ON THE EXPLICIT TORSION ANOMALOUS CONJECTURE

S. CHECCOLI, F. VENEZIANO, E. VIADA

ABSTRACT. The Torsion Anomalous Conjecture states that an irreducible variety V embedded in a semi-abelian variety contains only finitely many maximal V-torsion anomalous varieties. In this paper we consider an irreducible variety embedded in a produc of elliptic curves. Our main result provides a totally explicit bound for the Néron-Tate height of all maximal V-torsion anomalous points of relative codimension one, in the non CM case, and an analogous effective result in the CM case. As an application, we obtain the finiteness of such points. In addition, we deduce some new explicit results in the context of the effective Mordell-Lang Conjecture; in particular we bound the Néron-Tate height of the rational points of an explicit family of curves of increasing genus.

1. INTRODUCTION

In this article, by *variety* we mean an algebraic variety defined over the algebraic numbers. Equivalently, a variety X is defined by polynomials with coefficients in a number field k, however k will not play any role in our theorems. In addition, we identify $X = X(\overline{\mathbb{Q}})$.

Let G be a semi-abelian variety.

A subvariety $V \subseteq G$ is a *translate*, respectively a *torsion variety*, if it is a finite union of translates of proper algebraic subgroups of G by points, respectively by torsion points.

An irreducible variety $V \subseteq G$ is *transverse*, respectively *weak-transverse*, if it is not contained in any translate, respectively in any torsion variety.

Many important classical results such as, for instance, the Manin-Mumford, the Mordell-Lang, the Bogomolov Conjectures, nowadays theorems, and many open problems, such as the Zilber-Pink Conjecture, investigate the relationship between these geometrical definitions and the arithmetical properties of the variety V.

Recently E. Bombieri, D. Masser and U. Zannier in [BMZ07] introduced the notions of anomalous and torsion anomalous varieties and formulated some general conjectures. Following their work, we give the definition of torsion anomalous varieties. However, unlike [BMZ07], we allow torsion anomalous varieties to be zero dimensional. Like this, we can simplify the formulation of several statements.

Let V be a subvariety of a semi-abelian variety G. We say that an irreducible subvariety Y of V is a V*-torsion anomalous* variety if

(i) Y is an irreducible component of $V \cap (B + \zeta)$ with $B + \zeta$ an irreducible torsion variety of G;

(ii) the dimension of Y is larger than expected, i.e. the codimensions satisfy

$$\operatorname{codim} Y < \operatorname{codim} V + \operatorname{codim} B.$$

We say that $B + \zeta$ is *minimal* for Y if, in addition, it has minimal dimension. The codimension of Y in its minimal $B + \zeta$ is called the *relative codimension* of Y.

We also say that a V-torsion anomalous variety Y is *maximal* if it is not contained in any V-torsion anomalous variety of strictly larger dimension.

2010 *Mathematics Subject Classification.* Primary 11G50, Secondary 14G40.

The Torsion Anomalous Conjecture (TAC) is a natural variant of a conjecture by Bombieri, Masser and Zannier.

Conjecture (TAC)**.** *An irreducible subvariety V of a semi-abelian variety contains only finitely many maximal V-torsion anomalous varieties.*

Clearly, if V is not weak-transverse, then V is itself V-torsion anomalous. In addition, if V is a hypersurface, the only maximal V-torsion anomalous varieties are the maximal torsion varieties contained in V, and they are finitely many by the Manin-Mumford Conjecture. So the TAC is interesting when V is weak-transverse of codimension at least 2.

The Zilber-Pink Conjecture is a special case of the TAC. More precisely, it is equivalent to the TAC restricted only to the V-torsion anomalous varieties that come from an intersection expected to be empty. So the TAC implies, like the Zilber-Pink Conjecture, several other celebrated questions such as the Manin-Mumford and the Mordell-Lang Conjectures. Recent works also highlight links to model theory and to algebraic dynamics, in the context of the Morton Conjectures.

Only the following few cases of the TAC are known: for curves in a product of elliptic curves (Viada [Via08]), in abelian varieties with CM (Rémond [Rém09]) and in a torus (Maurin [Mau08]); for varieties of codimension 2 in a torus (Bombieri, Masser and Zannier [BMZ07]) and in a product of elliptic curves with CM ([CVV14]). Under stronger geometric hypotheses on V, related results are proved by many other authors.

It is proven in several works that, if the height of a set of maximal torsion anomalous points is bounded, then such a set is also finite. So when dealing with points, the obstruction to the TAC is due only to the lack of bounds for their height. This leads us to state the following natural extension of the Bounded Height Conjecture (BHC), formulated by Bombieri, Masser and Zannier [BMZ07].

Conjecture (BHC')**.** *For an irreducible variety V in a semi-abelian variety, the set of maximal V-torsion anomalous points has bounded height.*

Like above, if V is not weak-transverse then there are no maximal V-torsion anomalous points, because they are all contained in V, which is itself V-torsion anomalous.

Some relevant results in this context are due to Habbeger (see [Hab09.a] and [Hab09.b]). His theorems imply the BHC' in tori and abelian varieties, but only for the V-torsion anomalous points not contained in any V-anomalous variety. This condition is stronger than being maximal. In particular for varieties that do not satisfy a geometric condition even stronger than transversality his theorems are saying nothing (in his notations the set V^{oa} is the empty set).

In addition, his results are not effective. Effective theorems are essentially only known for transverse curves in tori and in products of elliptic curves.

In [CVV14] the authors prove the BHC', but only for V-torsion anomalous points of relative codimension one when V is a subvariety of a power of an elliptic curve with CM. The method is effective, however the use of a Lehmer type bound is a deep obstacle when trying to make the result explicit and such a bound is not known in the non CM case.

In this article we are concerned with subvarieties of a power of an elliptic curve, regardless of whether it has CM. From now on the ambient variety G will be E^N, where E is an elliptic curve defined over the algebraic numbers, embedded in $\mathbb{P}_2$ via its Weierstrass equation, and N is a positive integer. We consider on E^N the canonical Néron-Tate height, denoted $\hat{h}$.

The aim of this article is twofold:

- We prove the BHC' and the TAC, for maximal V-torsion anomalous points of relative codimension one. Our method is completely effective.
- In the non CM case, we make our proof explicit, computing all constants and obtaining the only known bounds.

The importance of giving an explicit result is due, for instance, to the implications on the Effective Mordell-Lang Conjecture specified below. More generally, it is well known that an effective TAC implies the Effective Mordell-Lang Conjecture, which has a strong impact in mathematics and it is only known for curves in a torus.

Our main result is:

Theorem 1.1. *Let V be an irreducible variety embedded in E^N. Then the set of maximal V-torsion anomalous points of relative codimension one has effectively bounded Néron-Tate height. If E is non CM the bound is explicit, we have*

$$\hat{h}(P) \leq C_1(N)h(V)(\deg V)^{N-1} + C_2(E,N)(\deg V)^N + C_3(E,N),$$

where

$$C_1(N) = (N!)^N N^{3N-2} \left(\frac{3^{N^2+N+1} 2^{2N^2+3N-1}(N+1)^{N+1}}{(\omega_N \omega_{N-1})^2} \right)^{N-1}$$

$$C_2(E,N) = C_1(N) \left(\frac{3^N \log 2}{2} + 12N \log 2 + N \log 3 + 6N h_{\mathcal{W}}(E) \right)$$

$$C_3(E,N) = \frac{7N^2}{6} \log 2 + \frac{N^2}{2} h_{\mathcal{W}}(E),$$

$\omega_r = \pi^{r/2}/\Gamma(r/2+1)$ is the volume of the euclidean unit ball in $\mathbb{R}^r$, $h(V)$ is the normalised height of V and $h_{\mathcal{W}}(E)$ is the height of the Weierstrass equation of E (see Section 2.2 for the definitions).

The bound of Theorem 1.1 does not depend on the field of definition of V, unlike other bounds in similar contexts. This is central for our applications.

The structure of the proof of Theorem 1.1 does not distinguish CM from non CM elliptic curves. The constants can be computed also in the CM case, however further technical complications due to the structure of the endomorphism ring of E would make the presentation less clear. For simplicity, we prefer to give the explicit computation only in the non CM case.

In [Via09] Theorem 1.1 (and a remark at page 1220 for the CM case), E. Viada proved, that on a weak-transverse variety $V \subseteq E^N$, the maximal V-torsion anomalous points of bounded height are finitely many. Since there are no maximal V-torsion anomalous points if V is not weak-transverse, we immediately deduce the following special case of the TAC.

Corollary 1.2. *An irreducible subvariety V of E^N contains only finitely many maximal V-torsion anomalous points of relative codimension one.*

As an application of our main theorem we obtain new explicit results in the context of the Effective Mordell-Lang Conjecture. In the setting of abelian varieties, the only known effective methods for the Mordell-Lang Conjecture are the Chabauty-Coleman method (see [PM10]) and the Manin-Demjanenko method (see [Ser89], Chapter 5.2). Both methods are quite difficult to apply; for some of the few explicit applications, see [PM10] and [Kul99].

In Section 4 we prove the following explicit theorem on points of rank 1; the rank of a point in E^N is the rank of the subgroup of E generated by its coordinates.

Theorem 1.3. *Let $N \geq 3$ and let $\mathcal{C} \subseteq E^N$ be a weak-transverse curve. The set of points $P \in \mathcal{C}$ of rank ≤ 1 is a set of Néron-Tate height effectively bounded. If E is non CM, we have that*

$$\hat{h}(P) \leq C_1(N) h(\mathcal{C})(\deg \mathcal{C})^{N-1} + C_2(E,N)(\deg \mathcal{C})^N + C_3(E,N),$$

where $C_1(N), C_2(E,N), C_3(E,N)$ are the same as in Theorem 1.1.

If $\mathcal{C}$ is a transverse curve in E^2, then the set of points $P \in \mathcal{C}$ of rank ≤ 1 is a set of Néron-Tate height effectively bounded. If E is non CM, we have that

$$\hat{h}(P) \leq D_1 h(\mathcal{C})(\deg \mathcal{C})^2 + D_2(E)(\deg \mathcal{C})^3 + D_3(E),$$

where

$$\begin{aligned} D_1 &= \frac{2^{64} 3^{40}}{\pi^8} && \approx 2.364 \cdot 10^{34} \\ D_2(E) &= \frac{2^{62} 3^{41}}{\pi^8} \left(71 \log 2 + 4 \log 3 + 30 h_{\mathcal{W}}(E)\right) && \approx (5.319 \cdot h_{\mathcal{W}}(E) + 9.504) \cdot 10^{35} \\ D_3(E) &= \frac{9}{2} h_{\mathcal{W}}(E) + \frac{21}{2} \log 2 && \approx 4.5 \cdot h_{\mathcal{W}}(E) + 7.279. \end{aligned}$$

In particular, in both cases, if k is a field of definition for E and $E(k)$ has rank 1, then all points in $\mathcal{C}(k)$ have Néron-Tate height effectively bounded as above.

