X and $\ker[N]$ are defined over $\overline{\mathbf{Q}}$ we find that P is algebraic, *i.e.* $P \in X(\overline{\mathbf{Q}})$. Second, $h(\lambda) \leq B$. So P is as in Subsection 2.4.

After omitting finitely many P we may suppose that N is sufficiently large; for example $N \geq c_{15}$, the constant from Lemma 2.11. We remark that P satisfies the hypothesis of this lemma.

We will prove part (ii) first. So we shall additionally assume that $(\mathcal{E}_L)_\lambda$ has complex multiplication. The j-invariant J of the elliptic curve $(\mathcal{E}_L)_\lambda$ is given by (2.4). By basic height properties and $h(\lambda) \leq B$, we find that $h(J)$ is bounded from above independently of P. A result of Poonen [15] states that the set of j-invariants of bounded height coming from elliptic curves with complex multiplication is finite.

So there are only finitely many possibilities for J. By (2.4) the same holds true for λ.

We now prove part (i). We now assume in addition $P \in X^{\mathrm{ta}} \subset X^{\star}$.

We have already assumed N to be large; this will lead to a contradiction as follows. Let $\chi \in \mathbf{Z}^3 \smallsetminus \{0\}$ and $C \subset X \cap G_\chi$ be as in Lemma 2.11. Then $C \neq X$ because otherwise $X \subset G_\chi$ would imply $X^{\mathrm{ta}} = \emptyset$. So $\dim C \leq 1$. General intersection theory implies $\dim C \geq \dim X - 1$. Hence C is an algebraic curve defined over $\overline{\mathbf{Q}}$. Recall that P^σ lies on C for some $\sigma \in \Sigma$. We split up into cases regarding whether $\pi|_C : C \to Y(2)$ is dominant or not.

First we assume $\pi|_C$ is dominant. By Lemma 2.12(i) the algebraic curve C lies in $G_{\chi'} \cap G_{\chi''}$ for independent $\chi', \chi'' \in \mathbf{Z}^3$. But for an appropriate conjugate C' of C we have $P \in C'$ and $C' \subset G_{\chi'} \cap G_{\chi''}$. Therefore, C' is torsion anomalous which contradicts $P \in X^{\mathrm{ta}}$.

Now say $\pi|_C$ is not dominant. This means that C is contained in a single fiber of $\mathcal{E}_L^3 \to Y(2)$. We know from Lemma 2.12(ii) that C is a translate of an algebraic subgroup of a fiber of $\mathcal{E}_L^3$. But C contains P^σ, which is torsion. So C is the translate of an algebraic subgroup by a torsion point. Conjugating, we find that P is on an algebraic curve C' which is the translate of an algebraic subgroup of $(\mathcal{E}_L^3)_\lambda$ by a torsion point.

If $(\mathcal{E}_L)_\lambda$ does not have complex multiplication then $C' \subset G_{\chi'} \cap G_{\chi''}$ for independent $\chi', \chi'' \in \mathbf{Z}^3$. This means that C' is a torsion anomalous subvariety of X as in part (i) of the definition. But $P \in C'$, contradicting our hypothesis $P \in X^{\mathrm{ta}}$.

Finally, suppose $(\mathcal{E}_L)_\lambda$ has complex multiplication. Then C' is a torsion anomalous subvariety as in part (iii) of the definition. As above we arrive at a contradiction. □

3. Torsion anomalous subvarieties

The results in this section are formulated using the Weierstrass family of elliptic curves. Recall that the base S is the algebraic surface given by (1.2). The fiber above $(a, b) \in S$ is an elliptic curve with j-invariant $j(a, b) = 2^8 3^3 a^3/(4a^3 + 27b^2)$. We regard $j : S \to \mathbf{A}^1$ as a morphism.

Recall that $\mathcal{E}^3$ is a five-dimensional non-singular irreducible variety. By abuse of notation, π denotes both structure morphisms $\mathcal{E} \to S$ and $\mathcal{E}^3 \to S$. Both are proper morphisms. It is straightforward to check that the 123-surface X is irreducible.

In Section 2 we defined torsion anomalous subvarieties of an irreducible algebraic surface in $\mathcal{E}_L^3$. The analog definition for a surface in $\mathcal{E}^3$ is somewhat more involved. This is due to the fact that fibers of $\mathcal{E}^3 \to S$ are isomorphic along algebraic curves in S where j is constant. Before coming to the definition we state an elementary lemma which is used through this section. It enables us to pass from the Weierstrass to the Tate model of an elliptic curve.

If K is a field then $K^\times = K \smallsetminus \{0\}$.

Lemma 3.1. *Let K be a field of characteristic not equal to 2 or 3. Say we are given two elliptic curves*

$$\begin{aligned} E &: y^2 = x^3 + ax + b \quad \text{and} \\ E' &: y^2 + xy = x^3 + a'x + b' \end{aligned} \tag{3.1}$$

with $a, b, a', b' \in K$ that are isomorphic over K. Then there exists $w \in K^\times$ such that

$$(x, y) \mapsto \left(w^2 x - \frac{1}{12}, w^3 y - \frac{1}{2} w^2 x + \frac{1}{24} \right)$$

determines an isomorphism $E \to E'$ with

$$w^4 a = a' - \frac{1}{48} \quad \text{and} \quad w^6 b = -\frac{1}{12} a' + b' + \frac{1}{864}. \tag{3.2}$$

Proof. This follows from the basic theory of elliptic curves [19]. □

Now we come to the auxiliary construction needed for the definition of torsion anomalous subvarieties. Let $A \subset \mathcal{E}_L^3$ be an irreducible closed subvariety such that $j \circ \pi|_A$ is constant with value $J \in \mathbf{C}$. Then $\pi(A)$ is either a point or an irreducible algebraic curve.

