Canad. J. Math. Vol. 70 (5), 2018 pp. 1173–1200
http://dx.doi.org/10.4153/CJM-2017-045-0

An Explicit Manin-Dem'janenko Theorem in Elliptic Curves

Evelina Viada

Abstract. Let $\mathcal{C}$ be a curve of genus at least 2 embedded in $E_1 \times \cdots \times E_N$, where the E_i are elliptic curves for $i = 1, \ldots, N$. In this article we give an explicit sharp bound for the Néron–Tate height of the points of $\mathcal{C}$ contained in the union of all algebraic subgroups of dimension $< \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}})$, where $t_{\mathcal{C}}$ (resp. $r_{\mathcal{C}}$) is the minimal dimension of a translate (resp. of a torsion variety) containing $\mathcal{C}$.

As a corollary, we give an explicit bound for the height of the rational points of special curves, proving new cases of the explicit Mordell Conjecture and in particular making explicit (and slightly more general in the CM case) the Manin–Dem'janenko method for curves in products of elliptic curves.

1 Introduction

By *variety* we mean a projective variety defined over the algebraic numbers $\overline{\mathbb{Q}}$. If not otherwise specified, we identify V with its algebraic points $V(\overline{\mathbb{Q}})$. We denote by E an elliptic curve and by A an abelian variety. For a positive integer N, we denote by E^N the cartesian product of N copies of E. We denote by $\mathrm{End}(E)$ the ring of endomorphism of E.

We say that a subvariety $V \subset A$ is a *translate* (resp. a *torsion variety*) if it is a finite union of translates of algebraic subgroups of A by points (resp. by torsion points).

Furthermore, an irreducible variety $V \subset A$ is *transverse* (resp. *weak-transverse*) if it is not contained in any proper translate (resp. in any proper torsion variety).

In this article, the word *rank* is used with several different meanings. For clarity, we recall that the rank of an abelian group of finite type is the number of generators over $\mathbb{Z}$ of its free part; the rank of an R-module M for R an integral domain with field of fraction $\mathrm{frac}(R)$ is the dimension of the vector space $M \otimes_R \mathrm{frac}(R)$; the k-rank of an abelian variety A defined over k, for k a number field, is the rank of $A(k)$ as an abelian group; and the rank of a point on an abelian variety A is the only new concept introduced in Definition 1.1.

A classical question in the context of Diophantine Geometry is to determine the points on a curve of a certain shape, for instance the rational points. Much work has been done in this direction. In a fundamental work, Faltings [Fal83] proved the Mordell Conjecture, namely that a curve of genus at least 2 defined over a number field k has only finitely many k-rational points.

Received by the editors May 17, 2017; revised October 15, 2017.
Published electronically January 24, 2018.
AMS subject classification: **11G50**, 14G40.
Keywords: height, elliptic curve, explicit Mordell conjecture, explicit Manin-Demjanenko theorem, rational points on a curve.

The innovative proof of this theorem is unfortunately not effective, in the sense that it does not give any information on how these points could be determined. By explicit method, we mean a statement that provides an explicit bound for the height of the rational points on a curve, thus also a method to find them. In this paper we provide such a bound for curves with a factor of the Jacobian isogenous to a product E^N with $E(\mathbb{Q})$ of rank at most $N-1$.

The classical effective methods for the Mordell Conjecture are, for instance, described by J. P. Serre in his book [Ser89, Chapter 5], and they can be used for some collection of curves to give their rational points. The Chabauty–Coleman method [Cha41, Col85] provides a sharp bound for the number of rational points on a curve transverse in an abelian variety of dimension strictly larger than its rank (here the varieties are defined over $\mathbb{Q}$). We refer to McCallum and Poonen [MP10] and Stoll [Sto11] and their references for overviews on the method and for examples of curves of genus 2, where the Chabauty–Coleman method can be used, in combination with some descent argument, for finding their rational points. Another effective method is given by Manin and Dem'janenko ([Dem68,Man69]); it applies to curves defined over a number field k that admit m different k-independent morphisms towards an abelian variety A defined over k with rank of $A(k) < m$. However, the method does not give an explicit dependence of the height of the k-rational points either in terms of the curve or in terms of the morphisms. Thus, to apply the method, such a dependence must be elaborated example by example. Some examples are given by Kulesz [Kul99] and Kulesz, Matera, and Schost [KMS04] for some curves with Jacobian isogenous to a product of special elliptic curves of rank one if the genus of the curve is 2 and of rank two if the genus is 3.

Using diophantine approximation to solve diophantine equations is a classical approach that goes back at least to Thue and Siegel and includes important results of many mathematicians. New insight to this topic has been brought by Bombieri, Masser, and Zannier [BMZ99] in the framework of anomalous intersections. They showed that the set of points of rank at most $N-2$ on a curve transverse in the torus $(\overline{\mathbb{Q}}^*)^N$ is finite. The rank of a point in an abelian variety is defined as follows, and an analogous definition can be given in semi-abelian varieties.

Definition 1.1 The rank of a point in an abelian variety A is the minimal dimension of a torsion variety containing the point.

The several implications and connections between conjectures on anomalous intersections and classical conjectures can be found, for instance, in the book of Zannier [Zan12] and in the survey article of the author [Via15].

A fundamental aspect of the proof of Bombieri, Masser, and Zannier for curves in tori is that it is effective, in the sense that it gives a bound for the height of the points of rank at most $N-2$. This, however, does not give any information about the rational points of the curve, as the rank of $\mathbb{Q}^N$ is not finite. In [Via03], the author extended their method to transverse curves in a product of N elliptic curves with CM. An interesting feature of her proof is that it gives a method to bound the height of the points of rank $\leq N-2$. However, as for the effective methods mentioned above, it is

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

far from being explicit, and it is completely not uniform, as the dependence on $\mathcal{C}$ and E is not specified and depends on special intersection numbers and height functions.

In [CV14, Corollary 1.6], S. Checcoli and the author used a Lehmer type bound to prove a uniform bound for the height of the points of rank $< N/2$ on weak-transverse curves in E^N, where E has CM. Furthermore, in [Via15, Theorem 6.4] the author proved a similar bound for points of rank $\leq N-1$ on transverse curves in E^N, where E has CM. The bounds are explicit in the dependence on $\mathcal{C}$ but not in the dependence on E^N. The method cannot be extended to the non CM case, as a Lehmer type bound is not known in this case. Moreover, the CM case is difficult to make explicit. The recent explicit bounds for the CM elliptic case by Winckler [Win17], even under GRH, are unfortunately too big to be implemented.

In recent years, S. Checcoli, F. Veneziano, and the author have been working to approach the problem with explicit methods aiming to prove new cases of the explicit Mordell Conjecture and to eventually find all the rational points on some curves. In [CVV17, CVV16] joint with S. Checcoli and F. Veneziano, we give an explicit bound for the Néron–Tate height of the set of points of rank one on curves of genus at least two in E^N, where E is without CM. The non-CM assumption is technical and there we handled the easier case where the endomorphism ring of E is $\mathbb{Z}$.

In this article, we generalize the result of [CVV17] in two directions. First we present the explicit computations needed to extend the method introduced in [CVV17] to the case of E with CM. This is done in Proposition 5.1. To prove this proposition, we give some estimates on the degrees of morphisms on E^N, where E has CM. Then using the geometry of numbers and in particular Minkowski's second theorem over number fields, we extend the approximations done in [CVV17] to K-lattices, for K an imaginary quadratic field.

Secondly, we give an explicit bound for the Néron–Tate height of points of rank larger than one. More precisely, for points of rank $< N$ if $\mathcal{C}$ is a transverse curve in E^N and for points of rank $< \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}})$ if $\mathcal{C}$ has genus at least 2, and contained in a translate of minimal dimension $t_{\mathcal{C}}$ and in a torsion variety of minimal dimension $r_{\mathcal{C}}$. In particular, this applies to points of rank $< \max(N - t_{\mathcal{C}}, t_{\mathcal{C}})$ if $\mathcal{C}$ is weak-transverse in E^N and contained in a translate of minimal dimension $t_{\mathcal{C}}$.

For transverse curves the result is optimal with respect to the rank, while for weak-transverse curves it is not optimal. We recall that an effective result with the optimal rank $N-2$ in the weak-transverse case is an extremely deep statement that would imply the effective Mordell–Lang Conjecture for curves whose Jacobian is isogenous to E^N. This is well known to be a very challenging open problem.