The assumption $N \geq 3$ is necessary for weak-transverse curves. Indeed any weak-transverse translate of E^2 (for example $E \times p$ with p not a torsion point) contains infinitely many points of rank 1 and of unbounded height (in the example the points $([n]p, p)$ for all natural n).

Finally, we give explicit bounds in a specific family of curves. This example is particularly interesting as it gives, at least in principle, an algorithm to find all their rational points. Let E be the elliptic curve defined by the equation $y^2 = x^3 + x - 1$; the group $E(\mathbb{Q})$ has rank 1 with generator $g = (1,1)$ (see Section 5). We write

$$\begin{aligned} y_1^2 &= x_1^3 + x_1 - 1 \\ y_2^2 &= x_2^3 + x_2 - 1 \end{aligned}$$

for the equations of E^2 in $\mathbb{P}_2^2$, using affine coordinates $(x_1, y_1) \times (x_2, y_2)$. We have the following theorem, proved in Section 5.

Theorem 1.4. *Let E be the elliptic curve defined above, and consider the family of curves $\{\mathcal{C}_n\}_n$ with $\mathcal{C}_n \subseteq E^2$ defined via the additional equation $x_1^n = y_2$. Then for every $n \geq 1$, if $P \in \mathcal{C}_n(\mathbb{Q})$ we have*

$$\hat{h}(P) \leq 8.253 \cdot 10^{38} (n+1)^3$$

Moreover, writing $P = ([a]g, [b]g)$, the following inequalities hold

$$|a| \leq 7.037 \cdot 10^{19} (n+1)$$

and

$$|b| \leq \left(\frac{3na^2}{2} + 14 \log 2 + 10 \right)^{\frac{1}{2}}.$$

Our explicit results cannot be obtained with the method used in [CVV14], because the Lehmer type bound is not known in the non CM case and anyway there are no published proofs that such a bound is effective. The available proof could possibly be made explicit, but to get reasonable bounds it would be necessary to avoid the use of a complicated descent argument, using instead a much simpler induction, as done for tori by Amoroso and Viada in [AV12]. Nevertheless, even with such improvements, the constants so obtained would be far from being optimal. Probably the dependence on the dimension N could not be improved further than N^{N^N}, which is of one exponential more than our bound.

We now briefly describe the proof-strategy of our main result.

The proof of Theorem 1.1 relies on an approximation process. Let P be a point as in Theorem 1.1; in particular P is a component of $V \cap (B+\zeta)$ for some torsion variety $B+\zeta$. We will replace $B+\zeta$ with an auxiliary translate of the form $H+P$ in such a way that P is still a component of $V \cap (H+P)$, and the degree and height of $H+P$ can be controlled in terms of $\hat{h}(P)$. Using the properties of the height functions, we can in turn control the height of P in terms of the height and degree of $H+P$ itself, and combining carefully these inequalities leads to the desired result.

This construction has been introduced in tori by Habegger [Hab08], Lemma 5. When adopting this strategy for subvarieties of a power of an elliptic curve several complications arise in computing degrees and heights. While the degree of a subtorus can be easily related to the associated matrix, to compute the degree of a subvariety of E^N, it is necessary to fix an embedding of the ambient variety in a projective space and to study how geometrical and arithmetical objects behave under this embedding. This is done in Section 6. Concerning heights, to make the results explicit, we need to work with different heights functions and use explicit versions of several bounds relating the height functions on E^N and those in the projective spaces $\mathbb{P}_2^N$ and $\mathbb{P}_m$. Furthermore, we need to adapt and simplify some of the arguments in [Hab08], in order to keep the constants as small as possible. This is done in Section 7.

The following is an outline of the content of the different sections of this paper.

In Section 2 we recall some classical results such as the Arithmetic Bézout Theorem, the Zhang Inequality and the Minkowski Theorem. We also present the geometrical setting and we give explicit bounds relating different height functions. Moreover, we recall the correspondence between algebraic subgroups of E^N and matrices with coefficients in $\mathrm{End}(E)$.

In Section 3 we give the structure of the proof of Theorem 1.1 while postponing to Sections 6 and 7 the proof of the technical step.

In Section 4 we give the proof of Theorem 1.3 and in Section 5 we prove Theorem 1.4.

In Section 6 we compute explicit bounds for the degree of the rational functions that represent morphisms from E^N to E.

In Section 7, for a torsion anomalous point P of relative codimension one, we give the construction of the auxiliary translate $H+P$, showing how to bound its height and degree.

2. Embeddings, heights and algebraic subgroups

Let E be an elliptic curve without complex multiplication. We fix a Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

with A and B algebraic integers (this hypothesis is not restrictive). As usual, we define

$$\Delta = -16(4A^3 + 27B^2) \qquad j = \frac{-1728(4A)^3}{\Delta}.$$

In this section we give explicit bounds for embeddings of varieties in the projective space. In Subsection 2.1 we compute the degree of E^N as a subvariety of $\mathbb{P}_{3^N-1}$, via the Segre embedding. In Subsection 2.2, we define several height functions, state their relevant properties and give explicit bounds between different heights. We also recall the Arithmetic Bézout Theorem and the Zhang Inequality. In Subsection

2.3 we recall the relations between algebraic subgroups and matrices, degrees and minors.

2.1. **Segre embedding.** Let us consider the composition of maps

$$E^N \hookrightarrow \mathbb{P}_2^N \hookrightarrow \mathbb{P}_{3^N-1}.$$

The first map sends a point $(X_1, \dots, X_N)$ to $((x_1, y_1), \dots (x_N, y_N))$ where (x_i, y_i) are the affine coordinates of X_i in the Weierstrass form of E. The second map is the Segre embedding. When computing heights and degrees of points and subvarieties, we will think them as embedded in $\mathbb{P}_{3^N-1}$ via the previous map.

The degree of a variety $V \subseteq \mathbb{P}_m$, in particular, is the maximal cardinality of a finite intersection $V \cap L$, with L a linear subspace of dimension equal to $\operatorname{codim} V$, the codimension of V. This degree is often conveniently computed as an intersection product.

Let $X(E, N)$ be the variety in $\mathbb{P}_{3^N-1}$ identified with E^N via the Weierstrass form and the Segre embedding. The following lemma computes its degree.

Lemma 2.1. *Let us denote by $c_1(N)$ the degree of $X(E, N)$. Then*

$$c_1(N) = 3^N N!. \tag{1}$$

Proof. We can compute this degree by means of the intersection product in $\mathbb{P}_2^N$. By definition, the degree of $X(E, N)$ is obtained intersecting it with N hyperplanes in general position in $\mathbb{P}_{3^N-1}$, and computing the degree of the cycle thus obtained in the Chow ring. Let l be the class of a line in the Picard group of $\mathbb{P}_2$, and l_i its pullback $\pi_i^*(l)$ through the projection $\pi_i : \mathbb{P}_2^N \to \mathbb{P}_2$ on the i-th factor. Then the Chow ring of $\mathbb{P}_2^N$ is described as $\mathbb{Z}[l_1, \dots, l_N]/(l_1^3, \dots, l_N^3)$. The class of a hyperplane of $\mathbb{P}_{3^N-1}$ restricts to the element $l_1 + \cdots + l_N$, and the class of E^N is easily seen to be $(3l_1) \cdots (3l_N)$. The desired intersection is therefore

$$(3l_1) \cdots (3l_N)(l_1 + \cdots + l_N)^N = 3^N N!(l_1 \cdots l_N)^2,$$

and the statement follows. □

2.2. **Heights.** We need to work with different height functions. These height functions are all related to one another by effective relations. Making these relations explicit for applications is sometimes a delicate task. In this section, based on the work of Silverman and Zimmer, we are going to make explicit the constants that we will need.

Let $\mathcal{M}_K$ be the set of places of a number field K. For a point $P = (P_0 : \cdots : P_m) \in \mathbb{P}_m(K)$ let

$$h(P) = \sum_{v \in \mathcal{M}_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max_i \{|P_i|_v\} \tag{2}$$

be the logarithmic Weil height, and let

$$h_2(P) = \sum_{v \text{ finite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max_i \{|P_i|_v\} + \sum_{v \text{ infinite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \left(\sum_i |P_i|_v^2 \right)^{1/2} \tag{3}$$

be a modified version of the height that differs from the Weil height at the archimedean places. They are both well-defined, they extend to $\overline{\mathbb{Q}}$ and it follows easily from their definitions that

$$h(P) \leq h_2(P) \leq h(P) + \frac{1}{2} \log(m + 1). \tag{4}$$

For an algebraic number $x \in K$, the logarithmic Weil height (for short Weil height) $h(x)$ is the logarithmic Weil height of the projective point $(x : 1) \in \mathbb{P}_1$. We also denote $h_\infty(x)$ the contribution to the Weil height coming from the archimedean places, namely:

$$h_\infty(x) = \sum_{v \text{ infinite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \max\{\log|x|, 0\}.$$

For a point P on E, $\hat{h}(P)$ is the canonical Néron-Tate height, which is related to the Weil height of the x coordinate of P by the following bound ([Sil90], Theorem 1.1):

$$(5)\quad -\frac{h(j)}{24} - \frac{h(\Delta)}{12} - \frac{h_\infty(j)}{12} - 0.973 \leq \hat{h}(P) - \frac{1}{2}h(x(P)) \leq \frac{h(\Delta)}{12} + \frac{h_\infty(j)}{12} + 1.07.$$

To relate $\hat{h}(P)$ and the Weil height of the point P, we define the *Weil height of the Weierstrass equation of E*

$$h_{\mathcal{W}}(E) = h(1 : A^{1/2} : B^{1/3})$$

as the Weil height of the projective point $(1 : A^{1/2} : B^{1/3}) \in \mathbb{P}_2$. Then by [Zim76], p. 40, we have

$$(6)\qquad -\frac{h_{\mathcal{W}}(E)}{2} - \frac{7}{6}\log 2 \leq \frac{1}{3}h(P) - \hat{h}(P) \leq h_{\mathcal{W}}(E) + 2\log 2.$$