We assume the latter for the moment and set $C = \pi(A)$. We take the coordinates a and b of S as elements in the function field $\mathbf{C}(C)$ of C. Then $4a^3(J - 1728) + 27b^2 J = 0$. So $\mathbf{C}(a, b)$ is a rational function field generated by some $t \in \mathbf{C}(C)$. We may assume

$$(a, b) = \begin{cases} (0, t) & : \quad \text{if } J = 0, \\ (t, 0) & : \quad \text{if } J = 1728, \\ (t^2, \zeta t^3) & : \quad \text{if } J \neq 0, 1728 \text{ for some } \zeta \in \mathbf{C}^\times. \end{cases} \tag{3.3}$$

The equation $y^2 = x^3 + ax + b$ defines an elliptic curve E over $\mathbf{C}(t)$. By the basic theory, there is an elliptic curve E' as in (3.1) with $a', b' \in \mathbf{C}$ and j-invariant J. Now E and E' are isomorphic over an algebraic closure $\overline{\mathbf{C}(t)}$ of $\mathbf{C}(t)$ as they share a common j-invariant. Lemma 3.1 provides $w \in \overline{\mathbf{C}(t)}^\times$ and an isomorphism between E and E'. We regard E' as an elliptic curve defined over $\mathbf{C}$. The isomorphism may be taken as an algebraic map on $\pi^{-1}(C)$ with image E'^3. We let A' denote the Zariski closure of the image of A in E'^3.

If $\pi(A)$ is a point, then we take $A' = A$ regarded as a subvariety of the Abelian variety $E'^3 = \pi^{-1}(\pi(A))$.

Let A be an arbitrary irreducible closed subvariety of an algebraic surface in $\mathcal{E}^3$. Then A is called torsion anomalous with respect to the given surface

(i) if $\dim A = 1$ and two independent integral relations hold on A,
(ii) or if $\dim A = 2$ and one non-trivial integral relation holds on A,

(iii) or if $\dim A \geq 1$ and $j \circ \pi|_A$ is constant and equal to the j-invariant of an elliptic curve with complex multiplication such that, in the notation above, A' is an irreducible component of an algebraic subgroup of E'^3.

Proposition 2.1 contained a finiteness statement on the torsion points outside the torsion anomalous locus of a surface in $\mathcal{E}_L^3$. The torsion anomalous subvarieties of the 123-surface will cause no problems.

Proposition 3.2. *The* 123*-surface contains no torsion anomalous subvarieties.*

3.1. Constant j-invariant

As a warm-up for the proof of Theorem 1.1 we show the following weaker version. An algebraic curve in the 123-surface on which j is constant contains only finitely many torsion points. We will use this statement in the proof of Proposition 3.2.

Lemma 3.3. *Let $A \subset X$ be an irreducible closed subvariety such that $j \circ \pi|_A$ is constant. Then A contains only finitely many torsion points and A is not a torsion anomalous subvariety as in part* (iii) *of the definition.*

Proof. We may assume $\dim A \geq 1$. We remark that A and $\pi(A) = C$ are algebraic curves since $\pi|_X$ is dominant and has finite fibers.

Let $J \in \mathbf{C}$ be said j-invariant. We let w, t, A', and E' be as in the auxiliary construction before the definition of anomalous subvarieties. We also consider a and b as elements in $\mathbf{C}(t)$.

We note that $w \notin \mathbf{C}$, indeed, otherwise a, b would be constant as well by (3.2). Using (3.3) we find that $1 + a + b \in \mathbf{C}(t)$ has odd degree. Therefore, there is a non-trivial valuation ord of $\mathbf{C}(t)$ with $\mathrm{ord}(1 + a + b)$ positive and odd. Using (3.3) again one finds $\mathrm{ord}(t) = 0$. Because $a', b' \in \mathbf{C}$ we can deduce $\mathrm{ord}(w) = 0$ from (3.2). Therefore, $\mathbf{C}(w, t)/\mathbf{C}(t)$ is unramified above ord. Since $\{(1, 1, 1), (8, 2, 1), (27, 3, 1)\}$ is linearly dependent we must have $\mathrm{ord}(8+2a+b) = 0$ or $\mathrm{ord}(27 + 3a + b) = 0$. For simplicity say the former holds; the argument below is readily modified in the latter case. We set $K = \mathbf{C}(y_2, w, t)$, then $K/\mathbf{C}(t)$ is unramified above ord. We extend this valuation to K and note that $K(y_1)/K$ is ramified. Because $y_1^2 \in K$ the extension $K(y_1)/K$ is of degree 2 and there is an automorphism σ of $K(y_1)/K$ with $\sigma(y_1) = -y_1$.