We now introduce all the notation needed to state our main theorem. We first recall the definition of the two invariants just introduced above.

Definition 1.2 For a curve $\mathcal{C} \subset A$, we denote by $t_{\mathcal{C}}$ the minimal dimension of a translate containing $\mathcal{C}$ and by $r_{\mathcal{C}}$ the minimal dimension of a torsion variety containing $\mathcal{C}$.

Notice that for a transverse curve, $t_{\mathcal{C}} = r_{\mathcal{C}} = \dim A$ and for a weak-transverse curve, $r_{\mathcal{C}} = \dim A$.

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

Let E be an elliptic curve. We fix a Weierstrass equation

$$y^2 = x^3 + Ax + B, \tag{1.1}$$

with A and B algebraic integers. Let Δ and j be the discriminant and j-invariant of E. Let $\mathrm{End}(E)$ be the ring of endomorphisms of E, K its field of fractions and D_K its discriminant. We embed E^N into $\mathbb{P}_2^N$ via the affine equation (1.1) and then via the Segre embedding in $\mathbb{P}_{3^N-1}$. Let $\widehat{h}$ be the Néron-Tate height on E^N and h_W the absolute logarithmic Weil height in the projective space. The degree of a curve $\mathcal{C} \subset E^N$ is the degree of its image in $\mathbb{P}_{3^N-1}$; the normalised height $h_2(\mathcal{C})$ is defined in terms of the Chow form of the ideal of $\mathcal{C}$ as done in [Phi95] and $h(\mathcal{C})$ is the canonical height of $\mathcal{C}$, as defined in [Phi91] (see Section 2 for more details).

We can now state our main theorem.

Theorem 1.3 *Let $\mathcal{C} \subset E^N$ be a curve of genus at least 2. Let $K = \mathrm{frac}(\mathrm{End}(E))$ with discriminant D_K. For $\mathcal{O}_K$ the ring of integers of K, let $f = [\mathcal{O}_K : \mathrm{End}(E)]$. Then the set of points $P \in \mathcal{C}$ of rank $r < \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}})$ is a set of Néron-Tate height explicitly bounded as*

$$\widehat{h}(P) \le C_1(N,E)h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{t_{\mathcal{C}}-r}} + C_2(N,E)(\deg \mathcal{C})^{\frac{t_{\mathcal{C}}}{t_{\mathcal{C}}-r}} + C_3(N,E),$$

where the constants are explicitly computed.

More precisely,

$$\widehat{h}(P) \le \delta_1 h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{t_{\mathcal{C}}-r}} + \delta_1\big(t_{\mathcal{C}}^2 C(E) + C_0\big)(\deg \mathcal{C})^{\frac{t_{\mathcal{C}}}{t_{\mathcal{C}}-r}} + (N-r)t_{\mathcal{C}}^2 C(E);$$

furthermore, if $\mathcal{C}$ is transverse, then

$$\widehat{h}(P) \le \delta_2 h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{N-r}} + \delta_2(N^2 C(E) + C_0)(\deg \mathcal{C})^{\frac{N}{N-r}} + N^2 C(E),$$

where, for any integer $n \ge r$,

$$\begin{aligned}
\delta(n,r,f,D_K) &= n^2 n! 6^{2n}\big(6^{4n} n^6 (2n)!^4\big)^{\frac{r}{n-r}} f^{2+\frac{(n+r+4)r}{n-r}} |D_K|^{1+\frac{(n+r+4)r}{2(n-r)}},\\
\delta_1 &= (N-r)\delta\big(t_{\mathcal{C}}, r, f, |D_K|\big),\\
\delta_2 &= \delta\big(N, r, f, |D_K|\big),\\
C(E) &= \frac{h_W(\Delta) + 3h_W(j)}{4} + \frac{h_W(A) + h_W(B)}{2} + 4
\end{aligned}$$

with Δ and j are the discriminant and j-invariant of E and C_0 is given in (6.3).

Sharper but less friendly constants are given in Theorems 6.1 and 6.2.

An interesting aspect of the theorem is that the field of definition of $\mathcal{C}$ and of the points P do not play any role in the bounds. This is a more general setting with respect to the Mordell–Lang problem, where the number field of definition is fixed.

As remarked in several works, the proof of Theorem 1.3 for points of a certain rank also works similarly for curves in a product of elliptic curves $E_1 \times \cdots \times E_N$ instead of E^N. It this case it simply happens that some of the coefficients of the linear forms defining an algebraic subgroup are zero. So Theorem 1.3 holds in $E_1 \times \cdots \times E_N$, where we fix equations of the type (1.1) for every E_i. Using the universal property of the

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

Jacobian one can easily state our theorems for curves with a factor of the Jacobian isogenous to $E_1 \times \cdots \times E_N$.

The proof of a sharper version of Theorem 1.3 is given is Section 6. We divide the theorem into two parts. The first one, given in Theorem 6.1, treats the case of a transverse curve. This is proved with typical tools of diophantine approximation, based on some estimates for degree and heights done in Section 4 and some refined argument of geometry of numbers presented in Section 5. The second part is given in Theorem 6.2. Via a geometric induction argument, we reduce the general case to the case of a transverse curve. Theorem 1.3 is then a reformulation of Theorems 6.1 and 6.2, where we compute the constants more explicitly.

Theorem 1.3 can be easily used to describe the height of rational points of curves in E^N under some conditions on the rank of the group $E(\mathbb{Q})$. We prove the following cases of the explicit Mordell Conjecture.

Corollary 1.4 *Let k be a number field of definition of E. Consider the* $\mathrm{End}(E)$*-module M generated by the points in $E(k)$. Assume that M has rank $r < \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}})$ (where $r = \dim_K M \otimes_{\mathrm{End}(E)} K$). Then the set of k-rational points $\mathcal{C}(k)$ has Néron–Tate height bounded as*

$$\widehat{h}(P) \le \delta_1 h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{t_{\mathcal{C}}-r}} + \delta_1\big(t_{\mathcal{C}}^2 C(E) + C_0\big)(\deg \mathcal{C})^{\frac{t_{\mathcal{C}}}{t_{\mathcal{C}}-r}} + (N-r)t_{\mathcal{C}}^2 C(E),$$

where notation and constants are the same as in Theorem 1.3.

Clearly, if the ring generated by the coordinates of $E(k)$ has rank as $\mathrm{End}(E)$-module at most r, then all points in $\mathcal{C}(k)$ have rank at most r in the sense of Definition 1.1. So our main theorem directly implies Corollary 1.4. This is the most general result we have obtained in the context of the explicit Mordell Conjecture, and it is not covered by any of our previous results; specifically, we had explicit results only for points of rank one in the non CM case.

Note that, by the Mordell–Weil Theorem, $E(k)$ is a finitely generated abelian group whose torsion-free part has r generators if $\mathrm{End}(E) = \mathbb{Z}$ and $2r$ generators if $\mathrm{End}(E) = \mathbb{Z} + \tau\mathbb{Z}$. Thus, to apply our theorem for transverse curves it is sufficient to assume that E^N has smaller k-rank (in the sense of number of generators of $E^N(k)$) than N^2 in the non-CM case and smaller than $2N^2$ in the CM case. In particular (in the CM case), this extends and makes explicit the Manin and Dem'janenko method for curves transverse in E^N. The coordinates morphisms restricted to the curve give the independent morphisms toward the elliptic curve E required by the Manin–Dem'janenko method. For E without CM, our assumption, and the Manin–Dem'janenko assumption on the rank are the same; in the CM case, our assumption is $\mathrm{rank}(E(k) < 2N$, while the Manin-Dem'janenko assumption is $\mathrm{rank}(E(k)) < N$.

We finally remark that the Chabauty–Coleman method in our setting of a product of elliptic curves becomes trivial; indeed, their assumption is that the rank of $E^N(\mathbb{Q})$ is smaller than $N - 1$. This implies that E has rank zero, and in a product of elliptic curves that at least one factor has rank zero. Then a simple use of the Arithmetic Bézout Theorem immediately gives a bound for the height of the rational points on the curve.

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

In [CVV16], we gave a criterion for constructing transverse curves in E^2 where

$$y_1^2 = x_1^3 + Ax_1 + B \quad \text{and} \quad y_2^2 = x_2^3 + Ax_2 + B$$

are the equations of E^2 in $\mathbb{P}_2^2$ for affine coordinates $(x_1, y_1) \times (x_2, y_2)$. We showed that it is sufficient to cut a curve in E^2 with any polynomial of the form $p(x_1) = y_2$, where $p(x) \in \overline{\mathbb{Q}}[x]$. In [CVV16] our examples were given under the assumption that E is non CM. We can now extend them to any E, obtaining interesting new examples. In Section 6.3, we prove the following corollary.