For a point $P = (P_1, \dots, P_r) \in \mathbb{P}_{d_1-1} \times \cdots \times \mathbb{P}_{d_r-1}$ we define $h(P)$ and $h_2(P)$ applying formulae (2) and (3) to the image of P in $\mathbb{P}_{d_1 \cdots d_r - 1}$ via the Segre embedding. With these definitions the following relation holds:

$$h(P) = \sum_{i=1}^{r} h(P_i).$$

For a point $P = (P_1, \dots, P_r) \in E^r$, the canonical height $\hat{h}(P)$ is the sum

$$(7)\qquad \hat{h}(P) = \sum_{i=1}^{r} \hat{h}(P_i).$$

In particular, combining (6) with (4) we get that for every point $P \in E^N$ we have

$$(8)\qquad \hat{h}(P) \leq \frac{h_2(P)}{3} + c_2(E, N),$$

where

$$(9)\qquad c_2(E, N) = \frac{N}{2}h_{\mathcal{W}}(E) + \frac{7N}{6}\log 2.$$

From (4) and (6), for every point P of E^N we also have

$$(10)\qquad h_2(P) \leq h(P) + \frac{N}{2}\log 3 \leq 3\hat{h}(P) + c_3(E, N),$$

where

$$(11)\qquad c_3(E, N) = N(3h_{\mathcal{W}}(E) + 6\log 2 + \frac{1}{2}\log 3).$$

For a subvariety $V \subseteq \mathbb{P}_m$ we consider the normalised height of V, denoted $h(V)$, defined in terms of the Chow form of the ideal of V, as done in [Phi91] and [Phi95]. We remark that, with this definition, the height of a point P regarded as a 0-dimensional variety is equal to the height $h_2(P)$ previously defined, which is not equal, in general, to the Weil height of the point. To avoid confusion, we will always write $h_2(P)$ to denote the height of the variety $\{P\}$.

We end this subsection by recalling two classical results on the normalised height, the Arithmetic Bézout Theorem and the Zhang Inequality.

Theorem 2.2 (Arithmetic Bézout Theorem)**.** *Let X and Y be irreducible closed subvarieties of $\mathbb{P}_m$ defined over $\overline{\mathbb{Q}}$. If $Z_1, \dots, Z_g$ are the irreducible components of $X \cap Y$, then*

$$\sum_{i=1}^{g} h(Z_i) \leq \deg(X)h(Y) + \deg(Y)h(X) + \frac{(m+1)\log 2}{2}\deg(X)\deg(Y).$$

For the constant $\frac{(m+1)\log 2}{2}$ see [BGS94], Theorem 5.5.1 (iii).

Theorem 2.3 (Zhang's inequality)**.** *Let $X \subseteq \mathbb{P}_m$ be an irreducible algebraic subvariety. Defining the essential minimum of X as*

$$\mu(X) = \inf\{\theta \in \mathbb{R} \mid \{P \in X \mid h_2(P) \leq \theta\} \textit{ is Zariski dense in } X\},$$

we have

$$\mu(X) \leq \frac{h(X)}{\deg X} \leq (1 + \dim X)\mu(X).$$

We also define a different essential minimum for subvarieties of E^N, that will be used in Subsection 7.2, as

$$\hat{\mu}(X) = \inf\{\theta \in \mathbb{R} \mid \{P \in X \mid \hat{h}(P) \leq \theta\} \text{ is Zariski dense in } X\}.$$

By (8) and (10), these two definitions are related by the inequality

$$3\hat{\mu}(X) - 3c_2(E,N) \leq \mu(X) \leq 3\hat{\mu}(X) + c_3(E,N) \tag{12}$$

where the constants $c_2(E,N)$ and $c_3(E,N)$ are defined in (9) and (11) respectively.

2.3. **Algebraic Subgroups.** In this subsection we present the relationship between several different descriptions of the algebraic subgroups of E^N.

Before explaining it in detail, we need to recall some classical tools in the geometry of numbers. Let r and N be positive integers, with $r \leq N$, and let Λ be a lattice of rank r in $\mathbb{R}^N$. We define the determinant of Λ as $\det\Lambda = \sqrt{\det(MM^t)}$, where $M \in \mathrm{Mat}_{r\times N}(\mathbb{R})$ is any matrix whose rows form a basis of Λ. We also define the successive minima λ_i of Λ as

$$\lambda_i = \inf\{t \in \mathbb{R} \mid \dim\langle B_t \cap \Lambda\rangle_{\mathbb{R}} = i\},$$

where B_t is the euclidean ball or radius t centered at the origin.

The following theorem by Minkowski plays an important role in this setting.

Theorem 2.4 (Minkowski's second theorem)**.** *Let Λ be a lattice of rank r. Then*

$$\frac{2^r}{r!}\det\Lambda \leq \omega_r\lambda_1\cdots\lambda_r \leq 2^r\det\Lambda,$$

where the λ_i's are the successive minima of Λ and

$$\omega_r = \frac{\pi^{r/2}}{\Gamma(r/2+1)} \tag{13}$$

is the volume of the euclidean unit ball in $\mathbb{R}^r$ (here Γ denotes the Euler Γ function).

It is well known that abelian subgroups of codimension r, matrices of rank r in $\mathrm{Mat}_{r\times N}(\mathrm{End}(E))$, and lattices of rank r in $(\mathrm{End}(E))^N$ are essentially representations of the same objects up to some torsion subgroup; analogously, their degree, minors and successive minima can be related up to constants.

In more detail, let $B + \zeta$ be an irreducible torsion variety of E^N of codimension $\operatorname{codim} B = r$ and let $\pi_B : E^N \to E^N/B$ be the natural projection. We know that E^N/B is isogenous to E^r; let $\varphi_B : E^N \to E^r$ be the composition of π_B and this isogeny.

We associate B with the morphism φ_B and we have that $\ker \varphi_B = B + \tau$ with τ a torsion subgroup whose cardinality is absolutely bounded (by [MW93] Lemma 1.3). Obviously φ_B is identified with a matrix in $\mathrm{Mat}_{r\times N}(\mathrm{End}(E))$ of rank r. Using basic geometry of numbers, we can choose the matrix representing φ_B such that the degree of B is essentially the product of the squares of the norms of the rows of the matrix.

More precisely, given $B \subseteq E^N$ an algebraic subgroup of rank r, we associate it with a matrix in $\mathrm{Mat}_{r\times N}(\mathrm{End}(E))$ with rows $u_1, \dots, u_r$ such that the euclidean norm $|u_i|$ of u_i equals the i-th successive minimum of the lattice $\Lambda = \langle u_1, \dots, u_r\rangle_{\mathbb{Z}}$. In Subsection 7.3 we show that there is a constant $c_4(N, r)$ such that

$$\deg B \leq c_4(N,r) \prod_{i=1}^{r} |u_i|^2 \tag{14}$$

and, when E is non CM, we have

$$c_4(N,r) = 3^N N! \left(\frac{3}{2}(N+1)12^{N-1}\right)^r .$$

Combining bound (14) and Minkowski's theorem one can relate the degree of an algebraic subgroup and the determinant of the associated lattice (*i.e.* the lattice generated by the rows of the associated matrix); when the curve E is non CM the following explicit bound holds:

$$\deg B \leq c_4(N,r) \frac{4^r}{\omega_r^2} (\det \Lambda)^2, \tag{15}$$

where $c_4(N, r)$ is given above.

3. The main result

In this section we give the proof of our main result, which is Theorem 1.1 of the Introduction. The constants that we obtain are always effective and also explicit in the non CM case.

The proof of our main theorem is based on the following idea: given a point $P \in E^N$ which is contained in a torsion variety of dimension 1, we construct, by means of the geometry of numbers, another abelian subvariety $H \subseteq E^N$ of dimension 1 so that the degree $\deg H$ and the height of the translate $H + P$ are both well controlled. An application of the Arithmetic Bézout Theorem, recalled in Subsection 2.2, leads then to the end of the proof. We will show in the technical Section 7 how to construct the auxiliary algebraic subgroup H; in order to compute all the constants explicitly we need several pages of careful computations, which we have collected in Section 6.

The overall construction of the auxiliary algebraic subgroup H is summarised in the following propositions, whose proofs are postponed to Section 7.

Proposition 3.1 (Non CM Case). *Let E be a non CM elliptic curve and let $1 \leq m \leq N$ be integers. Let $P = (P_1, \dots, P_N) \in B \subseteq E^N$, where B is a torsion variety of dimension $\leq m$. Say s is an integer with $1 \leq s \leq N$ and $T \geq 1$ a real number.*

Then there exists an abelian subvariety H of codimension s such that

$$\begin{aligned} \deg(H+P) &\leq c_4(N,s)T \\ h(H+P) &\leq c_5(N,m,s)T^{1-\frac{N}{ms}}\hat{h}(P) + c_6(E,N,s)T; \end{aligned}$$

where

$$\begin{aligned}
c_4(N,s) &= 3^N N! \left(\frac{3}{2}(N+1)12^{N-1}\right)^s\\
c_5(N,m,s) &= m^3(m!)^4\binom{N+m}{N}\frac{3sN^2(N-s+1)4^{3N-m+1}}{(\omega_s\omega_{N-s}\omega_N)^2}c_4(N,s)\\
c_6(E,N,s) &= 3N(N-s+1)\left(2\log 2+\frac{\log 3}{6}+h_{\mathcal{W}}(E)\right)c_4(N,s).
\end{aligned}$$

Here $\omega_r = \pi^{r/2}/\Gamma(r/2+1)$ *is the volume of the euclidean unit ball in* $\mathbb{R}^r$*, and* $h_{\mathcal{W}}(E)$ *is defined in Section 2.2.*

Proposition 3.2 (CM Case)**.** *Let* E *be a CM elliptic curve and let* $1 \le m \le N$ *be integers. Let* $P = (P_1, \dots, P_N) \in B \subseteq E^N$*, where* B *is a torsion variety of dimension* $\le m$*. Say* s *is an integer with* $1 \le s \le N$ *and* $T \ge 1$ *a real number.*

Then there exists an abelian subvariety H *of codimension* s *such that*

$$h(H+P) \le c_7 T^{1-\frac{N}{ms}}\hat{h}(P) + c_8 T$$

and

$$\deg(H+p) \le c_9 T,$$

where c_7, c_8, c_9 *are effective positive constants depending only on the integers* N, m, s*, the ring* $\mathrm{End}(E)$ *and the height* $h_{\mathcal{W}}(E)$ *(defined in Section 2.2).*

We now show how to deduce Theorem 1.1 from Propositions 3.1 and 3.2.

Proof of Theorem 1.1. If $N = 2$, then the codimensional inequality (ii) at page 1 tells us that the only V-torsion anomalous points are the torsion points contained in V, which have height zero. We can now assume that $N \ge 3$.