For $i \in \{1, 2, 3\}$ we have a point $(i, y_i) \in E(\overline{\mathbf{C}(t)})$. Its image in $E'(\overline{\mathbf{C}(t)})$ under the isomorphism coming from Lemma 3.1 is

$$\left(w^2 i - \frac{1}{12}, w^3 y_i - \frac{1}{2} w^2 i + \frac{1}{24}\right). \tag{3.4}$$

We may regard w, $y_{1,2,3}$ as rational functions on a ramified cover of A. The three points (3.4) determine a rational map from this cover to E'^3. Then A' is the Zariski closure of its image. If A contains infinitely torsion points then so does A'. We use the Manin-Mumford Conjecture for Abelian varieties, a result first proved by Raynaud [16]. It implies that A' is an irreducible component of an algebraic subgroup

of E'^3. In particular, there are endomorphisms α, β of E', not both zero, such that $\alpha(P_1) = \beta(P_2)$ for all $(P_1, P_2, P_3) \in A'$. This relation continues to hold generically, *i.e.* $\alpha(P_1') = \beta(P_2')$ with $P_i' = (w^2 i - 1/12, w^3 y_i - w^2 i/2 + 1/24) \in E(\overline{\mathbf{C}(t)})$. Because σ commutes with all endomorphisms of E', which are defined over $\mathbf{C}$, we get

$$\begin{aligned} -\beta(P_2') = -\alpha(P_1') &= \alpha(w^2 - 1/12, -w^3 y_1 - w^2/2 + 1/24) = \alpha(P_1')^\sigma \\ &= \beta(P_2')^\sigma = \beta(P_2'). \end{aligned}$$

Therefore, $2\beta(P_2') = 0$. So one of P_1', $P_2' \in E'(\overline{\mathbf{C}(t)})$ is a torsion point. But these torsion points are defined over $\mathbf{C}$ and hence $w \in \mathbf{C}$. This contradicts the fact that w is non-constant.

So A contains only finitely many torsion points. Because an algebraic subgroup of an Abelian variety contains a Zariski dense set of torsion points we also conclude that A is not torsion anomalous as in part (iii) of the definition. □

3.2. Tate curves

In this subsection we collect some basic facts on Tate curves. A general reference is Chapter V of Silverman's book [18] or Roquette's book [17].

Let K_v be a field, complete with respect to a discrete valuation $v : K_v \to \mathbf{Z} \cup \{+\infty\}$ which we assume to be surjective. If $q \in K_v^\times$ with $v(q) > 0$ then the Weierstrass equation

$$y^2 + xy = x^3 + a_4(q)x + a_6(q) \tag{3.5}$$

defines the Tate curve E_q where

$$a_4 = -\sum_{n\geq 1} \frac{n^3 q^n}{1-q^n} \quad \text{and} \quad a_6 = -\frac{1}{12}\sum_{n\geq 1} \frac{(5n^3+7n^5)q^n}{1-q^n}$$

converge in K_v, *cf.* [18, Theorem V 3.1]. By this theorem and Remark V 3.1.2 *ibid.*, *cf.* Roquette's work cited above, there exists a surjective homomorphism of groups

$$\phi : K_v^\times \to E_q(K_v)$$

with kernel $q^{\mathbf{Z}}$, the infinite cyclic subgroup of $K_v^\times$ generated by q.

We follow a convenient convention and represent points of $E_q(K_v) \setminus \{0\}$ using affine coordinates.

Equation (3.5) has coefficients in the ring of integers of K_v and is minimal. Let L be the residue field of K_v. The reduction $\widetilde{E_q}$ of E_q is an irreducible projective curve defined over L. We have the reduction map red : $E_q(K_v) \to \widetilde{E_q}(L)$. The set of non-singular points of $\widetilde{E_q}(L)$ carries a natural Abelian group structure. We define

$$E_q(K_v)_0 = \{P \in E_q(K_v);\ \text{red}(P) \text{ is non-singular on } \widetilde{E_q}\}.$$

This is a subgroup of finite index of $E_q(K_v)$ and $\mathrm{red}|_{E_q(K_v)_0}$ is a homomorphism of groups.

The Tate uniformization ϕ lets us do calculations explicitly on Tate curves.

Lemma 3.4. *Let $P \in E_q(K_v)_0 \smallsetminus \{0\}$. There is a unique $\tilde{u} \in K_v$ with $v(\tilde{u}) = 0$ and $\phi(\tilde{u}) = P$. Moreover, if $u \in L$ is the reduction of $\tilde{u}$ then $u \neq 0$ and*

(i) *either $u = 1$ and $\mathrm{red}(P) = 0$,*
(ii) *or $u \neq 1$ and $\mathrm{red}(P) = \left(\frac{u}{(1-u)^2}, *\right) \neq 0$.*

Proof. There is precisely one $\tilde{u} \in K_v^\times \smallsetminus q^{\mathbf{Z}}$ with $0 \leq v(\tilde{u}) < v(q)$ and $\phi(\tilde{u}) = (x, y) = P$. By [18, Lemma V 4.1.1] we have $v(x) \leq 0$ because $P \in E_q(K_v)_0$; we remark that the proof of this lemma involves only formal properties of the valuation on K_v and hence holds for any valued field.