Corollary 1.5 *Assume that E is defined over a number field k and that the ring generated by the coordinates of the points in $E(k)$ is an* $\mathrm{End}(E)$*-module of rank* 1*. Let $\mathcal{C}$ be the projective closure in E^2 of the affine curve cut by the additional equation*

$$p(x_1) = y_2,$$

with $p(x) = p_n x^n + \cdots + p_1 x + p_0 \in k[x]$ a non-constant polynomial of degree n having m non-zero coefficients.

Then every point $P \in \mathcal{C}(k)$ has Néron–Tate height bounded as

$$\widehat{h}(P) \le 3^2 \cdot 2^{40} f^9 |D_K|^{\frac{9}{2}} \big(h_W(p) + \log m + 3C(E) + 6 \big) (2n+3)^2 + 4C(E)$$

where $h_W(p) = h_W(1 : p_0 : \cdots : p_n)$ is the height of the polynomial $p(x)$ and the constants $C(E)$, f and D_K are defined in Theorem 1.3*.*

We finally remark that in [Via08] the author proved that the set of points of rank $N-2$ on a weak-transverse curve $\mathcal{C}$ in E^N has bounded height; the proof is not effective and it uses in a non effective way the Vojta inequality, as it is used in the proof of the Mordell–Lang Conjecture. However, in [Via03] the finiteness of the points of $\mathcal{C}$ of rank $\le N-2$ is effective and the bound on their number depends on $\mathcal{C}$, E, N and on the bound for their height in an effective way. In Section 6.4, we use our Theorem 1.3, [Via08, Theorem 1.3] and a projection argument to prove the following corollary.

Corollary 1.6 *For any curve $\mathcal{C}$ of genus at least two embedded in E^N, the set of points of $\mathcal{C}$ of rank $< \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}} - 1)$ has cardinality effectively bounded.*

We can also replace E^N by $E_1 \times \cdots \times E_N$, as explained above.

2 Preliminaries

In this section, we introduce the notations, and we recall several explicit relations between different height functions. We also recall some basic results in Arithmetic Geometry that play an important role in our proofs: Minkowski's second theorem, the Arithmetic Bézout Theorem, and the Zhang Inequality.

Let E be an elliptic curve defined over a number field k by a fixed Weierstrass equation $E : y^2 = x^3 + Ax + B$ with A and B in the ring of integers of k (this assumption is not restrictive). We denote the discriminant of E by

$$\Delta = -16(4A^3 + 27B^2)$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

and the j-invariant by

$$j = \frac{-1728(4A)^3}{\Delta}.$$

We consider E^N embedded in $\mathbb{P}_{3^N-1}$ via the composition map

$$E^N \hookrightarrow \mathbb{P}_2^N \hookrightarrow \mathbb{P}_{3^N-1}, \tag{2.1}$$

where the first map sends a point $(X_1, \dots, X_N)$ to $((x_1, y_1), \dots, (x_N, y_N))$ (the (x_i, y_i) being the affine coordinates of X_i in the Weierstrass form of E) and the second map is the Segre embedding. Degrees and heights are computed with respect to this fixed embedding.

2.1 Heights of Points

If $P = (P_1 : \cdots : P_n) \in \mathbb{P}_n(\overline{\mathbb{Q}})$ is a point in the projective space, then the absolute logarithmic Weil height of P is defined as

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

where K is a field of definition for P and $\mathcal{M}_K$ is its set of places. If $\alpha \in \overline{\mathbb{Q}}$, then the Weil height of α is defined as $h_W(\alpha) = h_W(1 : \alpha)$.

We also define another height that differs from the Weil height at the Archimedean places:

$$h_2(P) = \sum_{v \text{ finite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max_i \{|P_i|_v\} + \sum_{v \text{ infinite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \Big(\sum_i |P_i|_v^2 \Big)^{1/2}. \tag{2.2}$$

For a point $P \in E$ we denote by $\widehat{h}(P)$ its Néron–Tate height as defined in [Phi91] (which is one third of the usual Néron–Tate height used also in [CVV17]).

If $P = (P_1, \dots, P_N) \in E^N$, then for h equal to h_W, h_2 and $\widehat{h}$ we define

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

The following proposition directly follows from [Sil90, Theorem 1.1] and [CVV16, Proposition 3.2].

Proposition 2.1 *For $P \in E^N$,*

$$-NC(E) \le h_2(P) - \widehat{h}(P) \le NC(E),$$

where

$$C(E) = \frac{h_W(\Delta) + 3h_W(j)}{4} + \frac{h_W(A) + h_W(B)}{2} + 4.$$

Further details on the relations between the different height functions defined above can be found in [CVV16, Section 3].

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

2.2 Heights of Varieties

For a subvariety $V \subset \mathbb{P}_m$ we denote by $h_2(V)$ the normalised height of V defined in terms of the Chow form of the ideal of V, as in [Phi95]. This height extends the height h_2 defined for points by formula (2.2) (see [BGS94, equation (3.1.6)]). We also consider the canonical height $h(V)$, as defined in [Phi91]; when the variety V reduces to a point P, $h(P) = \widehat{h}(P)$ (see [Phi91, Proposition 9]).

2.3 The Degree of a Variety

The degree of an irreducible variety $V \subset \mathbb{P}_m$ is the maximal cardinality of a finite intersection $V \cap L$, where L is a linear subspace of dimension equal to the codimension of V. The degree is often conveniently computed as an intersection product.

If $X(E,N)$ is the image of E^N in $\mathbb{P}_{3^N-1}$ via the above map, then by [CVV17, Lemma 2.1] we have $\deg X(E,N) = 3^N N!$.

2.4 The Arithmetic Bézout Theorem

The following explicit result is proven by Philippon in [Phi95, Théorème 3]. It describes the behavior of the height for intersections.

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

$$\sum_{i=1}^{g} h_2(Z_i) \le \deg(X) h_2(Y) + \deg(Y) h_2(X) + C_0(\dim X, \dim Y, m) \deg(X) \deg(Y),$$

where

$$C_0(d_1, d_2, m) = \Big(\sum_{i=0}^{d_1} \sum_{j=0}^{d_2} \frac{1}{2(i+j+1)} \Big) + \Big(m - \frac{d_1 + d_2}{2} \Big) \log 2. \tag{2.3}$$

2.5 The Zhang Inequality

In order to state Zhang's inequality, we define the essential minimum $\mu_2(X)$ of an irreducible algebraic subvariety $X \subset \mathbb{P}_m$ as

$$\mu_2(X) = \inf \Big\{ \theta \in \mathbb{R} \;\Big|\; \{P \in X \mid h_2(P) \le \theta\} \text{ is Zariski dense in } X \Big\}.$$

The following result is due to Zhang [Zha95, Theorem 5.2].

Theorem 2.3 (Zhang inequality) *Let $X \subset \mathbb{P}_m$ be an irreducible algebraic subvariety. Then*

$$\mu_2(X) \le \frac{h_2(X)}{\deg X} \le (1 + \dim X) \mu_2(X).$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

We also define a different essential minimum for subvarieties of E^N, relative to the height function $\widehat{h}$:

$$\widehat{\mu}(X) = \inf\left\{\theta \in \mathbb{R} \;\middle|\; \{P \in X \mid \widehat{h}(P) \le \theta\} \text{ is Zariski dense in } X\right\}.$$

Using the definitions and a simple limit argument, one sees that Zhang's inequality holds also with $\widehat{\mu}$, namely

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

If X is an irreducible subvariety in E^N, using Proposition 2.1 we have

$$-NC(E) \le \mu_2(X) - \widehat{\mu}(X) \le NC(E), \tag{2.4}$$

where the constant $C(E)$ is defined in Proposition 2.1.

We finally remark that by definition of essential minimum, for a translate $H + P$, we have $\widehat{\mu}(H+P) \ge h(P^\perp)$, where $P^\perp$ is the component of P in $H^\perp$. Indeed the points $\mathrm{Tor}_H + P^\perp$ are dense in $H + P$. Moreover, equality holds by [Phi12] equality holds; thus,

$$h(P^\perp) = \widehat{\mu}(H + P) \le \frac{h(H+P)}{\deg H}.$$

2.6 Complex Multiplication

We denote by $\mathrm{End}(E)$ the ring of endomorphisms of E. We recall that an elliptic curve E is non-CM if $\mathrm{End}(E)$ is isomorphic to $\mathbb{Z}$, while E is CM if $\mathrm{End}(E)$ is isomorphic to an order in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K.