The point P is a component of the intersection $V \cap (B+\zeta)$, where $B+\zeta$ is a torsion variety of $\dim B = 1$.

Assume first that E is non CM. Let T be a free parameter that will be specified later; we apply Proposition 3.1 to P, T, $m = 1$ and $s = N-1$. This gives a translate $H+P$ of dimension $\dim(H+P) = 1$, of degree bounded in terms of T and such that $h(H+P)$ is bounded solely in terms of $\deg H$ and $\hat{h}(P)$.

Explicitely, if

$$\begin{aligned}
c_{10}(N) = c_4(N,N-1) &= 3^N N!\left(\frac{3}{2}(N+1)12^{N-1}\right)^{N-1}\\
c_{11}(N) = c_5(N,1,N-1) &= \frac{3}{2}\frac{N^2(N^2-1)64^N}{(\omega_N\omega_{N-1})^2}c_{10}(N)\\
c_{12}(E,N) = c_6(E,N,N-1) &= 6N(h_{\mathcal{W}}(E)+2\log 2+\frac{1}{6}\log 3)c_{10}(N),
\end{aligned}$$

then the degree and the height of the translate $H+P$ are bounded by Proposition 3.1 as

$$\deg(H+P) \le c_{10}(N)T$$

and

$$h(H+P) \le \frac{c_{11}(N)}{T^{1/(N-1)}}\hat{h}(P) + c_{12}(E,N)T.$$

We want to prove that P is a component of $V \cap (H+P)$. If not, then $H+P \subseteq V$ because $\dim(H+P) = 1$. In addition $\dim(B+H+\zeta) \le 2$, as $\dim B = 1$. Since $N \ge 3$, the torsion variety $B+H+\zeta$ is proper. Thus $H+P \subseteq V \cap (B+H+\zeta)$ would be V-torsion anomalous, contradicting the maximality of P.

This means that P is a component of $V \cap (H+P)$. In order to bound the height of P we can apply the Arithmetic Bézout Theorem to the irreducible varieties V and $H+P$. We have
(16)

$$h_2(P) \leq h(V)c_{10}(N)T + \deg V \left(\frac{c_{11}(N)}{T^{1/(N-1)}} \hat{h}(P) + c_{12}(E,N)T \right) + \frac{3^N \log 2}{2} c_{10}(N) T \deg V.$$

We now choose

$$T = \left(\frac{N}{N-1} \frac{c_{11}(N)}{3} \deg V \right)^{N-1},$$

so that the coefficient of $\hat{h}(P)$ at the right-hand side of (16) becomes $3(N-1)/N$. Recall that by (8)

$$\hat{h}(P) \leq \frac{h_2(P)}{3} + c_2(E,N)$$

where $c_2(E,N)$ is the explicit constant in (9) depending only on the coefficients of E and on N. Then we get

$$\begin{aligned} 3\hat{h}(P) \leq & \frac{3(N-1)}{N} \hat{h}(P) + 3c_2(E,N) + c_{10}(N)Th(V) + \\ & + \left(\frac{3^N \log 2}{2} c_{10}(N) + c_{12}(E,N) \right) T \deg V, \end{aligned}$$

and hence

$$\hat{h}(P) \leq \frac{N}{3} c_{10}(N) T h(V) + \frac{N}{3} \left(\frac{3^N \log 2}{2} c_{10}(N) + c_{12}(E,N) \right) T \deg V + N c_2(E,N),$$

which is the desired bound for $\hat{h}(P)$.

This concludes the proof of the non CM case. Notice that the application of Proposition 3.1 is the only point in the proof where it is required that E is non CM. Therefore the same argument, with the use of Proposition 3.2 instead of Proposition 3.1, proves the result in the CM case. □

4. An application to the Effective Mordell-Lang Conjecture

We now clarify the implications of our theorems on the Effective Mordell-Lang Conjecture, proving Theorem 1.3 from the introduction.

Proof of Theorem 1.3. The last part of the theorem is a direct consequence of the first part. Indeed if $E(k)$ has rank 1, then all points in $\mathcal{C}(k)$ have rank at most one.

We now prove the first part of the theorem. The points of rank zero are exactly the torsion points; for these points the bound is trivially true because their height is zero.

Consider first the case that $\mathcal{C}$ is weak-transverse and $N \geq 3$. Let $P = (P_1, \dots, P_N) \in \mathcal{C}$ be a point of rank 1 and let $g \in E$ be a generator of $\Gamma_P = \langle P_1, \dots, P_N \rangle_{\mathbb{Q}}$. Then the coordinates of P satisfy $a_i P_i = b_i g$ for some $a_i \neq 0$ and b_i in $\mathbb{Z}$. Since P is not a torsion point, at least one of the b_i must be different from zero; let's say that $b_1 \neq 0$. Then P lies on the algebraic subgroup B in E^N given by the intersection of the $N-1$ algebraic subgroups of equations $a_i b_1 X_i = a_1 b_i X_1$ for $i = 2, \dots, N$. Note that the matrix of coefficients has obviously rank $N-1$, so the dimension of B is one.

Since $\mathcal{C}$ is weak-transverse, P is a component of $\mathcal{C} \cap B$; thus for $N \geq 3$ P is $\mathcal{C}$-torsion anomalous and it has relative codimension 1. In addition, on weak-transverse curves all torsion anomalous points are maximal; thus P is a maximal $\mathcal{C}$-torsion anomalous point of relative codimension 1. We can now apply Theorem 1.1 to $V = \mathcal{C}$ to obtain the height bound, thus concluding the case of $N \geq 3$.

For $N = 2$, the previous argument cannot be directly applied, indeed a point of rank 1 is never torsion anomalous in E^2. We now show how to reduce the case of a transverse curve $\mathcal{C} \subseteq E^2$ to the previous case. Let $P = (P_1, P_2) \in \mathcal{C}$ be a point of rank 1 and let $g \in E$ be a generator of $\Gamma_P = \langle P_1, P_2 \rangle_{\mathbb{Q}}$. Fix a positive real ε, and choose an integer M such that $\varepsilon M^2 \geq \hat{h}(g) \deg(\mathcal{C})$. Let Q_M be a point in E such that $MQ_M = g$; by our choice of M we have that

$$\hat{h}(Q_M) = \frac{\hat{h}(g)}{M^2} \leq \frac{\varepsilon}{\deg \mathcal{C}}.$$

We define $\mathcal{C}'_M = \mathcal{C} \times \{Q_M\} \subseteq E^3$ and $P'_M = P \times \{Q_M\} \in \mathcal{C}'_M$. Since $\mathcal{C}$ is transverse in E^2, $\mathcal{C}'_M$ is weak-transverse in E^3. Notice that $P'_M \in \mathcal{C}'_M$ is a point of rank 1 and

$$\hat{h}(P) \leq \hat{h}(P'_M).$$

In addition $\deg \mathcal{C}'_M = \deg \mathcal{C}$ and $\hat{\mu}(\mathcal{C}'_M) = \hat{\mu}(\mathcal{C}) + \hat{h}(Q_M)$. By Zhang's inequality and (12) we have

$$\begin{aligned} h(\mathcal{C}'_M) \leq 2\mu(\mathcal{C}'_M) \deg \mathcal{C} \leq 2 \deg \mathcal{C}\,(3\hat{\mu}(\mathcal{C}'_M) + c_3(E,3)) = \\ = 2 \deg \mathcal{C} \left(3\hat{\mu}(\mathcal{C}) + 3\hat{h}(Q_M) + c_3(E,3)\right) \leq \\ \leq 2 \deg \mathcal{C} \left(\mu(\mathcal{C}) + 3c_2(E,3) + 3\hat{h}(Q_M) + c_3(E,3)\right) \leq \\ \leq 2h(\mathcal{C}) + 6\varepsilon + 6 \deg \mathcal{C} \left(c_2(E,3) + \frac{c_3(E,3)}{3}\right) \end{aligned}$$

where the constant $c_2(E,3)$ is defined in (9) and $c_3(E,3)$ in (11).

To bound $\hat{h}(P'_M)$ and in turn $\hat{h}(P)$, we apply the first part of the theorem to $\mathcal{C}'_M \in E^3$, obtaining:

$$\begin{aligned} \hat{h}(P) \leq & 2C_1(3)h(\mathcal{C})(\deg \mathcal{C})^2 + (C_2(E,3) + 6c_2(E,3)C_1(3) + 2c_3(E,3)C_1(3))\,(\deg \mathcal{C})^3 + \\ & + C_3(E,3) + 6\varepsilon C_1(3)(\deg \mathcal{C})^2. \end{aligned}$$

Clearly the point P does not depend on the initial choice of ε and, letting ε go to zero, we get the desired bound for the height. □

5. Rational points on an explicit family of curves

We now give an explicit method to find, in principle, all rational points on a family of curves in a power of a non CM elliptic curve.

Let E be the elliptic curve defined by the Weierstrass equation

$$E : y^2 = x^3 + x - 1.$$

With an easy computation one can check that

$$\begin{aligned} \Delta(E) &= -496, \\ j(E) &= \frac{6912}{31}, \\ h_{\mathcal{W}}(E) &= 0, \end{aligned}$$

in particular the curve is non CM because $j(E) \notin \mathbb{Z}$. Furthermore the group $E(\mathbb{Q})$ has rank 1 with generator $g = (1,1)$ and no non-trivial torsion points; this can be checked on a database of elliptic curve data (such as `http://www.lmfdb.org/EllipticCurve/Q`). The Néron-Tate height of the generator g can be bounded from below, computationally, as

$$\hat{h}(g) \geq 1/4 \tag{17}$$

(we used dedicated software (PARI/GP) which implements an algorithm with sigma and theta functions due to Silverman).

As an application of our main result we give the proof of Theorem 1.4, which is an example of the explicit Mordell Conjecture for a family of curves in E^2 of increasing genus and degrees. We recall the definition of the curves from the introduction. We write

$$\begin{aligned} y_1^2 &= x_1^3 + x_1 - 1 \\ y_2^2 &= x_2^3 + x_2 - 1 \end{aligned}$$

for the equations of E^2 in $\mathbb{P}_2^2$, using affine coordinates $(x_1, y_1) \times (x_2, y_2)$ and we consider the family of curves $\{\mathcal{C}_n\}_n$ with $\mathcal{C}_n \subseteq E^2$ defined via the additional equation

$$x_1^n = y_2.$$

Proof of Theorem 1.4. To prove the theorem we first show that the curves $\mathcal{C}_n$ are irreducible and transverse in E^2 and then we apply Theorem 1.3 with $N = 2$ and $E(\mathbb{Q})$ of rank 1, computing all invariants of the case.