The homomorphism ϕ is explicitly given in [18, Theorem V 3.1] as

$$\phi(\tilde{u}) = \left(\sum_{n \in \mathbf{Z}} \frac{q^n \tilde{u}}{(1 - q^n \tilde{u})^2} - 2 \sum_{n \geq 1} \frac{n q^n}{1 - q^n}, \sum_{n \in \mathbf{Z}} \frac{q^{2n} \tilde{u}^2}{(1 - q^n \tilde{u})^3} + \sum_{n \geq 1} \frac{n q^n}{1 - q^n} \right)$$

because $\tilde{u} \notin q^{\mathbf{Z}}$. All terms in the sum for x have positive valuation except possibly $\frac{q^n \tilde{u}}{(1-q^n \tilde{u})^2}$ for $n = 0$. A similar remark holds for y. We can write

$$P = \left(\frac{\tilde{u}}{(1 - \tilde{u})^2} + x', \frac{\tilde{u}^2}{(1 - \tilde{u})^3} + y' \right) \quad \text{with} \quad v(x') > 0 \quad \text{and} \quad v(y') > 0. \tag{3.6}$$

Since $v(x) \leq 0$ we must have $v(\tilde{u}) \leq 2v(1 - \tilde{u})$. This inequality implies $v(\tilde{u}) = 0$. The reduction u of $\tilde{u}$ is thus non-zero in the residue field L.

If $v(1 - \tilde{u}) > 0$, then $u = 1$ in L. The orders satisfy

$$v(x) = -2v(1 - \tilde{u}) \quad \text{and} \quad v(y) = -3v(1 - \tilde{u}).$$

In particular, $y \neq 0$ and in projective coordinates we have $P = [x/y : 1 : 1/y]$ with $v(x/y) = v(1 - \tilde{u}) > 0$ and $v(1/y) = 3v(1 - \tilde{u}) > 0$. Therefore, $\mathrm{red}(P) = 0$ and we are in case (i).

On the other hand, if $v(1 - \tilde{u}) \leq 0$, then $v(1 - \tilde{u}) = 0$ and so $u \neq 1$. From (3.6) we see that x reduces to $u/(1 - u)^2$ in the L. We are in case (ii). □

3.3. Function fields

Let K be the function field of an irreducible algebraic curve defined over $\mathbf{C}$. Let $a, b \in K$ with $4a^3 + 27b^2 \neq 0$. Then

$$y^2 = x^3 + ax + b$$

determines an elliptic curve E defined over K.

After replacing K by a finite extension we have points

$$P_1 = (1, *) \in E(K), \quad P_2 = (2, *) \in E(K), \quad \text{and} \quad P_3 = (3, *) \in E(K).$$

The choice of sign of the second coordinate will be irrelevant. After again passing to a finite extension of K we may assume that E has either good or multiplicative reduction at all places of K. Multiplicative reduction is automatically split because the residue field $\mathbf{C}$ is algebraically closed.

For any place v of K we let K_v denote the completion of K with respect to v. We identify v with the corresponding surjective valuation $K_v \to \mathbf{Z} \cup \{+\infty\}$. We define a finite (possibly empty) set

$$S = \{\text{places of } K \text{ where } E \text{ has bad reduction}\}.$$

If $v \in S$, then E is isomorphic over K_v to the Tate curve E_{q_v} for some $q_v \in K_v^\times$ with $v(q_v) > 0$. Let $f_v : E \to E_{q_v}$ be an isomorphism as in Lemma 3.1. If $v \notin S$, then E is isomorphic over K_v to an elliptic curve E_v given by the equation $y^2 + xy = x^3 + a'x + b'$ with a', b' integers in K_v and with good reduction. Let $f_v : E \to E_v$ be an isomorphism given by said lemma. To unify notation we sometimes write $E_v = E_{q_v}$ if $v \in S$.

Lemma 3.5. *Let $v \in S$ and $i, j \in \{1, 2, 3\}$ with $i \neq j$. If $f_v(P_i) \notin E_v(K_v)_0$, then*

$$\operatorname{red} f_v(P_j) = \left(\frac{1}{12}\left(\frac{j}{i} - 1\right), *\right) \in \widetilde{E_v}(\mathbf{C}) \quad \textit{and} \quad f_v(P_j) \in E_v(K_v)_0.$$

Proof. The isomorphism f_v is given on the affine part of E by

$$(x, y) \mapsto \left(w^2 x - \frac{1}{12}, *\right).$$

for some $w \in K_v^\times$. The reduction $\widetilde{E_v}$ is determined by the Weierstrass equation $y^2 + xy = x^3$ and $(0, 0)$ is its only singular point. By hypothesis, $f_v(P_i)$ reduces to $(0, 0)$. Therefore, $v(w^2 i - 1/12) > 0$. Since $i \neq 0$ we find $v(w^2 - 1/(12i)) > 0$. In other words, w^2 reduces to $1/(12i)$ at v. So $w^2 j - 1/12$ reduces to $(j/i - 1)/12$ at v and this is the first coordinate of red $f_v(P_j)$. Finally, because $i \neq j$ we have $f_v(P_j) \in E_v(K_v)_0$. □

For $i \in \{1, 2, 3\}$ we define the finite (possibly empty) set

$$S_i = \{v \in S;\ f_v(P_i) \notin E_v(K_v)_0\}.$$

For a finite sequence $P, \ldots, Q \in E(K)$ we set $\rho(P, \ldots, Q)$ to be the rank of the $\mathbf{Z}$-submodule of $E(K)$ generated by $P, \ldots, Q$.

Lemma 3.6. *Suppose $\rho(P_1, P_2, P_3) \leq 1$. Then $S_1 = S_2 = \emptyset$.*

Proof. Say $i \in \{1, 2\}$. Assuming the existence of $v \in S_i$ we will eventually arrive at a contradiction.