We will write $K = \mathbb{Q}(\sqrt{D})$, for some squarefree negative integer D, and we set $\theta = \sqrt{D}$ or $(1+\sqrt{D})/2$ so that $\mathcal{O}_K = \mathbb{Z}[\theta]$. If D is congruent to 1 modulo 4, then the discriminant D_K of K satisfies $D_K = D$. If D is not congruent to 1 modulo 4, then $D_K = 4D$.

Then $\mathrm{End}(E)$ is isomorphic to an order in $\mathcal{O}_K$, which we can write as $\mathbb{Z} + f\mathcal{O}_K$ for a positive integer f, called the *conductor* of the order. We set $\tau = f\theta$ so that $\mathrm{End}(E) = \mathbb{Z}[\tau]$.

2.7 Minkowski's Second Theorem

In this section we follow the notation and arguments of [BG06, Appendix 6]. A version of Minkowski's second theorem has been proved by Bombieri and Vaaler [BV83, Theorem 4], where they use it to prove Siegel's lemma over number fields.

Let K be an imaginary quadratic number field with ring of integers $\mathcal{O}_K$, and let r and N be positive integers. Let $\mathcal{O}$ be an order in $\mathcal{O}_K$. A K-lattice Λ of rank r is a torsion free finitely generated $\mathcal{O}$-module of rank r such that $\Lambda \otimes_{\mathcal{O}} K$ is a K-vector space of dimension r (see [BG06, Definition C.2.5]).

Fix compatible embeddings of K into $\mathbb{C}$. Consider a matrix $M \in \mathrm{Mat}_{r\times N}(\mathcal{O})$ of rank r. Then the rows of M generate a torsion free $\mathcal{O}$-module and so a K-lattice $\Lambda \subset \mathcal{O}^N \subset K^N$. Let $f = [\mathcal{O}_K : \mathcal{O}]$. We define the determinant of Λ to be $\det \Lambda =$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

$\sqrt{\det(M\overline{M}^t)}$, where $\overline{M}^t$ is the transpose of the complex conjugate of M. This is also the covolume of a fundamental domain of Λ.

The following is a special case of the Minkowski second theorem proved in [BV83, Theorem 3] and also in [BG06, Theorem C.2.11 and Section C.2.18].

Theorem 2.4 *Let K be an imaginary quadratic field with discriminant D_K and Λ a K-lattice of rank r over $\mathcal{O}$ with $f = [\mathcal{O}_K : \mathcal{O}]$ as defined above. Then there exist K-linearly independent elements $u_1, \dots, u_r \in \Lambda$ with euclidean norm $\|u_i\| = \lambda_i$ such that*

$$\omega_{2r}(\lambda_1 \cdots \lambda_r)^2 \leq 2^r f^r |D_K|^{r/2} (\det \Lambda)^2,$$

where $\omega_{2r} = \pi^r/r!$ is the volume of the unit ball in $\mathbb{R}^{2r}$.

Moreover, for $\Gamma = \langle u_1, \dots, u_r \rangle$ we have $[\Lambda : \Gamma] = c_0 \leq M_0 = (2f|D_K|^{1/2})^{\frac{r}{2}}/\omega_{2r}^{\frac{1}{2}}$ and $c_0\Lambda \subset \Gamma$.

Proof The proof follows [BG06, Appendix C.2.18]. Note that $\Lambda \otimes_{\mathcal{O}} K$ makes Λ a full K-lattice as defined by Bombieri and Vaaler. In addition Λ is embedded in $\mathrm{End}(E)^N$ and so in K^N. We choose the standard $\mathbb{Z}$-basis of $\mathcal{O}_K$ and then identify K^r with $\mathbb{Q}^{2r}$ and in turn see Λ embedded in K^N and $\mathbb{Q}^{2N}$. Then our K-lattice Λ can be viewed as an $\mathbb{R}$-lattice Λ_∞ of rank $2r$ embedded in $\mathbb{R}^{2N}$. The classical Minkowski Theorem tells us that there exist linearly independent elements v_i for $i = 1, \dots, 2r$ of Λ_∞ (defining the classical successive minima) such that

$$\omega_{2r}\|v_1\| \cdots \|v_{2r}\| \leq 4^r (\mathrm{vol}\, \Lambda_\infty).$$

A computation shows that

$$\mathrm{vol}(\Lambda_\infty) \leq (\mathrm{vol}\, \mathcal{O})^r \,\mathrm{vol}\, \Lambda^2,$$

where $\mathcal{O}$ is considered as a $\mathbb{Q}$-lattice of rank 2. In addition, $\mathrm{vol}\, \Lambda = \det \Lambda$ by definition, and

$$\mathrm{vol}\, \mathcal{O} = f \,\mathrm{vol}\, \mathcal{O}_K = f\frac{|D_K|^{1/2}}{2}$$

by classical results; see, for instance, [Neu99, Proposition 5.2] where his volume is twice our Lebesgue volume as he points out just above the proposition. Finally, from the v_i one can extract K-linearly independent elements $u_1, \dots, u_r$ of Λ such that $\|u_i\| \leq \|v_{2i-1}\|$. So $(\lambda_1 \cdots \lambda_r)^2 \leq \|v_1\| \cdots \|v_{2r}\|$ that together with the above bounds gives the theorem.

For the last claim simply note that $\mathrm{vol}\, \Gamma \leq \lambda_1 \cdots \lambda_r$ thus the index is bounded by the first part of the theorem. That $c_0\Lambda \subset \Gamma$ is a direct consequence of the fact that Λ/Γ is a finite abelian group of order c_0. ∎

Note that from the proof one sees that $\|u_i\| = \lambda_i$ are the uccessive minima of Λ, where the definition is as follows. Let S be the unitary complex ball of $\mathbb{C}^r$ with respect to the Lebesgue measure. The i-th successive minimum is

$$\lambda_i = \inf\{\lambda \geq 0 \mid \lambda \cdot S \text{ contains } i \text{ linearly independent vectors of } \Lambda\}.$$

This definition is equivalent to the one given in [BG06, C.2.9], as explained in [BV83, (3.2)].

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

2.8 Algebraic Subgroups

In this subsection, we recall the several different descriptions of the algebraic subgroups of E^N.

By the uniformization theorem there exists a unique lattice $\Lambda_0 \subset \mathbb{C}$ such that the map $\mathbb{C} \to \mathbb{P}^2(\mathbb{C})$ given by

$$z \longmapsto \begin{cases} [\wp_{\Lambda_0}(z) : \frac{1}{2}\wp'_{\Lambda_0}(z) : 1] & z \notin \Lambda_0, \\ [0:1:0] & z \in \Lambda_0, \end{cases}$$

induces an isomorphism $\mathbb{C}/\Lambda_0 \xrightarrow{\sim} E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ of complex Lie groups (see [Sil86, Theorem VI.5.1]. Here, $\wp_{\Lambda_0}$ denotes the Weierstrass $\wp$-function associated with the lattice Λ_0. The N-th power of this isomorphism gives the analytic uniformization

$$\wp_e : \mathbb{C}^N/{\Lambda_0}^N \xrightarrow{\sim} E^N(\mathbb{C})$$

of E^N. Note that $\mathbb{C}^N$ can be identified with the Lie algebra of $E^N(\mathbb{C})$ and the composition of the canonical projection $\pi : \mathbb{C}^N \to \mathbb{C}^N/{\Lambda_0}^N$, and $\wp_e$ can be identified with the exponential map of the Lie group $E^N(\mathbb{C})$. By [BG06, 8.9.8], the set of abelian subvarieties of E^N is in natural bijection with the set of complex vector subspaces $W \subset \mathbb{C}^N$ for which $W \cap {\Lambda_0}^N$ is a lattice of full rank in W. Such a W corresponds to the abelian subvariety B of E^N with $B(\mathbb{C}) = (\wp_e \circ \pi)(W)$, and we identify W with the Lie algebra of B.