The irreducibility of the $\mathcal{C}_n$ is easily seen to be equivalent to the primality of the ideal generated by the polynomials $y_1^2 - x_1^3 - x_1 + 1$ and $x_1^{2n} - x_2^3 - x_2 + 1$ in the ring $\mathbb{Q}[x_1, x_2, y_1]$. This follows from an easy argument in commutative algebra.

Notice that in E^2 the only irreducible curves that are not transverse are translates, so curves of genus one. Thus, we need to show only that each $\mathcal{C}_n$ has genus at least 2; in fact we prove that $\mathcal{C}_n$ has genus $4n + 2$.

Consider the morphism $\pi_n : \mathcal{C}_n \to \mathbb{P}_1$ given by the function y_2. The morphism π_n has degree $6n$, because for a generic value of y_2 there are three possible values for x_2, n values for x_1, and two values of y_1 for each x_1.

Let $\alpha_1, \alpha_2, \alpha_3$ be the three distinct roots of the polynomial $f(T) = T^3 + T - 1$; let also $\beta_1, \beta_2, \beta_3, \beta_4$ be the four roots of the polynomial $27T^4 + 54T^2 + 31$, which are the values such that $f(T) - \beta_i^2$ has multiple roots. Notice that none of the α_i can be equal to the β_j because they have different degrees.

The morphism π_n is ramified over $\beta_1, \beta_2, \beta_3, \beta_4, 0, \alpha_1^n, \alpha_2^n, \alpha_3^n, \infty$. Each of the points β_i has $2n$ preimages of index 2 and $2n$ unramified preimages. The point 0 has 6 preimages ramified of index n. The points α_i^n have 3 preimages ramified of index 2 and $6n - 6$ unramified preimages. The point at infinity is totally ramified.

By Hurwitz formula

$$\begin{aligned} 2 - 2g(\mathcal{C}_n) &= \deg \pi_n (2 - 2g(\mathbb{P}_1)) - \sum_{P \in \mathcal{C}_n} (e_P - 1) \\ 2 - 2g(\mathcal{C}_n) &= 12n - (4 \cdot 2n + 6(n-1) + 3 \cdot 3 + 6n - 1) \\ g(\mathcal{C}_n) &= 4n + 2. \end{aligned}$$

Thus the family $\{\mathcal{C}_n\}_n$ is a family of transverse curves in E^2. We can therefore apply Theorem 1.3 with $N = 2$ to each $\mathcal{C}_n$, which gives, for $P \in \mathcal{C}_n(\mathbb{Q})$

$$\hat{h}(P) \leq \left(2.364 \cdot 10^{34} h(\mathcal{C}_n) + 9.504 \cdot 10^{35} \deg \mathcal{C}_n\right) (\deg \mathcal{C}_n)^2. \tag{18}$$

We now compute $\deg \mathcal{C}_n$ and $h(\mathcal{C}_n)$.

We can compute the degree of $\mathcal{C}_n$ as an intersection product. Let ℓ, m be the classes of lines of the two factors of $\mathbb{P}_2^2$ in the Chow group. Then the degree of $\mathcal{C}_n$ is obtained multiplying the classes of the hypersurfaces cut by the equation $x_1^n = y_2$, which is $n\ell + m$, by the two Weierstrass equations of E, which are 3ℓ and $3m$, and by the restriction of an hyperplane of $\mathbb{P}_8$, which is $\ell + m$. In the Chow group

$$(n\ell + m)(3\ell)(3m)(\ell + m) = 9(n + 1)(\ell m)^2$$

and then

$$\deg \mathcal{C}_n = 9(n + 1).$$

We estimate the height of $\mathcal{C}_n$ using Zhang's inequality and computing an upper bound for the essential minimum $\mu(\mathcal{C}_n)$ of $\mathcal{C}_n$. To this aim, we construct an infinite set of points on $\mathcal{C}_n$ of bounded height. By the definition of essential minimum, this gives also an upper bound for $\mu(\mathcal{C}_n)$.

Let $Q_\zeta = ((x_1,y_1),(\zeta,y_2)) \in \mathcal{C}_n$, where $\zeta \in \overline{\mathbb{Q}}$ is a root of unity. Clearly there exist infinitely many such points on $\mathcal{C}_n$. Denoting by h the logarithmic Weil height on $\overline{\mathbb{Q}}$ and using the equations of E and $\mathcal{C}_n$, we have:

$$h(\zeta)=0, h(y_2) \leq \frac{\log 3}{2}, h(x_1) \leq \frac{\log 3}{2n}, h(y_1) \leq \frac{\log 3}{n} + \frac{\log 3}{2}.$$

Thus

$$h(x_1,y_1) \leq \log 3 \left(\frac{n+3}{2n}\right), h(\zeta,y_2) \leq \frac{\log 3}{2}$$

and from (4)

$$h_2(x_1,y_1) \leq \log 3 \left(\frac{2n+3}{2n}\right), h_2(\zeta,y_2) \leq \log 3.$$

So for all points Q_ζ we have

$$h_2(Q_\zeta) = h_2(x_1,y_1) + h_2(\zeta,y_2) \leq \log 3 \left(\frac{4n+3}{2n}\right).$$

By the definition of essential minimum, we deduce

$$\mu(\mathcal{C}_n) \leq \log 3 \left(\frac{4n+3}{2n}\right)$$

and by Zhang's inequality $h(\mathcal{C}_n) \leq 2 \deg \mathcal{C}_n \mu(\mathcal{C}_n) \leq 9(n+1)\log 3 \left(\frac{4n+3}{n}\right)$.

From formula (18), if $P \in \mathcal{C}_n(\mathbb{Q})$ then

$$\hat{h}(P) \leq 8.253 \cdot 10^{38}(n+1)^3. \tag{19}$$

Let us now write $P = ([a]g,[b]g)$, with $g=(1,1)$ the generator of $E(\mathbb{Q})$. By the definition of $\hat{h}$ on E^2 (see (7)) and the properties of the Néron-Tate height, we have

$$\hat{h}(P) = (a^2+b^2)\hat{h}(g).$$

Now, by relations (5), (6) and $(x([a]g))^n = y([b]g)$ because P is on the curve, we have

$$\begin{aligned}2na^2\hat{h}(g) &\leq nh(x([a]g)) + 2n\left(\frac{h(\Delta)}{12} + \frac{h_\infty(j)}{12} + 1.07\right) \leq \\ &= h(y([b]g)) + 5n \leq h([b]g) + 5n \leq \\ &\leq 3b^2\hat{h}(g) + 6\log 2 + 5n,\end{aligned}$$

and therefore

$$\left(\frac{2n}{3}+1\right)a^2\hat{h}(g) \leq \hat{h}(P) + 2\log 2 + \frac{5}{3}n.$$

Combining this with (19) and the lower bound (17) we obtain

$$|a| \leq 7.037 \cdot 10^{19}(n+1).$$

Using again (5) and (6) as before, we get that

$$2b^2\hat{h}(g) \leq 3na^2\hat{h}(g) + 7\log 2 + 5$$

and from this and (17) we get

$$|b| \leq \left(\frac{3na^2}{2} + 14\log 2 + 10\right)^{\frac{1}{2}}. \qquad \square$$

6. Estimates for degrees of maps

The central aim of this section is to produce sharp bounds for the degree of algebraic subgroups of E^N.

For example, consider the algebraic subgroup of codimension 1 defined by the morphism $(l_1, \cdots, l_N) : E^N \to E$ sending $(X_1, \cdots, X_N) \mapsto l_1X_1 + \cdots + l_NX_N$, where $l_1, \ldots, l_N \in \mathrm{End}(E)$. The degree of this subgroup is equal to a constant times $|(l_1, \cdots, l_N)|^2$. To get explicit results we need to compute this constant and, to this purpose, we have to describe the sum of two points and the multiplication by an integer on E and E^N in terms of rational maps. We will examine these maps in detail and bound their degrees. These bounds will be used to prove Propositions 3.1 and 3.2, which are the core of our main theorem.

We briefly anticipate here what is needed to prove the above mentioned propositions. We consider an algebraic subgroup H of E^N of codimension s. It is defined by s equations

$$\begin{gathered} L_1(X_1, \ldots, X_N) = 0, \\ \vdots \\ L_s(X_1, \ldots, X_N) = 0 \end{gathered}$$

where $L_i(X_1, \ldots, X_N) = l_{i_1}X_1 + \cdots + l_{i_N}X_N$ are morphisms from E^N to E; here the coefficients are endomorphisms $l_{i_j} \in \mathrm{End}(E)$, and they are expressed by certain rational functions; similarily the $+$ that appears in this expression is the addition map in E^N, which is expressed by a rational function of the coordinates.

More precisely, if the X_i's are all points on E with affine coordinates (x_i, y_i) in $\mathbb{P}_2$, then $L_i(\mathbf{X})$ are also points on E with coordinates in $\mathbb{P}_2$ $(x(L_i(\mathbf{X})), y(L_i(\mathbf{X})))$ which are rational functions of the x_i's and y_i's.

The purpose of this section is to study the rational functions $x(L_i(\mathbf{X}))$ and to bound the sums of the partial degrees (not only the partial degrees) of their numerators and denominators. The reason is that, in the proof of the main theorem, we will need to study the image of the algebraic subgroup H in $\mathbb{P}_{3^N-1}$ via the Segre embedding, and when studying the effect of the Segre embedding on the functions defining the embedded variety, it is the sum of the partial degrees that comes into play.

To this aim, we proceed in the following way: in Subsection 6.1 we give bounds for the sums of the partial degrees of the product and the sum of quotients of polynomials in several variables. Then, in Subsection 6.2 we estimate the multiplication map on E. In Subsection 6.3, we study the sum of many points on an elliptic curve. Finally, we estimate the sums of the partial degrees of $L_i(X_1, \ldots, X_N)$.

All the computations are carried out for linear combinations of points with integral coefficients (which is to say, when E is non CM). In Remark 6.1 we describe how to adapt this to the CM case.

6.1. **Estimates for degrees of rational functions.**

In this short paragraph we recall how to bound the sums of the partial degrees of products and sums of quotients of polynomials in the field of rational functions.

If $\frac{f_i}{g_i}$ are rational functions, with f_i, g_i polynomials in several variables and coefficients in $\mathbb{Z}$, we denote by $d(f_i/g_i)$ the maximum of the sums of the partial degrees of both f_i, g_i. Then

$$\frac{f}{g} = \prod_{i=1}^{r} \frac{f_i}{g_i} \qquad d(f/g) \leq \sum_{i=1}^{r} d(f_i/g_i) \tag{20}$$

$$\frac{f}{g} = \sum_{i=1}^{r} \frac{f_i}{g_i} \qquad d(f/g) \leq \sum_{i=1}^{r} d(f_i/g_i) \tag{21}$$

where $d(f/g)$ is the bound for the sum of partial degrees of the product (in (20)) and of the sum (in (21)) of the f_i/g_i's respectively.