Let us fix j and k with $\{i, j, k\} = \{1, 2, 3\}$ and $j < k$. By Lemma 3.5 we find

$$\operatorname{red} f_v(P_j) = \left(\frac{1}{12}\left(\frac{j}{i} - 1\right), *\right) \neq 0, \quad \operatorname{red} f_v(P_k) = \left(\frac{1}{12}\left(\frac{k}{i} - 1\right), *\right) \neq 0,$$

and $f_v(P_j)$, $f_v(P_k) \in E_v(K_v)_0 \smallsetminus \{0\}$.

We apply Lemma 3.4 to $f_v(P_j)$ and $f_v(P_k)$ and obtain elements $\tilde{u} \in K_v$ and $\tilde{u}' \in K_v$, respectively. We are in case (ii) of said lemma, so $u \neq 1$ and $u' \neq 1$ for the reductions of $\tilde{u}$ and $\tilde{u}'$, respectively. These reductions satisfy

$$\frac{u}{(1-u)^2} = \frac{1}{12}\left(\frac{j}{i} - 1\right), \quad \text{and} \quad \frac{u'}{(1-u')^2} = \frac{1}{12}\left(\frac{k}{i} - 1\right). \tag{3.7}$$

Since $\rho(P_1, P_2, P_3) \leq 1$ we have $\rho(P_j, P_k) \leq 1$. So there are $M, N \in \mathbf{Z}$, not both zero, with $[M](P_j) = [N](P_k)$. Using the Tate uniformization, this relation reads $\phi(\tilde{u}^M) = [M](f_v(P_j)) = [N](f_v(P_k)) = \phi(\tilde{u}'^N)$. So $\tilde{u}^M \tilde{u}'^{-N} \in q^{\mathbf{Z}}$. Since $\tilde{u}$ and $\tilde{u}'$ have valuation zero, we find $\tilde{u}^M = \tilde{u}'^N$ and in particular, $u^M = u'^N$.

The contradiction now follows by simply evaluating u and u' in the two possible cases $i = 1, 2$ using (3.7). Rewriting these identities gives

$$u^2 + 2\frac{5i + j}{i - j}u + 1 = 0 \quad \text{and} \quad u'^2 + 2\frac{5i + k}{i - k}u' + 1 = 0$$

with solutions

$$(u, u') = \begin{cases} (7 \pm 4\sqrt{3}, 4 \pm \sqrt{15}) & : \text{if } (i, j, k) = (1, 2, 3), \\ (-11 \pm 2\sqrt{30}, 13 \pm 2\sqrt{42}) & : \text{if } (i, j, k) = (2, 1, 3). \end{cases}$$

In both cases u, u' are algebraic units with $\mathbf{Q}(u) \cap \mathbf{Q}(u') = \mathbf{Q}$. Hence $u^M = u'^N \in \{\pm 1\}$, the algebraic units of $\mathbf{Q}$. So one among u, u' is a root of unity. This is impossible for the totally real u and u'; the lemma follows. □

One can go a bit further and also show $S_3 = \emptyset$. But this will not be necessary.

If v is any place of K, then λ_v denotes the Néron local height on any elliptic curve over K_v, *cf.* Chapter VI [18]. It does not depend on the choice of a model of the elliptic curve. For a place v of bad reduction we will use the Tate curve $E_{q_v} = E_v$ to calculate λ_v. There is an explicit formula for λ_v restricted to $E_v(K_v)_0 \smallsetminus \{0\}$ given by [18, Theorem VI 4.1]. We can use it to handle $\lambda_v(P_1)$ and $\lambda_v(P_2)$ because $S_1 = S_2 = \emptyset$.

Lemma 3.7. *Suppose $\rho(P_1, P_2, P_3) \leq 1$. If v is any place of K, then*

$$\lambda_v(P_1) = \lambda_v(P_2).$$

Proof. Let v be any place of K. Recall that $f_v : E \to E_v$ is an isomorphism of elliptic curves over K. By Lemma 3.6 the points $f_v(P_1)$ and $f_v(P_2)$ reduce to a non-singular point.

Since $P_{1,2} \neq 0$ we may use Theorem VI 4.1 to evaluate

$$\lambda_v(P_1) = \lambda_v(f_v(P_1)) = \frac{1}{2}\max\{0, -v(x_1)\} + \frac{1}{12}v(\Delta_v) \quad \text{and}$$
$$\lambda_v(P_2) = \lambda_v(f_v(P_2)) = \frac{1}{2}\max\{0, -v(x_2)\} + \frac{1}{12}v(\Delta_v)$$

where x_1 and x_2 are the first coordinates of $f_v(P_1)$ and $f_v(P_2)$, respectively, and Δ_v is the local discriminant of E_v. We remark that x_1 and x_2 depend on v.

By Lemma 3.1, the isomorphism f_v is determined by some $w \in K_v^\times$. So

$$x_1 = w^2 - \frac{1}{12} \quad \text{and} \quad x_2 = 2w^2 - \frac{1}{12}.$$

We split up into two cases.

First, let us suppose $v(w) \geq 0$. Then $v(x_1) \geq 0$ and $v(x_2) \geq 0$ by the ultrametric triangle inequality. So we have

$$\lambda_v(P_1) = \lambda_v(P_2) = \frac{1}{12}v(\Delta_v).$$

Second, we assume $v(w) < 0$. In this case the ultrametric triangle inequality yields $v(x_1) = v(x_2) = v(w^2)$. Therefore,

$$\lambda_v(P_1) = \lambda_v(P_2) = -\frac{1}{2}v(w^2) + \frac{1}{12}v(\Delta_v). \qquad \square$$

Now we will show that E has good reduction everywhere under the hypothesis of the previous lemma. This is done by a global argument using local data from the last lemma.