The *orthogonal complement* of an abelian subvariety $B \subset E^N$ with Lie algebra $W_B \subset \mathbb{C}^N$ is the abelian subvariety $B^\perp$ with Lie algebra $W_B^\perp$, where $W_B^\perp$ denotes the orthogonal complement of W_B with respect to the canonical Hermitian structure of $\mathbb{C}^N$. Note that $W_B^\perp \cap {\Lambda_0}^N$ is a lattice of full rank in $W_B^\perp$ and its volume can be estimated using the Siegel Lemma over number fields of Bombieri and Vaaler [BV83].

Let B be an algebraic subgroup of E^N with $\operatorname{codim} B = r$. By [MW93, Lemma 1.3] there exists a morphism $\varphi_B : E^N \to E^r$ such that $\ker \varphi_B = B + \tau$ with τ a torsion set of cardinality T_0 absolutely bounded. In turn, φ_B is identified with a matrix in $\mathrm{Mat}_{r\times N}(\mathrm{End}(E))$ of rank r and, using the geometry of numbers, we can choose the matrix representing φ_B in such a way that the degree of $\ker \varphi_B$ is essentially the product of the squares of the norms of the rows of the matrix.

More precisely, given $B \subset E^N$ an algebraic subgroup of rank r, we associate it with a matrix of maximal rank r 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 K-lattice $\Lambda = \langle u_1, \dots, u_r \rangle_{\mathrm{End}(E)}$ for $K = \mathrm{frac}(\mathrm{End}(E))$. In Subsection 4.1, we show that

$$\deg B \le 3^N N! (12^{N-1}2)^r \prod_{i=1}^{r} \|u_i\|^2.$$

Combining this with Minkowski's second theorem recalled above, with $\mathcal{O} = \mathrm{End}(E)$ and $f = [\mathcal{O}_K : \mathrm{End}(E)]$ its conductor, we get

$$\frac{\deg B}{(\det \Lambda)^2} \le 3^N N! (12^{N-1}2)^r \frac{2^r f^r |D_K|^{\frac{r}{2}}}{\omega_{2r}}.$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

3 Estimates for the Degree of Morphisms

In this section, we give the preliminary bounds for the degree of an algebraic subgroup of E^N, where the embedding of E^N in the projective space is fixed as in (2.1).

An algebraic subgroup H of E^N of codimension s is defined by s equations

$$\begin{aligned} L_1(X_1,\dots,X_N) &= 0,\\ &\vdots\\ L_s(X_1,\dots,X_N) &= 0, \end{aligned}$$

where $L_i(X_1,\dots,X_N) = l_{i_1}X_1 + \cdots + l_{i_N}X_N$ are morphisms from E^N to E; here the coefficients $l_{i_j} \in \mathrm{End}(E)$ are expressed by certain rational functions; similarly 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 $\mathbb{P}_2$ $(x(L_i(\mathbf{X})), y(L_i(\mathbf{X})))$ that are rational functions of the x_is and y_is.

The purpose of this section is to study the rational functions $x(L_i(\mathbf{X}))$ and to bound the sums of their partial degrees.

3.1 Estimates for Degrees of Rational Functions

Recall that if f_i/g_i are rational functions, with f_i, g_i polynomials in several variables, we denote by $d(f_i/g_i)$ the maximum of the sums of the partial degrees of both f_i, g_i. Then

$$\frac{f}{g} = \prod_{i=1}^{r} \frac{f_i}{g_i}, \qquad d(f/g) \le \sum_{i=1}^{r} d(f_i/g_i), \tag{3.1}$$

$$\frac{f}{g} = \sum_{i=1}^{r} \frac{f_i}{g_i}, \qquad d(f/g) \le \sum_{i=1}^{r} d(f_i/g_i), \tag{3.2}$$

where $d(f/g)$ is the bound for the sum of partial degrees of the product (in (3.1)) and of the sum (in (3.2)) of the f_i/g_i's, respectively.

3.2 Estimates for Endomorphisms

In this section we are going to estimate the degree of the rational functions on E giving the multiplication by an element of $\mathrm{End}(E)$. Recall that if E has CM by τ and $\alpha \in \mathrm{End}(E)$, then $\alpha = m + n\tau$ for some integers m, n. We denote by $|\cdot|$ the complex absolute value. Notice that since α is an algebraic integer, $|\alpha| \ge 1$ for every $\alpha \neq 0$.

From the theory of elliptic functions we can deduce the following result. This will be used, together with other estimates for the non CM case, to bound the degree of an algebraic subgroup.

Lemma 3.1 *Let $P = (x, y)$ be a point in E and let $\alpha \in \mathrm{End}(E)$. Then*

$$\alpha(x, y) = \left(f(x), \frac{y f'(x)}{\alpha} \right)$$

with f a rational function with partial degrees bounded by $|\alpha|^2$.

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

In particular, the coordinates of $\alpha(x, y)$ are rational functions of x and y the sums of whose partial degrees are upper bounded by $2|\alpha|^2$ and lower bounded by $|\alpha|^2$.

Proof Let $\alpha \in \mathrm{End}(E)$. Then

$$\alpha(x, y) = \big(f(x) + yg(x), h(x) + yl(x)\big)$$

for f, g, h, l rational functions. Since the multiplication by α is an isogeny on E, we have that $\alpha(-P) = -\alpha P$ for every $P \in E$; thus,

$$\begin{aligned}\alpha(x, -y) &= \big(f(x) - yg(x), h(x) - yl(x)\big) = -\alpha(x, y)\\ &= \big(f(x) + yg(x), -h(x) - yl(x)\big)\end{aligned}$$

from which we deduce $g = h = 0$.

Notice that if $(x, y) = (\wp(z), \frac{1}{2}\wp'(z))$, with $\wp$ the Weiertrass $\wp$-function, then $\alpha(x, y) = (\wp(\alpha z), \frac{1}{2}\wp'(\alpha z))$. So we obtain $\alpha(x, y) = (f(x), yf'(x)/\alpha)$, where f is a rational function. Writing $f(x) = a(x)/b(x)$ with a, b polynomials, by [Cox89, Theorem 10.14], we have that $\deg a(x) = \deg b(x) + 1 = |\alpha|^2$. Therefore, the sums of the partial degrees of $f(x)$ and $yf'(x)$ are smaller than $2|\alpha|^2$ and bigger than $|\alpha|^2$. ■

3.3 Estimates for Group Morphisms

We first estimate the degree of an algebraic subgroup of codimension one, thus defined by one linear equation. Then we generalize the estimate to algebraic subgroups of any codimension, thus defined by several linear equations.

Consider first M points on E, $P_1 = (x_1, y_1), P_2 = (x_2, y_2), \dots, P_M = (x_M, y_M)$, and let $P_{M+1} = (x_{M+1}, y_{M+1}) = P_1 + P_2 + \cdots + P_M$ be their sum. Then x_{M+1} and y_{M+1} are certain explicit rational functions of the coordinates x_i, y_i for $i = 1, \dots, M$.

We proved in [CVV17, Section 6.3.1] that if the points (x_i, y_i) for $i = 1, \dots, M$ have coordinates given by some rational functions in certain variables, and whose sums of the partial degrees are bounded by d_i, then the sum d of the partial degrees of the functions x_{M+1}, y_{M+1} in the variables x_i, y_i is bounded as

$$d \le 12^{M-1}d_1 + \sum_{i=2}^{M} 12^{M-i+1}d_i \le 12^{M-1}\sum_{i=1}^{M} d_i. \tag{3.3}$$

Let us consider the morphism $L\colon E^N \to E$ defined as

$$L(\mathbf{X}) = l_1X_1 + \cdots + l_NX_N,$$

where $l_i \in \mathrm{End}(E)$ 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 $(x(L(\mathbf{X})), y(L(\mathbf{X})))$ that are rational functions in the coordinates (x_i, y_i) of all X_i's. We want to bound the sum of the partial degrees of the rational function $x(L(\mathbf{X}))$.

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

Now combining inequality (3.3) with the bounds from Subsection 3.2 we obtain

$$d(L) \le 12^{N-1}2\Big(\sum_{i=1}^{N} |l_i|^2\Big). \tag{3.4}$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

4 Estimates for Degree and Height of a Translate

In this section we give explicit bounds for the degree of a translate $H + P$ in E^N in terms of the coefficients of the linear forms defining H, and we bound its height in terms of the height of P.

For a vector in $\mathbb{C}^N$, we denote by $\|\cdot\|$ the standard hermitian norm.

4.1 A Bound for the Degree

To bound the degree of a translate, we do the same construction as in [CVV17], recalled here for clarity, and we use the explicit bounds computed above for the CM case. 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 Bézout's theorem inductively for the case of several equations.