6.2. **The multiplication by** m**.** Let m be a positive integer and let E be an elliptic curve. The aim of this subsection is to bound the sum of the partial degrees of the rational function giving the multiplication by m on E. If $P = (x, y) \in E$, then by [Sil86], Ex 3.7, p. 105 we have that

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)} \right)$$

where $\phi_m, \psi_m, \omega_m \in \mathbb{Z}[A, B, x, y]$ are certain polynomials defined below.

The polynomial ψ_m is defined inductively as follows:

$$\begin{aligned}
&\psi_1 = 1, \psi_2 = 2y, \\
&\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2, \\
&\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),
\end{aligned}$$

and for $m \geq 2$

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \qquad (m \geq 2) \\
2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \qquad (m \geq 2).
\end{aligned}$$

The polynomials ϕ_m and ω_m are defined as:

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
4y\omega_m &= \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

As Silverman points out, one can prove that $\psi_m, \phi_m, y^{-1}\omega_m$ (for m odd) and $(2y)^{-1}\psi_m, \phi_m, \omega_m$ (for m even) are polynomials in $\mathbb{Z}[A, B, x, y^2]$. Hence, using the Weierstrass equation for E to replace y^2, they can be treated as polynomials in $\mathbb{Z}[A, B, x]$.

Moreover, as polynomials in x we have

$$\begin{aligned}
\phi_m(x) &= x^{m^2} + \text{ lower order terms,} \\
\psi_m^2(x) &= m^2 x^{m^2-1} + \text{ lower order terms.}
\end{aligned}$$

We need to find bounds for the degrees of the polynomials ψ_m, ϕ_m, ω_m.

The following bounds are obtained combining the above definitions in [Sil86] and the expressions for ϕ_m and ψ_m^2:

$$\begin{aligned}
d(\phi_m) &= m^2 \\
d(\psi_m^2) &= m^2 - 1 \\
d(\psi_m) &\leq \frac{m^2 + 1}{2} \\
d(\psi_m^3) &\leq \frac{3m^2 - 1}{2} \\
d(\omega_m) &\leq \frac{3}{2}(m^2 + 1).
\end{aligned}$$

Using the above bounds and the formula for the coordinates of $[m]P$, we see that the sum of the partial degrees of the polynomials $\phi_m, \psi_m^2, \omega_m, \psi_m^3$, which are numerators and denominators of the rational functions given by the coordinates of $[m]P$, are bounded by $\frac{3}{2}(m^2+1)$.

6.3. **Estimates for linear maps.** We now look first at the functions giving the sum of two, and then many, points on an elliptic curve. Our aim is to obtain explicit bounds on the sum of the partial degrees of the rational function expressing a linear combination of N points in E.

Then we will study equations defining algebraic subgroups of E^N, obtained equating to zero linear combinations of N variables with coefficients in $\mathrm{End}(E)$. Evaluating the functions at points in E whose coordinates are themselves rational functions, we will bound the sum of partial degrees of these linear combinations, viewed as rational functions in the new coordinates.

6.3.1. *Estimates for the addition map.* We consider an elliptic curve E embedded in $\mathbb{P}_2$ via its Weierstrass equation.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E and $P_3 = (x_3, y_3) = P_1 \oplus P_2$ be their sum.

If $x_1 \neq x_2$, from [Sil86], Chap. 3, setting

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

we have that

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= -\lambda x_3 - \nu. \end{aligned} \tag{22}$$

So x_3 and y_3 are rational functions of the coordinates of P_1 and P_2, and we now want to control the sum of their partial degrees.

Using (22), if (x_1, y_1) and (x_2, y_2) already have coordinates given by certain other rational functions, whose sums of the partial degrees are bounded respectively by d_1, d_2, then the sums of the partial degrees, in the variables of x_1, y_1, x_2, y_2, of the functions x_3, y_3 are given by:

$$d(x_3) \leq 5(d_1 + d_2)$$
$$d(y_3) \leq 12(d_1 + d_2).$$

If instead $x_1 = x_2$ and $y_1 = y_2$, then setting

$$\lambda = \frac{3x_1^2 + A}{2y_1}$$

we have that

$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = y_1 + \lambda(x_3 - x_1).$$

Again applying (20), (21), if $P_1 = P_2$ have coordinates given by rational functions in certain variables with sums of the partial degrees bounded by d_1, then x_3 and y_3 are rational functions, in the same variables, with sums of the partial degrees bounded as

$$d(x_3) \leq 7d_1$$
$$d(y_3) \leq 11d_1.$$

If $x_1 = x_2$ and $y_1 = -y_2$, then the two points are opposite and the sum is the zero of the elliptic curve.

Comparing the bounds obtained in the three cases, one checks that in any case

$$\max(d(x_3), d(y_3)) \leq 12(d_1 + d_2) \tag{23}$$

holds. This computation was carried out for the sum of two points. We now iterate it $M-1$ times to obtain bounds for the rational function expressing the sum of M points. It follows by induction from (23) that

$$d \leq 12^{M-1} d_1 + \sum_{i=2}^{M} 12^{M-i+1} d_i \leq 12^{M-1} \sum_{i=1}^{M} d_i, \tag{24}$$

where d_i is a bound for the sum of the partial degrees of the x and y coordinates of the i-th point.

6.3.2. *Estimates for group morphisms.* Let us consider the morphism $L : E^N \to E$ defined as

$$L(\mathbf{X}) = l_1 X_1 + \cdots + l_N X_N$$

where $l_i \in \mathbb{Z}$ and $X_i = (x_i, y_i)$ is in the i-th factor of E^N. Then $L(\mathbf{X})$ is also a point on E with coordinates $(x(L(\mathbf{X})), y(L(\mathbf{X})))$. By the considerations above, these are rational functions in the coordinates (x_i, y_i) of all X_i's. We want to combine the results from the previous subsections to bound the sum of the partial degrees of the rational function $x(L(\mathbf{X}))$.

Let us set $d(L) = d(x(L(\mathbf{X})))$ to be the sum of the partial degrees in the numerator and denominator of $x(L(\mathbf{X}))$.

Now combining inequality (24) with the bounds from Subsection 6.2 we obtain

$$d(L) \leq \frac{3}{2} 12^{N-1} \left(N + \sum_{i=1}^{N} |l_i|^2 \right). \tag{25}$$

Remark 6.1. *The content of this section holds analogously when E is CM. In this case* $\mathrm{End}(E) = \mathbb{Z} + \tau\mathbb{Z}$ *for some imaginary quadratic integer τ.*

For a point $P = (x, y)$ we denote $\tau(P) = (x_\tau, y_\tau)$. Then x_τ and y_τ are rational functions of x and y and we let $d_{CM}(\tau)$ be the sum of their partial degrees. Writing $\tau = \sqrt{-d}$ for some non-square positive integer d we have

$$d_{CM}(\tau) \leq 2d.$$

Since every element $l_i \in \mathrm{End}(E)$ can be written as $l_i = r_i + \tau s_i$, where $r, s \in \mathbb{Z}$, we can write

$$L(\mathbf{X}) = r_1 X_1 + \cdots + r_N X_N + \tau s_1 X_{N+1} + \cdots + \tau s_N X_{2N}$$

and, using the above results, we can effectively compute a bound

$$d(L) \leq D(E, N, \tau) \sum_{i=1}^{N} |l_i|^2 \qquad \text{for } l_i \in \mathrm{End}(E) \text{ not all } 0,$$

corresponding to the bound (25)*. However we omit here the explicit computations.*

7. Conclusion

In this section we prove Proposition 3.1 (explicit for non CM varieties) and Proposition 3.2 (effective for CM varieties), which are the core of the proofs of our main results. Essentially the propositions state that: if a point $P \in E^N$ belongs to an algebraic subgroup B then we can construct a translate $H + P \subseteq E^N$ of controlled degree and height.

To prove these results, we use the bounds for the height of Subsection 2.2 and for the degree of Section 6. Then we use the geometry of numbers, to construct the algebraic subgroup H.

Before moving on with the main proof, we need a short section in linear algebra.

7.1. **A lemma on adjugate matrices.** Let A be a $n \times n$ matrix with complex coefficients. Let $a_i \in \mathbb{C}^n$ be the rows of A.

Definition 7.1. *The* adjugate matrix of A*, denoted* A^**, is the transpose of the matrix* $((-1)^{i+j} \det M_{ij})_{ij}$*, where* M_{ij} *is the* $(n-1) \times (n-1)$ *minor obtained from* A *after deleting the* i*-th row and the* j*-th column.*

The adjugate matrix has the property that

$$AA^* = A^*A = (\det A)\mathrm{Id}$$

and its entries are bounded as it follows:

Lemma 7.2. *Let* $A \in M_{n\times n}(\mathbb{C})$ *be the matrix with rows* $a_1, \dots, a_n \in \mathbb{C}^n$*. Then every entry in the* i*-th column of* A^* *has absolute value bounded by*

$$\frac{|a_1| \cdots |a_n|}{|a_i|}.$$

Proof. Applying Hadamard's inequality to M_{ij}, and denoting by $a'_i \in \mathbb{C}^{n-1}$ the vector obtained from a_i after deleting the j-th entry, we have that

$$|\det M_{ij}| \leq \prod_{k\neq i} |a'_k| \leq \prod_{k\neq i} |a_k| = \frac{|a_1| \cdots |a_n|}{|a_i|}.$$

The thesis follows multiplying by $(-1)^{i+j}$ and transposing. □

7.2. **A bound for the height.** To estimate the height of $H+P$ we use an argument based on linear algebra, and some bounds on heights from Subsection 2.2.

Let H be a component of the algebraic subgroup defined by the $s \times N$ matrix with rows $u_1, \dots, u_s \in \mathbb{Z}^N$. Let $\Lambda \subseteq \mathbb{R}^N$ be the associated lattice, and $\Lambda^\perp$ its orthogonal lattice. Let $u_{s+1}, \dots, u_N$ be a basis of $\Lambda^\perp$ such that $|u_{s+1}|, \dots, |u_N|$ are the successive minima of $\Lambda^\perp$, as defined in Subsection 2.3.

The $(N-s) \times N$ matrix with rows $u_{s+1}, \dots, u_N$ defines an algebraic subgroup $H^\perp$, and for any point $P \in E^N$ there are two points $P_0 \in H$, $P^\perp \in H^\perp$, unique up to torsion points in $H \cap H^\perp$, such that $P = P_0 + P^\perp$.