The Néron-Tate or canonical height is defined for $P \in E(K) \smallsetminus \{0\}$ as $\hat{h}(P) = \sum_v \lambda_v(P)$ where the sum runs over all places of K; for $P = 0$ we set $\hat{h}(P) = 0$.

Lemma 3.8. *Suppose $\rho(P_1, P_2, P_3) \leq 1$. Then $S = \emptyset$.*

Proof. First we show that there exists $Q \in E(K) \smallsetminus \{0\}$ with $\hat{h}(Q) = 0$ and $f_v(Q) \in E_v(K_v)_0$ for all $v \in S$. If $\hat{h}(P_1) = 0$ then we take $Q = P_1$ and our claim follows because $S_1 = \emptyset$. So say $\hat{h}(P_1) \neq 0$. By Lemma 3.7 the global heights coincide $\hat{h}(P_1) = \hat{h}(P_2)$. Since $\rho(P_1, P_2) \leq 1$ there are $M, N \in \mathbf{Z}$ not both zero with $[M](P_1) = [N](P_2)$. The Néron-Tate height is quadratic, hence $M^2\hat{h}(P_1) = N^2\hat{h}(P_2) = N^2\hat{h}(P_1)$ and thus $M^2 = N^2 \neq 0$. So $[M](P_1 \pm P_2) = 0$ and therefore $\hat{h}(Q) = 0$ with $Q = P_1 \pm P_2$. Clearly, $Q \neq 0$ and $f_v(Q) \in E_v(K_v)_0 \smallsetminus \{0\}$ for all $v \in S$ because $S_1 = S_2 = \emptyset$.

Now that we have found Q we can easily conclude the proof. Indeed, the Néron local heights of Q can be evaluated by Theorem VI 4.1. Just as in the proof of Lemma 3.7, we use our model with good reduction E_v if $v \notin S$ and the Tate curve E_{q_v} otherwise. The Néron local heights are non-negative so they all vanish. But a Néron local height coming from a place of bad reduction contributes by a positive term through the vanishing order of the local discriminant. Therefore, $S = \emptyset$. □

Lemma 3.9. *We have* $\rho(P_1, P_2, P_3) \geq 2$.

Proof. We assume $\rho(P_1, P_2, P_3) \leq 1$ and deduce a contradiction.

For a certain reordering (i, j, k) of $(1, 2, 3)$ and fixed $M, N, N' \in \mathbf{Z}$ with $M \neq 0$ we have

$$[N](P_i) = [M](P_j) \quad \text{and} \quad [N'](P_i) = [M](P_k). \tag{3.8}$$

By the previous lemma we have $S = \emptyset$. So the j-invariant of E is a constant $2^8 3^3 a^3/(4a^3 + 27b^2) \in \mathbf{C}$.

We may reformulate our situation as follows. There exists an irreducible algebraic curve C in the 123-surface for which $j|_C$ is constant and where relations as in (3.8) hold.

We will prove below that there are infinitely many points on C where the i-th coordinate is torsion. The relations (3.8) and Lemma 3.3 lead to a contradiction.

As in the argument stated after Lemma 3.1 there is an elliptic curve E' given by (3.1) with $a', b' \in \mathbf{C}$ and an isomorphism $E \to E'$ determined by some $w \neq 0$ in an algebraic closure of K satisfying (3.2). We remark $w \notin \mathbf{C}$ because $\mathbf{C}(a, b)$ is not algebraic over $\mathbf{C}$. We may regard w as a non-constant algebraic function on C. The image of P_i under this isomorphism is $(w^2 i - 1/12, *)$. We may regard it as an algebraic curve in E'. Now $w^2 i - 1/12$ attains, up-to finitely many exceptions, any complex value. In particular, it attains the first coordinate of a torsion point of E' infinitely often. This gives the infinitely many points on C with the desired property. □

3.4. There are no torsion anomalous subvarieties

We now prove Proposition 3.2. First we show that X does not contain any torsion anomalous subvarieties as in part (i) of the definition. Let $C \subset X$ be an irreducible algebraic curve. The coordinate functions $a, b : S \to \mathbf{A}^1$ induce rational functions on C. They determine an elliptic curve E defined over $\mathbf{C}(a, b)$ given in Weierstrass $y^2 = x^3 + ax + b$. We consider three points $P_{1,2,3}$ as in the previous section. Then $\rho(P_1, P_2, P_3) \geq 2$ by Lemma 3.9. This means that two independent relations cannot simultaneously hold on C. In other words, C cannot be torsion anomalous.