Let U be a matrix of rank s in $\mathrm{Mat}_{s\times N}(\mathrm{End}(E))$ with rows $\mathbf{u}_1,\dots,\mathbf{u}_s \in \mathrm{End}(E)^N$ and let $H \subset E^N$ be an irreducible component of the algebraic subgroup associated with the matrix U (see Subsection 2.8).

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

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

Now let $P = (P_1,\dots,P_N) \in E^N$ be a point. Take the k-th row $\mathbf{u}_k \in \mathrm{End}(E)^N$ of U and consider the equation

$$x\big(\mathbf{u}_k(\mathbf{X})\big) = x\big(\mathbf{u}_k(P)\big)$$

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

Clearing out the denominators, the previous equation can be written as

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

where $f_{\mathbf{u}_k,P}$ is a polynomial of degree bounded by $d(\mathbf{u}_k)$ (see formula (3.3)), which 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 Section 2 we defined $X(E, N)$ to be the image of E^N in $\mathbb{P}_{3^N-1}$. Denote by $Y_k' \subset \mathbb{P}_{3^N-1}$ the zero-set of the polynomial $f_{\mathbf{u}_k,P}(x_1, y_1,\dots,x_N, y_N)$ 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

$$\mathbf{u}_k(\mathbf{X}) = \mathbf{u}_k(P)$$

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

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

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

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

By Bézout's theorem,

$$\deg Y_k \leq \deg X(E,N) \deg Y_k' \leq 3^N N! 12^{N-1} 2 \|\mathbf{u}_k\|^2,$$

where the last inequality follows from formula (3.4).

In a similar way, considering all the rows we get

$$\deg(H+P) \leq \deg X(E,N) \deg Y_1' \cdots \deg Y_s' \leq 3^N N! (12^{N-1}2)^s \prod_{i=1}^{s} \|\mathbf{u}_i\|^2. \tag{4.1}$$

4.2 A Bound for the Height

The aim of this section is to prove the following proposition.

Proposition 4.1 *Let E be an elliptic curve with CM by τ. Let $K = \mathbb{Q}(\tau)$, D_K its discriminant and $f = [\mathcal{O}_K : \mathrm{End}(E)]$. Let $P \in E$ be a point. Let $H \subset E^N$ be a component of the algebraic subgroup of codimension s associated with an $s \times N$ matrix with rows $\mathbf{u}_1, \ldots, \mathbf{u}_s \in \mathrm{End}(E)^N$ such that $\|\mathbf{u}_i\|$ are the successive minima of the K-lattice $\Lambda = \langle \mathbf{u}_1, \ldots, \mathbf{u}_s \rangle_{\mathrm{End}(E)}$. Then*

$$h_2(H+P) \leq C_1(N,s) \prod_{i=1}^{s} \|\mathbf{u}_i\|^2 \Big(\frac{2^N f^N |D_K|^{\frac{N}{2}}}{\omega_{2(N-s)}\omega_{2s}} \sum_{i=1}^{s} \frac{\widehat{h}(\mathbf{u}_i(P))}{\|\mathbf{u}_i\|^2} + C(E) \Big),$$

where

$$C_1(N,s) = N(N-s+1)6^N N! 12^{s(N-1)},$$

$\omega_{2n} = \pi^n/n!$ and $C(E)$ is defined in Proposition 2.1.

Proof Let $\Lambda^\perp$ be the orthogonal K-lattice of Λ and let $\mathbf{u}_{s+1}, \ldots, \mathbf{u}_N$ K-linearly independent vectors that give the successive minima of $\Lambda^\perp$.

The $(N-s) \times N$ matrix with rows $\mathbf{u}_{s+1}, \ldots, \mathbf{u}_N$ 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 $\mathbf{u}_1, \ldots, \mathbf{u}_N$, and let ∇ be its determinant. Notice that $|\nabla| = \det \Lambda \cdot \det \Lambda^\perp$, because Λ and $\Lambda^\perp$ are orthogonal. We remark that $\mathbf{u}_i(P_0) = 0$ for all $i = 1, \ldots, s$, because $P_0 \in H$, and $\mathbf{u}_i(P^\perp) = 0$ for all $i = s+1, \ldots, N$, because $P^\perp \in H^\perp$.

Therefore,

$$UP^\perp = \begin{pmatrix} \mathbf{u}_1(P^\perp) \\ \vdots \\ \mathbf{u}_s(P^\perp) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1(P_0+P^\perp) \\ \vdots \\ \mathbf{u}_s(P_0+P^\perp) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1(P) \\ \vdots \\ \mathbf{u}_s(P) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

Recall that there exists a matrix U^*, called the adjugate matrix of U, with coefficients in $\mathrm{End}(E)$, such that $UU^* = U^*U = (\det U)\,\mathrm{Id}$. So

$$\nabla P^\perp = U^* U P^\perp = U^* \begin{pmatrix} \mathbf{u}_1(P) \\ \vdots \\ \mathbf{u}_s(P) \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{4.2}$$

Moreover, by Hadamard's inequality, the i-th column of U^* has all entries with absolute value bounded by

$$\frac{\|\mathbf{u}_1\| \cdots \|\mathbf{u}_N\|}{\|\mathbf{u}_i\|}. \tag{4.3}$$

Recall that for $\alpha \in \mathrm{End}(E)$ and $Q \in E$, $\widehat{h}(\alpha Q) = |\alpha|^2 \widehat{h}(Q)$, because $\deg \alpha = |\alpha|^2$. Therefore, computing canonical heights in (4.2) and using (4.3) we have

$$\widehat{h}(P^\perp) \le \frac{N\|\mathbf{u}_1\|^2 \cdots \|\mathbf{u}_N\|^2}{|\nabla|^2} \sum_{i=1}^{s} \frac{\widehat{h}(\mathbf{u}_i(P))}{\|\mathbf{u}_i\|^2}.$$

Recall inequality (2.4), which gives

$$\mu_2(H+P) \le \widehat{\mu}(H+P) + NC(E),$$

where $C(E)$ was defined in Proposition 2.1. By [Phi12], we have $\widehat{\mu}(H+P) = \widehat{h}(P^\perp)$, and therefore, applying Zhang's inequality and (2.4) we obtain

$$\begin{aligned} h_2(H+P) &\le (N-s+1)(\deg H)\big(\widehat{h}(P^\perp) + NC(E)\big) \\ &\le N(N-s+1)(\deg H)\Big(\frac{\|\mathbf{u}_1\|^2 \cdots \|\mathbf{u}_N\|^2}{|\nabla|^2} \sum_{i=1}^{s} \frac{\widehat{h}(\mathbf{u}_i(P))}{\|\mathbf{u}_i\|^2} + C(E)\Big). \end{aligned} \tag{4.4}$$

By (4.1), we know that

$$\deg H \le 3^N N!(12^{N-1}2)^s \prod_{i=1}^{s} \|\mathbf{u}_i\|^2.$$

Using Minkowski's Theorem 2.4, we deduce

$$\begin{aligned} \frac{\deg H}{(\det \Lambda)^2} &\le 3^N N!(12^{N-1}2)^s \frac{2^s f^s |D_K|^{\frac{s}{2}}}{\omega_{2s}}, \\ \frac{\prod_{i=s+1}^{N} \|\mathbf{u}_i\|^2}{(\det \Lambda^\perp)^2} &\le \frac{2^{N-s} f^{N-s} |D_K|^{\frac{N-s}{2}}}{\omega_{2(N-s)}}. \end{aligned}$$

Plugging these inequalities in (4.4) and using $|\nabla| = \det \Lambda \det \Lambda^\perp$, we obtain the desired bound of the statement. ∎

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

5 The Auxiliary Translate

In this section we will ensure the existence of auxiliary translates by the point P that approximate the torsion variety passing through P, and we will explicitly estimate their height and degree in terms of $\widehat{h}(P)$ and some parameters. A good choice of the parameters in the proof of the main theorem will allow us to deduce the desired bound on $\widehat{h}(P)$. The reader shall be warned that the winning term in the height bound is the exponent $1 - N/ms$ of the parameter T, which becomes negative as soon as $ms < N$ and will play in our favour for T large.

In [CVV17, Proposition 3.1] we did it for the non-CM case. In the following proposition we generalize the result also to the CM case.