Let U be the $N \times N$ matrix with rows $u_1, \dots, u_N$, and let Δ be its determinant. Notice that

$$|\Delta| = \det \Lambda \cdot \det \Lambda^\perp$$

because Λ and $\Lambda^\perp$ are orthogonal.

We remark that $u_i(P_0) = 0$ for all $i = 1, \dots, s$, because $P_0 \in H$, and $u_i(P^\perp) = 0$ for all $i = s+1, \dots, N$ because $P^\perp \in H^\perp$.

Therefore

$$UP^\perp = \begin{pmatrix} u_1(P^\perp) \\ \vdots \\ u_s(P^\perp) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} u_1(P_0 + P^\perp) \\ \vdots \\ u_s(P_0 + P^\perp) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} u_1(P) \\ \vdots \\ u_s(P) \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

hence

$$[\Delta]P^{\perp} = U^*UP^{\perp} = U^* \begin{pmatrix} u_1(P) \\ \vdots \\ u_s(P) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where U^* is the adjugate matrix of U from Definition 7.1.

Computing canonical heights and applying Lemma 7.2 yields

$$|\Delta|^2 \, \hat{h}(P^{\perp}) = \hat{h}([\Delta]P^{\perp}) \leq N \, |u_1|^2 \cdots |u_N|^2 \sum_{i=1}^{s} \frac{\hat{h}(u_i(P))}{|u_i|^2}.$$

Recall inequality (12), which gives

$$\mu(H+P) \leq 3\hat{\mu}(H+P) + c_3(E,N),$$

where $c_3(E,N)$ was defined as

$$c_3(E,N) = N(3h_{\mathcal{W}}(E) + 6\log 2 + \frac{1}{2}\log 3).$$

By [Phi12] we know that

$$\hat{\mu}(H+P) = \hat{h}(P^{\perp})$$

and therefore, by Zhang's inequality

$$\begin{aligned} h(H+P) &\leq (N-s+1)(\deg H)\mu(H+P) \leq \\ &\leq (N-s+1)(\deg H)(3\hat{\mu}(H+P) + c_3(E,N)) \leq \\ &\leq (N-s+1)(\deg H)(3\hat{h}(P^{\perp}) + c_3(E,N)) \leq \\ &\leq (N-s+1)\deg H \left(\frac{3N}{|\Delta|^2} \, |u_1|^2 \cdots |u_N|^2 \sum_{i=1}^{s} \frac{\hat{h}(u_i(P))}{|u_i|^2} + c_3(E,N) \right). \end{aligned} \tag{26}$$

By (14) we get

$$\deg H \leq c_4(N,s) \prod_{i=1}^{s} |u_i|^2,$$

by (15) we obtain

$$\frac{\deg H}{(\det \Lambda)^2} \leq c_4(N,s) \frac{4^s}{\omega_s^2},$$

and by Minkowski's second theorem

$$\frac{\prod_{i=s+1}^{N} |u_i|}{\det \Lambda^{\perp}} \leq \frac{2^{N-s}}{\omega_{N-s}}.$$

Plugging these inequalities in (26) we obtain

$$h(H+P) \leq \frac{3N(N-s+1)4^N}{(\omega_{N-s}\omega_s)^2} c_4(N,s) \prod_{i=1}^{s} |u_i|^2 \sum_{i=1}^{s} \frac{\hat{h}(u_i(P))}{|u_i|^2} + c_3(E,N)(N-s+1)c_4(N,s) \prod_{i=1}^{s} |u_i|^2.$$

So, we have proved the following proposition

Proposition 7.3. *Let E be a non CM elliptic curve. Let $H \subseteq E^N$ be a component of the algebraic subgroup associated with an $s \times N$ matrix with rows $u_1, \ldots, u_s \in \mathbb{Z}^N$. Then*

$$h(H+P) \leq \frac{3N(N-s+1)4^N}{(\omega_{N-s}\omega_s)^2} c_4(N,s) \prod_{i=1}^{s} |u_i|^2 \sum_{i=1}^{s} \frac{\hat{h}(u_i(P))}{|u_i|^2} + c_6(E,N,s) \prod_{i=1}^{s} |u_i|^2,$$

where ω_n is defined at (13),

$$c_4(N,s) = 3^N N! \left(\frac{3}{2}(N+1)12^{N-1}\right)^s$$

and

$$c_6(E,N,s) = N(N-s+1)c_4(N,s)(3h_{\mathcal{W}}(E) + 6\log 2 + \frac{1}{2}\log 3).$$

7.3. **A bound for the degree.** Here we use an inductive geometric construction to bound the degree of a translate.

We first consider an algebraic subgroup given by a single equation in E^N. Then we apply the Segre embedding and see this subgroup as a subvariety of $\mathbb{P}_{3^N-1}$. In doing this we must be careful in selecting irreducible components. Finally we apply inductively Bézout's theorem for the case of several equations.

Let U be a matrix in $\mathrm{Mat}_{s\times N}(\mathbb{Z})$ with rows $u_1,\dots,u_s \in \mathbb{Z}^N$ and let $H \subseteq E^N$ be an irreducible component of the algebraic subgroup associated with the matrix U (see Subsection 2.3).

If $X_1 = (x_1,y_1),\dots,X_N = (x_N,y_N)$ are points on E and $v = (v_1,\dots,v_N) \in \mathbb{Z}^N$ is a vector, we denote $v(\mathbf{X}) = v_1X_1 + \ldots + v_NX_N$.

As remarked in the previous section, $v(\mathbf{X}) = (x(v(\mathbf{X})), y(v(\mathbf{X})))$ is a point in E and $x(v(\mathbf{X}))$ is a rational function of the x_i, y_i's.

Let now $P = (P_1,\dots,P_N) \in E^N$ be a point. Take the k-th row $u_k \in \mathbb{Z}^N$ of U and consider the equation

$$x(u_k(\mathbf{X})) = x(u_k(P))$$

with $\mathbf{X} = (X_1,\dots,X_N) \in E^N$ as before.

Clearing out the denominators the previous equation can be written as

$$f_{u_k,P}(x_1,y_1,\dots,x_N,y_N) = 0,$$

where $f_{u_k,P}$ is a polynomial of degree bounded by $d(u_k)$ (see formula (24)).

This polynomial defines a variety in $\mathbb{P}_2^N$. Applying the Segre embedding, we want to study this variety as a subvariety of $\mathbb{P}_{3^N-1}$.

The Segre embedding induces a morphism between the fields of rational functions, whose effect on the polynomials in the variables $(x_1,y_1,\dots,x_N,y_N)$ is simply to replace any monomial in the variables of $\mathbb{P}_2^N$ with another monomial in the new variables, without changing the coefficients; the total degree in the new variables is the sum of the partial degrees in the old ones.

Recall that in Subsection 2.1 we defined $X(E,N)$ as the image of E^N in $\mathbb{P}_{3^N-1}$.

Denote by $Y_k' \subseteq \mathbb{P}_{3^N-1}$ the zero-set of the polynomial $f_{u_k,P}(x_1,y_1,\dots,x_N,y_N)$ after embedding $\mathbb{P}_2^N$ in $\mathbb{P}_{3^N-1}$.

Now consider an irreducible component of the translate in E^N defined by

$$u_k(\mathbf{X}) = u_k(P)$$

and denote by Y_k its image in $\mathbb{P}_{3^N-1}$. We want to obtain bounds for the degree of the hypersurfaces Y_k.

Notice that

$$Y_k \subseteq Y_k' \cap X(E,N)$$

and it is a component. This is because setting the first coordinate of $u_k(\mathbf{X})$ equal to $x(u_k(P))$ defines two cosets, $u_k(\mathbf{X}) = u_k(P)$ and $u_k(\mathbf{X}) = -u_k(P)$.

By Bézout's theorem

$$\deg Y_k \leq \deg X(E,N) \deg Y_k' \leq c_1(N)\frac{3}{2}12^{N-1}\left(N + |u_k|^2\right),$$

where the last inequality follows from formula (25) and the definition of $c_1(N)$ in Lemma 2.1.

In a similar way, considering all the rows we get

$$\deg(H+P) \leq \deg X(E,N) \deg Y_1' \cdots \deg Y_s' \leq c_1(N) \left(\frac{3}{2} 12^{N-1}\right)^s \prod_{i=1}^s (|u_i|^2 + N) \leq$$

$$\leq c_1(N) \left(\frac{3}{2}(N+1) 12^{N-1}\right)^s \prod_{i=1}^s |u_i|^2 \tag{27}$$

where we recall that, from relation (1), $c_1(N) = 3^N N!$.

Remark 7.4. *Clearly the degree of $H+P$ is equal to the degree of H and does not depend on P. Thus we can deduce the value of the constant $c_4(N,r)$ of Subsection 2.3, formula* (14)*, when the elliptic curve E is non CM; by the previous inequality, we may take*

$$c_4(N,r) = 3^N N! \left(\frac{3}{2}(N+1) 12^{N-1}\right)^r. \tag{28}$$

7.4. **Geometry of numbers.** In this subsection, inspired by the work of Habegger [Hab08], we give two lemmas based on tools from the geometry of numbers which are used to define H. We have the following version for powers of elliptic curves of Lemma 1 in [Hab08].

Lemma 7.5. *Let $1 \leq m \leq N$ be integers and let $P = (P_1, \dots, P_N) \in B \subseteq E^N$, where B is a torsion variety of dimension $\leq m$ and E is non CM.*

There exist linear forms $L_1, \dots, L_m \in \mathbb{R}[X_1, \dots, X_N]$ such that $|L_j| \leq 1 \quad \forall j$, where $|L_j|$ is the euclidean norm of the vector of the coefficients of L_j, and

$$\hat{h}(t_1 P_1 + \dots + t_N P_N) \leq c_{16}(N,m) \max_{1 \leq j \leq m} \{|L_j(\mathbf{t})|^2\} \hat{h}(P)$$

for all $\mathbf{t} = (t_1, \dots, t_N) \in \mathbb{Z}^N$. The constant $c_{16}(N,m)$ is given by

$$c_{16}(N,m) = \frac{m^3 (m!)^4 N}{4^{m-1}}.$$

Proof. The points P_i lie in a finitely generated subgroup of E of rank at most m.