Now we show that X cannot contain a torsion anomalous surface as in part (ii) of the definition. Assuming the contrary, X is a torsion anomalous subvariety of itself. So there is $(\alpha, \beta, \gamma) \in \mathbf{Z}^3 \smallsetminus \{0\}$ with

$$[\alpha]\left(1, \sqrt{1 + a + b}\right) + [\beta]\left(2, \sqrt{8 + 2a + b}\right) + [\gamma]\left(3, \sqrt{27 + 3a + b}\right) = 0$$

for all $(a, b) \in S$. We suppose first $\beta \neq 0$ or $\gamma \neq 0$. There is an irreducible algebraic curve $C \subset X$ on which $1 + a + b = 0$ holds identically. So the first coordinate in $\mathcal{E}$ of a point in C has order 2. In addition to (α, β, γ), a second and independent relation $(2, 0, 0)$ holds on C. Therefore, C is torsion anomalous as in part (i) of the definition. This contradicts the already proven part of the proposition. If $\beta = \gamma = 0$ we also conclude a contradiction by a similar argument using a curve on which $8 + 2a + b = 0$ holds.

Finally, by Lemma 3.3 the surface X cannot contain any torsion anomalous subvarieties as in part (iii) of the definition. □

4. Proof of the main result

Recall that $\mathcal{E}_L$ is the Legendre family of elliptic curves over $Y(2) = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ and that $\mathcal{E}$ is the Weierstrass family of elliptic curves over $S = \{(a, b);\ 4a^3 + 27b^2 \neq 0\}$.

Let X_L be an irreducible closed algebraic surface in $\mathcal{E}_L^3$. In Section 2 we introduced the notion of a torsion anomalous subvariety of X_L. We call an irreducible closed subvariety of X_L a strongly torsion anomalous subvariety of X_L if it satisfies (i) or (ii) in the definition of a torsion anomalous subvariety. We write X_L^{sta} for $X_L \setminus \bigcup_A A$, here A runs over all strongly torsion anomalous subvarieties of X_L.

Let $X \subset \mathcal{E}^3$ be the 123-surface. We recall that is irreducible. We start off by using it to construct an algebraic surface X_L in the Legendre family $\mathcal{E}_L^3$. We first introduce a covering S' of S by setting

$$\begin{aligned} S' = \{(a, b, e_1, e_2, e_3, t, r) \in S \times \mathbf{A}^5;\ & e_i^3 + ae_i + b = 0 \text{ for } 1 \leq i \leq 3, \\ & (e_2 - e_1)^2(e_3 - e_2)^2(e_1 - e_3)^2 t = 1, \\ & e_2 - e_1 = r^2\}. \end{aligned}$$

Note that $(e_2 - e_1)^2(e_3 - e_2)^2(e_1 - e_3)^2 = -(4a^3 + 27b^2)$ is invertible in the coordinate ring of S. So t as well as $e_{1,2,3}$ and r are integral over the coordinate ring of S. In geometric terms this means that the natural projection morphism $S' \to S$ is finite. It is also surjective. The irreducible components of S' have dimension 2. We obtain a new Abelian scheme $\mathcal{E}'^3 \to S'$ by taking the fibered product of $\mathcal{E}^3 \to S$ with $S' \to S$. Let $f : \mathcal{E}'^3 \to \mathcal{E}^3$ be the induced morphism. It is finite and surjective since these properties are preserved under base change. Since f is a closed surjective morphism and X is irreducible, the pre-image $f^{-1}(X)$ contains an irreducible component X' with $f(X') = X$. We must have $\dim X' = 2$ by standard results in dimension theory, *cf.* Exercise II 3.22 [7].

We define a morphism $S' \to Y(2)$ by $(a, b, e_1, e_2, e_3, t, r) \mapsto \frac{e_3 - e_1}{e_2 - e_1}$. Then

$$(x, y, a, b, e_1, e_2, e_3, r) \mapsto \left(\frac{x - e_1}{e_2 - e_1}, \frac{y}{r^3}, \frac{e_3 - e_1}{e_2 - e_1} \right)$$

induces a morphism $g : \mathcal{E}'^3 \to \mathcal{E}_L^3$. Restricted to a fiber of $\mathcal{E}'^3 \to S'$, it gives an isomorphism between Weierstass and Legendre models of an elliptic curve. Moreover, it fits into the commutative diagram

$$\begin{array}{ccc} \mathcal{E}'^3 & \xrightarrow{g} & \mathcal{E}_L^3 \\ \downarrow & & \downarrow \\ S' & \longrightarrow & Y(2). \end{array}$$

A straight-forward verification shows that $g|_{X'} : X' \to \mathcal{E}_L^3$ has finite fibers. The image $g(X')$ is constructable in $\mathcal{E}_L^3$ by Chevalley's Theorem. Let X_L be the Zariski closure of $g(X')$ in $\mathcal{E}_L^3$. Then X_L is irreducible and from dimension theory we conclude $\dim X_L = 2$.

Next, let us show that X_L does not contain any torsion anomalous subvariety as in part (ii) of the definition. Indeed, otherwise a non-trivial integral relation would hold identically on X_L. Any such integral relation would hold on X' and also on X because g is fiberwise the cube of an isomorphism of elliptic curves. But no non-trivial integral relation holds on X by Proposition 3.2.

Next, we claim that X_L contains only finitely many torsion anomalous subvarieties as in part (i) of the definition. We also claim that each such subvariety intersects $g(X')$ in only finitely many points.

Let $C \subset X_L$ be such a torsion anomalous subvariety. Then C is an algebraic curve and there are two possibilities.

Say first that $g|_{X'}^{-1}(C)$ has positive dimension. Then it contains an irreducible algebraic curve C'. Two independent integral relations hold on C. These must continue to hold on C'. Finally, these relations also hold on $f(C) \subset X$. Latter must have dimension 1 because f is a finite morphism. We have found a torsion anomalous subvariety in X and so a contradiction to Proposition 3.2.