Proposition 5.1 *Let E be an elliptic curve with CM by τ and let $K = \mathbb{Q}(\tau)$ with discriminant D_K. Let $P = (P_1, \dots, P_N) \in B \subset E^N$, where B is a torsion variety of dimension m. Let $T \geq 1$ be a real number.*

Then there exists an abelian subvariety $H \subset E^N$ of codimension s such that

$$\begin{aligned} \deg(H + P) &\leq C_3(N, s)|\tau|^{2s} T, \\ h_2(H + P) &\leq C_4(N, s, m) f^{N+r} |D_K|^{\frac{N+r}{2}} |\tau|^{2s+2} T^{1-\frac{N}{ms}} \widehat{h}(P) \\ &\quad + C_5(N, s, E)|\tau|^{2s} T, \end{aligned}$$

where

$$\begin{aligned} C_3(N, s) &= 3^N N! (12^{N-1} 2)^s, \\ C_4(N, s, m) &= \frac{C_1(N, s) C_2(m) s 2^{N+2} (2(2N)^{2N})^{\frac{2}{m}}}{\omega_{2(N-s)} \omega_{2s}}, \\ C_5(N, s, E) &= C_1(N, s) C(E), \end{aligned}$$

where $C_1(N, s) = N(N - s + 1)6^N N! 12^{s(N-1)}$, $C_2(m) = ((2m)!N)^2 m^3$, $\omega_{2n} = \pi^n / n!$, and $C(E)$ is given in Proposition 2.1.

To extend to an imaginary quadratic field K what was done in [CVV17] for rational numbers, we use the second Minkowski theorem in the form presented in Section 2.7. The estimates in the CM case are more complicated, and they are carried out in the next few paragraphs.

5.1 Geometry of Numbers

For $Q, R \in E$, consider the pairing defined by Philippon in [Phi12]:

$$\langle Q, R \rangle = \langle Q, R \rangle_{NT} - \frac{1}{\sqrt{D}} \langle Q, \sqrt{D} R \rangle_{NT},$$

where $\langle \cdot, \cdot \rangle_{NT}$ is the Néron–Tate pairing and D is a squarefree negative integer such that $K = \mathbb{Q}(\sqrt{D})$.

This pairing is sesquilinear. Moreover, it gives the Néron–Tate height, since $\langle Q, Q \rangle = 2\widehat{h}(Q)$ and the induced norm $\| \cdot \|$ is hermitian. The following is a version for

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

$\mathrm{End}(E)$-Modules of a lemma of Bombieri reported, for instance, in [Via03, Lemma 3]. There the coefficients α_i must be integers while here are in $\mathrm{End}(E)$.

Lemma 5.2 *Let Λ be a finitely generated subgroup of E of rank r over $\mathrm{End}(E)$. Then there are elements $g_1,\dots,g_r \in \Lambda$ that generate a K-sublattice Γ of $\Lambda/\mathrm{Tor}(\Lambda)$ of index $c_0 \le (2f|D_K|^{\frac{1}{2}})^{\frac{r}{2}}/\omega_{2r}^{1/2}$ and such that for all $\alpha_i \in \mathrm{End}(E)$, we have*

$$\widehat{h}\Big(\sum \alpha_i g_i\Big) \ge c(r) f^{-r} |D_K|^{\frac{-r}{2}} \Big(\sum |\alpha_i|^2 \widehat{h}(g_i)\Big),$$

where $c(r) = (r(2r)!)^{-2}$.

Proof The above pairing shows that the height function extends on $\Lambda_{\mathbb{C}} := \Lambda \otimes_{\mathrm{End}(E)} \mathbb{C}$ to the square of a norm. Then $\Lambda/\mathrm{Tor}(\Lambda)$ is a K-lattice.

Let $B := \{x \in \mathbb{C}^r : \|x\| \le 1\}$ be the closed complex ball of radius 1. Let $\lambda_1,\dots,\lambda_r$ be the successive minima of B with respect to the lattice $\Lambda/\mathrm{Tor}(\Lambda)$. Let $\Gamma = \langle g_1,\dots,g_r\rangle_{\mathrm{End}(E)}$ with $\|g_i\| = \lambda_i$ and $g_i \in \Lambda/\mathrm{Tor}(\Lambda)$. Then by the Minkowski theorem for the K-lattice $\Lambda/\mathrm{Tor}(\Lambda)$, we obtain $c_0 = \mathrm{vol}(\Gamma)/\mathrm{vol}(\Lambda/\mathrm{Tor}(\Lambda)) \le (2f|D_K|^{\frac{1}{2}})^{\frac{r}{2}}/\omega_{2r}^{1/2}$. To obtain the estimate on the height we apply the Minkowski theorem to the K-lattice Γ. Let $V := \mathrm{vol}(\Gamma)$ be the volume of a fundamental domain of Γ. By the second Minkowski theorem, we have

$$\lambda_1 \cdots \lambda_r \,\mathrm{vol}(B) \le 2^{2r} f^{\frac{r}{2}} |D_K|^{\frac{r}{4}} V.$$

We write

$$w_i = \frac{g_i}{\|g_i\|}, \tag{5.1}$$

and we define B^* to be

$$B^* = \{y \in \mathbb{R}^r : \|y_1 w_1 + y_2 w_2 + \cdots + y_r w_r\| \le 1\}.$$

Since B is the image of B^* under a linear map that sends the g_i to w_i, we have (by the above relations)

$$\mathrm{vol}(B^*) = \frac{\mathrm{vol}(B)}{V} \prod_{i=1}^{r} \|g_i\| \le 2^{2r} f^{\frac{r}{2}} |D_K|^{\frac{r}{4}}. \tag{5.2}$$

A lower bound is obtained as follows.

Let e_j, $j = 1,\dots,r$ be the standard basis in $\mathbb{C}^r$ with respect to our scalar product. Let us identify $\mathbb{C}^r$ with $\mathbb{R}^{2r}$ and let e_j, $\mathbf{i}e_j$ be the real basis in $\mathbb{R}^{2r}$ ($\mathbf{i}$ is the imaginary unit such that $\mathbf{i}^2 = -1$). Let y be the boundary point of B^* on a real coordinate axis. Then for each i the set B^* contains the convex closure of the points $\pm y$ and $\pm\mathbf{i}e_i$, $\pm e_j, \pm\mathbf{i}e_j$ for $j = 1,\dots,i-1,i+1,\dots,r$. This set is the union of 2^{2r} simplices of volume $|y_i|/(2r)!$. Therefore, we get the lower bound

$$|y_i| \frac{2^{2r}}{(2r)!} \le \mathrm{vol}(B^*),$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

which, combined with (5.2), gives

$$\sum_{i=1}^{r}|y_i| \le r(2r)!f^{\frac{r}{2}}|D_K|^{\frac{r}{4}}\Big\|\sum_{i=1}^{r}y_iw_i\Big\|, \tag{5.3}$$

where the norm on the right is 1, because y is a boundary point of B^*. Now, from (5.1), we can rewrite (5.3) as

$$\Big\|\sum_{i=1}^{r}x_ig_i\Big\| \ge (r(2r)!)^{-1}f^{-\frac{r}{2}}|D_K|^{-\frac{r}{4}}\sum_{i=1}^{r}|x_i|\cdot\|g_i\|, \tag{5.4}$$

where $x_i = y_i/\|g_i\|$.

Now choose $p_1', \dots, p_r'$ to be representatives of $p_1, \dots, p_r$ in Λ and define

$$g_i = \sum_{j=1}^{r}v_{ij}p_j' \quad i = 1, \dots, r.$$

The g_i generate a submodule of finite index, and we see that

$$2\widehat{h}\Big(\sum_{i=1}^{r}\alpha_ig_i\Big) = \Big\|\sum_{i=1}^{r}\alpha_iv_i\Big\|^2 \quad \text{and} \quad 2\widehat{h}(g_i) = \|v_i\|^2,$$

and therefore from (5.4) with $x_i = \alpha_i$ it follows that

$$\Big\|\sum_{i=1}^{r}\alpha_ig_i\Big\|^2 \ge (r(2r)!)^{-2}f^{-r}|D_K|^{-\frac{r}{2}}\Big(\sum_{i=1}^{r}|\alpha_i|\cdot\|g_i\|\Big)^2.$$

Since in the last bracket we only have positive numbers, the square of the sum is at least the sum of the squares. Thus,

$$\widehat{h}\Big(\sum_{i=1}^{r}\alpha_ig_i\Big) \ge (r(2r)!)^{-2}f^{-r}|D_K|^{-\frac{r}{2}}\sum_{i=1}^{r}|\alpha_i^2|\cdot\widehat{h}(g_i). \qquad \blacksquare$$

If u is a vector, we denote by $\|u\|$ its euclidean norm, and for a linear form L we denote by $\|L\|$ the norm of the vector of the coefficients of L.