By [Via03], Lemma 3, there are elements $g_1, \dots, g_m \in E$, and torsion points $\zeta_1, \dots, \zeta_N \in E$, such that

$$P_i = \zeta_i + v_{i1} g_1 \cdots + v_{im} g_m \quad \text{for } i = 1, \dots, N \text{ and some } v_{ij} \in \mathbb{Z}$$

and

$$\hat{h}(b_1 g_1 + \dots + b_m g_m) \geq \frac{2^{2m-2}}{m^2 (m!)^4} \max_{1 \leq i \leq m} \{|b_i|^2 \hat{h}(g_i)\} \quad \forall \mathbf{b} \in \mathbb{Z}^m.$$

Let $A = \max_{i,j} \{|v_{ij}|^2 \hat{h}(g_j)\}$ and define

$$\begin{aligned} \tilde{L}_j &= v_{1j} X_1 + \dots + v_{Nj} X_N & j &= 1, \dots, m \\ L_j &= \left(\frac{\hat{h}(g_j)}{NA}\right)^{\frac{1}{2}} \tilde{L}_j & j &= 1, \dots, m. \end{aligned}$$

Notice that we can assume $A > 0$, otherwise the point P would be a torsion point, and the thesis of the lemma would be trivially true. Notice also that $|L_j| \leq 1$.

With these definitions, for every $\mathbf{t} \in \mathbb{Z}^N$ we have that

$$t_1 P_1 + \dots + t_N P_N = \xi + \sum_{i=1}^m \tilde{L}_j(\mathbf{t}) g_j$$

where ξ is a torsion point. Therefore

$$\hat{h}(t_1P_1 + \cdots + t_NP_N) = \hat{h}\left(\sum_{j=1}^{m} \tilde{L}_j(\mathbf{t})g_j\right) \leq \sum_{j=1}^{m} |\tilde{L}_j(\mathbf{t})|^2 \hat{h}(g_j) =$$

$$= NA\sum_{j=1}^{m} |L_j(\mathbf{t})|^2 \leq mNA \max_{1\leq j\leq m}\{|L_j(\mathbf{t})|^2\}. \tag{29}$$

If i_0, j_0 are the indices for which the maximum is attained in the definition of A, then

$$\frac{2^{2m-2}}{m^2(m!)^4}A = \frac{2^{2m-2}}{m^2(m!)^4}|v_{i_0j_0}|^2\hat{h}(g_{j_0}) \leq \hat{h}(P_{i_0}) \leq \hat{h}(P).$$

Combining this with inequality (29), we get the thesis of the lemma. □

We now recall the following lemma of Habegger ([Hab08], Lemma 3), obtained applying Minkowski's second theorem.

Lemma 7.6. *Let $1 \leq m \leq N$ and let $L_1, \ldots, L_m \in \mathbb{R}[X_1, \ldots, X_N]$ be linear forms with $|L_j| \leq 1 \quad \forall j$. If $T \geq 1$, then for any integer s with $1 \leq s \leq n$ there exist linearly independent $u_1, \ldots, u_s \in \mathbb{Z}^N$ such that $|u_1|\cdots|u_s| \leq T$ and*

$$|u_1|\cdots|u_s|\frac{L_j(u_k)}{|u_k|} \leq c_{17}(N,m)T^{1-\frac{N}{ms}}$$

for $1 \leq j \leq m$ and $1 \leq k \leq s$ and

$$c_{17}(N,m) = \binom{m+N}{N}^{1/2}\frac{4^N}{\omega_N}.$$

The value of $c_{17}(N,m)$ follows from formulae (27) and (28) in the proof of [Hab08], *Lemma 2.*

7.5. **The proofs of Propositions 3.1 and 3.2.**

7.5.1. *The non-CM case.*

Proof of Proposition 3.1. By Lemma 7.5, and Lemma 7.6 applied to $\sqrt{T}$, there are linearly independent vectors $u_1, \ldots, u_s \in \mathbb{Z}^N$ such that

$$|u_1|^2\cdots|u_s|^2 \leq T \tag{30}$$

and

$$\left(\frac{|u_1|\cdots|u_s|}{|u_k|}\right)^2\hat{h}(u_k(P)) \leq c_{16}(N,m)c_{17}(N,m)^2T^{1-\frac{N}{ms}}\hat{h}(P).$$

If we consider the algebraic subgroup defined by equations $u_k(\mathbf{X}) = 0$, and call H the irreducible component containing 0, then, combining (30) and (27), its degree is bounded as

$$\deg(H + P) \leq c_4(N,s)T$$

and we can use Proposition 7.3 to bound the height of $H + P$ as

$$h(H+P) \leq \frac{3sN(N-s+1)4^N}{(\omega_s\omega_{N-s})^2}c_4(N,s)c_{16}(N,m)c_{17}(N,m)^2T^{1-\frac{N}{ms}}\hat{h}(P)+c_6(E,N,s)T.$$

□

7.5.2. *The CM case.*

Proof of Proposition 3.2. If the elliptic curve is CM, one can still apply the arguments of Section 7. More precisely, the geometric arguments of Subsection 7.3 do not depend on E having CM, one only needs to replace the application of formula (25) with the corresponding bound for the CM case, as discussed in Remark 6.1.

The argument of Subsection 7.2 assumes that $\mathrm{End}(E) = \mathbb{Z}$ because it uses the formulae from Subsection 2.3, which are straightforward consequences of the second Minkowski's theorem, here stated in the classical form for a lattice in $\mathbb{R}^N$. Analogous inequalities may be derived, when $\mathrm{End}(E)$ is an order in an imaginary quadratic number field, from more general reformulations of Minkowski's theorem, such as Theorem 3 of [BV83]. The linear algebra used in Subsection 7.2 remains the same if the entries of the matrix lie in $\mathbb{C}$ instead of $\mathbb{R}$.

Of the two lemmas in Subsection 7.4, Lemma 7.6 holds regardless of whether E is CM, while in Lemma 7.5 it is necessary to replace [Via03], Lemma 3 with the Proposition 2 of [Via03]. This proves Proposition 3.2. □

Acknowledgments

We thank P. Habegger for useful discussions and for bringing to our attention the construction in [Hab08]. We thank the referee for his remarks, that gave us the opportunity to improve our paper. We warmly thank the FNS for the financial support and for optimal working conditions.

References

[AV12] Francesco Amoroso and Evelina Viada, *Small points on rational subvarieties of tori*, Comment. Math. Helv. **87** (2012), no. 2, 355–383. MR 2914852

[BGS94] Jean-Benoît Bost, Henri Gillet, and Christophe Soulé, *Heights of projective varieties and positive Green forms*, J. Amer. Math. Soc. **7** (1994), no. 4, 903–1027. MR 1260106 (95j:14025)

[BMZ07] Enrico Bombieri, David Masser, and Umberto Zannier, *Anomalous subvarieties—structure theorems and applications*, Int. Math. Res. Not. IMRN (2007), no. 19, Art. ID rnm057, 33. MR 2359537 (2008k:11060)

[BV83] Enrico Bombieri and Jeffrey Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), no. 1, 11–32.

[CVV14] Sara Checcoli, Francesco Veneziano, and Evelina Viada, *On torsion anomalous intersections*, Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. **25** (2014), no. 1, 1–36.

[CV14] Sara Checcoli and Evelina Viada, *On the torsion anomalous conjecture in CM abelian varieties*, Pacific J. Math. **271** (2014), no. 2, 321–345.

[Hab08] Philipp Habegger, *Intersecting subvarieties of $\mathbb{G}_m^n$ with algebraic subgroups*, Math. Ann. **342** (2008), no. 2, 449–466. MR 2425150 (2009f:14044)

[Hab09.a] Philipp Habegger, *On the Bounded Height Conjecture*, Int. Math. Res. Not. IMRN (2009); doi: 10.1093/imrn/rnn149

[Hab09.b] Philipp Habegger, *Intersecting subvarieties of abelian varieties with algebraic subgroups of complementary dimension*, Invent. Math. 176 (2009), no. 2, 405-447

[Kul99] Leopoldo Kulesz, *Application de la méthode de Dem′janenko-Manin à certaines familles de courbes de genre 2 et 3*, J. Number Theory **76** (1999), no. 1, 130–146. MR 1688176 (2000c:11102)

[Mau08] Guillaume Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. **341** (2008), no. 4, 789–824. MR 2407327 (2009g:14026)

[MW93] David Masser and Gisbert Wüstholz, *Periods and minimal abelian subvarieties*, Ann. of Math. (2) **137** (1993), no. 2, 407–458. MR 1207211 (94g:11040)

[Phi91] Patrice Philippon, *Sur des hauteurs alternatives. I*, Math. Ann. **289** (1991), no. 2, 255–284.

[Phi95] Patrice Philippon, *Sur des hauteurs alternatives. III*, J. Math. Pures Appl. (9) **74** (1995), no. 4, 345–365. MR 1341770 (97a:11098)

[Phi12] Patrice Philippon, *Sur une question d'orthogonalité dans les puissances de courbes elliptiques*, (preprint), 2012 (hal–00801376).

[PM10] Bjorn Poonen and William McCallum, *The method of Chabauty and Coleman*, Explicit methods in number theory; rational points and diophantine equations, Panoramas et Synthèses **36**, Société Math. de France (2012), 99–117.

[Rém09] Gaël Rémond, *Intersection de sous-groupes et de sous-variétés III*, Comment. Math. Helv. **84** (2009), 835–863.

[Ser89] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. MR 1002324 (90e:11086)

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 817210 (87g:11070)

[Sil90] Joseph H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743. MR 1035944 (91d:11063)

[Via03] Evelina Viada, *The intersection of a curve with algebraic subgroups in a product of elliptic curves*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **2** (2003), no. 1, 47–75. MR 1990974 (2004c:11099)

[Via08] Evelina Viada, *The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve*, Algebra Number Theory **2** (2008), no. 3, 249–298. MR 2407116 (2009f:11079)

[Via09] Evelina Viada, *Nondense subsets of varieties in a power of an elliptic curve*, Int. Math. Res. Not. IMRN (2009), no. 7, 1214-1246.

[Zim76] Horst Günter Zimmer, *On the difference of the Weil height and the Néron-Tate height*, Math. Z. **147** (1976), no. 1, 35–51. MR MR0419455 (54 #7476)

Sara Checcoli: Institut Fourier, 100 rue des Maths, BP74 38402 Saint-Martin-d'Hères Cedex, France. email: sara.checcoli@ujf-grenoble.fr

Francesco Veneziano: Mathematisches Institut, Universität Basel, Spiegelgasse 1, CH-4051 Basel, Switzerland. email: francesco.veneziano@unibas.ch

Evelina Viada: Mathematisches Institut, Georg-August Universität Göttingen, Bunsenstraße 3-5, D-37073 Göttingen, Germany. email: viada@uni-math.gwdg.de