Now say $g|_{X'}^{-1}(C)$ has dimension 0. This implies that $C \cap g(X')$ is finite. Because C is irreducible it follows that C is in the Zariski closure of $X_L \smallsetminus g(X')$ in X_L. This closure is a finite union of points and irreducible algebraic curves. Therefore, it contains C as an irreducible component. This leaves only finitely many possibilities for C and our claim above holds.

We have proved that $g(X') \cap (X_L \smallsetminus X_L^{\mathrm{sta}})$ is finite.

Say $P_1, P_2, \ldots$ is a sequence of distinct torsion points on X. We will deduce a contradiction. Since $f|_{X'} : X' \to X$ is surjective we find a pre-image, which must be torsion, of each P_i in X'. Because $g|_{X'}$ has finite fibers, $g(X')$ contains infinitely many torsion points $Q_1, Q_2, \ldots$.

By the discussion above, only finitely many of the $Q_1, Q_2, \ldots$ can lie on $X_L \smallsetminus X_L^{\mathrm{sta}}$. We remove these from our sequence and suppose $Q_i \in X_L^{\mathrm{sta}}$. By Proposition 2.1(i), only finitely many of the remaining Q_i can lie on X_L^{ta}. We remove these as well. So $Q_i \in X_L^{\mathrm{sta}} \smallsetminus X_L^{\mathrm{ta}}$.

All Q_i are on a torsion anomalous subvariety of X_L as in part (iii) of the definition of torsion anomalous. In particular, each Q_i is in some fiber with complex

multiplication. We use Proposition 2.1(ii). After passing to an infinite subsequence, the Q_i are all in the same fiber of $\mathcal{E}_L^3 \to Y(2)$. Let $J \in \mathbf{C}$ be the j-invariant of a factor of this fiber. Each of the corresponding P_i lies in the cube of an elliptic curve with j-invariant J. By passing to a infinite subsequence a last time we find infinitely many torsion points on an irreducible algebraic curve in X on which the j-invariant is constant. This contradicts Lemma 3.3 and completes the proof of Theorem 1.1. □

References

[1] J. AX, *Some topics in differential algebraic geometry I: Analytic subgroups of algebraic groups*, Amer. J. Math. **94** (1972), 1195–1204.

[2] D. BERTRAND, *Extensions de D-modules et groupes de Galois différentiels*, In: "p-adic Analysis" (Trento, 1989), Lecture Notes in Math., Vol. 1454, Springer, Berlin, 1990, 125–141.

[3] D. BERTRAND, *Special points and Poincaré bi-extensions, with an Appendix by Bas Edixhoven*, arXiv:1104.5178v1 (2011).

[4] E. BOMBIERI and W. GUBLER, "Heights in Diophantine Geometry", Cambridge University Press, 2006.

[5] S. DAVID, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory **64** (1997), 104–129.

[6] P. HABEGGER, *Special points on fibered powers of elliptic surfaces*, J. Reine Angew. Math., to appear.

[7] R. HARTSHORNE, "Algebraic Geometry", Springer, 1997.

[8] D. HUSEMÖLLER, "Elliptic Curves", Springer, 2004.

[9] D. W. MASSER and U. ZANNIER, *Torsion points on families of squares of elliptic curves*, Math. Ann. **352** (2012), 453-484.

[10] D. W. MASSER and U. ZANNIER, *Torsion anomalous points and families of elliptic curves*, C. R. Acad. Sci. Paris Sér. I **346** (2008), 491–494.

[11] D. W. MASSER and U. ZANNIER, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), 1677–1691.

[12] J. PILA and A. J. WILKIE, *The rational points of a definable set*, Duke Math. J. **133** (2006), 591–616.

[13] 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), 149–162.

[14] R. PINK, *A Common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang*, preprint (2005), 13 pp.

[15] B. POONEN, *Spans of Hecke points on modular curves*, Math. Res. Lett. **8** (2001), 767–770.

[16] M. RAYNAUD, *Sous-variétés d'une variété abélienne et points de torsion*, In: "Arithmetic and geometry", Vol. I, Progr. Math., Vol. 35, Birkhäuser Boston, Boston, MA, 1983, 327–352.

[17] P. ROQUETTE, "Analytic Theory of Elliptic Functions over Local Fields", Hamburger Mathematische Einzelschriften (N.F.), Heft 1, Vandenhoeck & Ruprecht, Göttingen, 1970.

[18] J. H. SILVERMAN, "Advanced Topics in the Arithmetic of Elliptic Curves", Graduate Texts in Mathematics, Vol. 151, Springer-Verlag, New York, 1994.

[19] J. H. SILVERMAN, "The Arithmetic of Elliptic Curves", Springer, 1986.

[20] L. VAN DEN DRIES, *A generalization of the Tarski-Seidenberg theorem, and some nondefinability results*, Bull. Amer. Math. Soc. (N.S.) **15** (1986), 189–193.
[21] L. VAN DEN DRIES, "Tame Topology and o-minimal Structures", London Mathematical Society Lecture Note Series, Vol. 248, Cambridge University Press, Cambridge, 1998.
[22] B. ZILBER, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. (2) **65** (2002), 27–44.

Technische Universität Darmstadt
Fachbereich Mathematik
Schlossgartenstrasse, 7
64289 Darmstadt, Germany
habegger@mathematik.tu-darmstadt.de