We have the following lemma.

Lemma 5.3 *Let E be an elliptic curve with CM by τ and let $K = \mathbb{Q}(\tau)$ and $f = [\mathcal{O}_K:\mathcal{O}]$. Let $P = (P_1, \dots, P_N) \in B \subset E^N$, where B is a torsion variety of dimension m. Then there exist linear forms $\mathbf{L}_1, \dots, \mathbf{L}_m \in \mathbb{C}[X_1, \dots, X_N]$ such that $\|\mathbf{L}_j\| \le 1/|\tau|$ and*

$$\widehat{h}(t_1P_1 + \cdots + t_NP_N) \le C_2(m)f^m|D_K|^{\frac{m}{2}}|\tau|^2\max_{1\le j\le m}\{|\mathbf{L}_j(\mathbf{t})|^2\}\widehat{h}(P)$$

for all $\mathbf{t} = (t_1, \dots, t_N) \in \mathrm{End}(E)^N$, where $C_2(m) = N^2m^3(2m)!^2$.

Proof Let $\Lambda = \langle P_1, \dots, P_N\rangle_{\mathrm{End}(E)}$. By Lemma 5.2 there exists a K-lattice Γ contained in Λ with generators $g_1, \dots, g_m \in E$ and $c_0\Lambda \subset \Gamma$ such that for every $\alpha_i \in \mathrm{End}(E)$,

$$\widehat{h}(\alpha_1g_1 + \cdots + \alpha_mg_m) \ge (m(2m)!)^{-2}f^{-m}|D_K|^{\frac{-m}{2}}\Big(\sum_{i=1}^{m}|\alpha_i|^2\widehat{h}(g_i)\Big). \tag{5.5}$$

By the choice of the g_i, for every $1 \le i \le N$, we can write

$$c_0P_i = \zeta_i + \gamma_{i1}g_1 + \cdots + \gamma_{im}g_m$$

for some $\gamma_{ij} \in \mathrm{End}(E)$ and torsion points $\zeta_i \in E$.

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

Let $A = \max_{i,j}\{|\tau|^2|\gamma_{ij}|^2\widehat{h}(g_j)\}$. We can suppose $A > 0$; otherwise, P would be a torsion point and the lemma would be trivial. Now define

$$\widetilde{L}_j = \gamma_{1j}X_1 + \cdots + \gamma_{Nj}X_N, \qquad j = 1, \dots, m$$
$$L_j = \Big(\frac{\widehat{h}(g_j)}{NA}\Big)^{\frac{1}{2}}\widetilde{L}_j, \qquad j = 1, \dots, m.$$

By the definition of A we obtain $\|L_j\| \le 1/|\tau|$. Moreover, for every $\mathbf{t} = (t_1, \dots, t_N) \in \mathrm{End}(E)^N$, we have

$$c_0(t_1P_1 + \cdots + t_NP_N) = \xi + \sum_{i=1}^{m}\widetilde{L}_j(\mathbf{t})\mathbf{g}_j,$$

where ξ is a torsion point. Computing heights we get

$$c_0^2\widehat{h}(t_1P_1 + \cdots + t_NP_N) = \widehat{h}\Big(\sum_{j=1}^{m}\widetilde{L}_j(\mathbf{t})g_j\Big) \le N\sum_{j=1}^{m}|\widetilde{L}_j(\mathbf{t})|^2\widehat{h}(g_j)$$
$$= N^2A\sum_{j=1}^{m}|L_j(\mathbf{t})|^2 \le mN^2A\max_{1\le j\le m}\{|L_j(\mathbf{t})|^2\}. \tag{5.6}$$

If i_0, j_0 are the indices for which the maximum is attained in the definition of A, then by (5.5) we get

$$\big(m(2m)!\big)^{-2}f^{-m}|D_K|^{\frac{-m}{2}}A = (m(2m)!)^{-2}f^{-m}|D_K|^{\frac{-m}{2}}|\tau|^2|\gamma_{i_0j_0}|^2\widehat{h}(\mathbf{g}_{j_0})$$
$$\le |\tau|^2\widehat{h}(c_0P_{i_0}) \le |\tau|^2c_0^2\widehat{h}(P).$$

Combining this with inequality (5.6), we conclude the proof. ∎

The following lemma is proved by a simple computation with complex numbers, and it is useful for decomposing linear forms over $\mathbb{C}$ into linear forms over $\mathbb{R}$.

Lemma 5.4 *Let E be an elliptic curve with CM by τ. Let $K = \mathbb{Q}(\tau)$ and let D_K be its discriminant. Let $\mathbf{L} \in \mathbb{C}[X_1, \dots, X_N]$ be a linear form and let $\mathbf{t} \in \mathrm{End}(E)^N$; then*

$$\mathbf{L}(\mathbf{t}) = L_1(t_1) + L_2x_0(t_2) + (L_2(t_1) + L_1(t_2) + L_2y_0(t_2))\tau,$$

where $\mathbf{L} = L_1 + L_2\tau$ with $L_i \in \mathbb{R}[X_1, \dots, X_N]$, $\mathbf{t} = t_1 + t_2\tau$ with $t_i \in \mathbb{Z}^N$, and $\tau^2 = x_0 + y_0\tau$.
Moreover,

$$\|(L_1, L_2x_0)\| \le |\tau|\,\|L\| \quad \text{and} \quad \|(L_2, L_1 + L_2y_0)\| \le |\tau|\,\|L\|,$$

where the norm of a form is the norm of the vector of its coefficients.

Proof The first part is a simple computation implied from the linearity and from the rule of multiplication of complex numbers; namely, for $a_i, b_i \in \mathbb{R}$ we have

$$(a_1 + a_2\tau)(b_1 + b_2\tau) = a_1b_1 + a_2x_0b_2 + (a_1b_2 + a_2b_1 + a_2y_0b_2)\tau.$$

The second part is given by a simple computation. ∎

We can now prove a lemma of geometry of numbers that relies on [Hab08, Lemma 2] and on a decomposition of forms over $\mathbb{C}$ in forms over $\mathbb{R}$.

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

Lemma 5.5 *Let E be an elliptic curve with CM by τ and $K = \mathbb{Q}(\tau)$. Let $1 \le m \le N$ and let $\mathbf{L}_1, \dots, \mathbf{L}_m \in \mathbb{C}[X_1, \dots, X_N]$ be linear forms with $\|\mathbf{L}_j\| \le 1/|\tau|$ for all j. Then for any real number $T \ge 1$ and any integer s with $1 \le s \le N$, there exist linearly independent vectors $\mathbf{u}_1, \dots, \mathbf{u}_s \in \mathrm{End}(E)^N$ such that*

$$\|\mathbf{u}_1\| \cdots \|\mathbf{u}_s\| \le |\tau|^s T,$$

and for $1 \le j \le m$ and $1 \le k \le s$,

$$\|\mathbf{u}_1\| \cdots \|\mathbf{u}_s\| \frac{|\mathbf{L}_j(\mathbf{u}_k)|}{\|\mathbf{u}_k\|} \le 2(2(2N)^{2N})^{\frac{1}{m}} |\tau|^s T^{1-\frac{N}{ms}}.$$

Proof If $T \le (2(2N)^{2N})^{\frac{s}{N}}$, then $(2(2N)^{2N})^{\frac{1}{m}} T^{1-\frac{N}{ms}} \ge 1$. It is then sufficient to take u_i to be s elements of the standard basis of $\mathbb{Z}^N$.

We can then assume that $T > (2(2N)^{2N})^{\frac{s}{N}}$.

We will define new forms in $\mathbb{R}[X_1, \dots, X_N, \tau X_1, \dots, \tau X_N]$ that will allow us to use Habegger [Hab08, Lemma 2] and to produce the desired estimates. Let $\mathbf{L}_i = L_{1i} + L_{2i}$ with L_{1i} in $\mathbb{R}[X_1, \dots, X_N]$ and L_{2i} in $\mathbb{R}[\tau X_1, \dots, \tau X_N]$. In view of Lemma 5.4, we define

$$L_i = (L_{1i}, L_{2i} x_0) \in \mathbb{R}[X_1, \dots, X_N, \tau X_1, \dots, \tau X_N],$$
$$L'_i = (L_{2i}, L_{2i} y_0 + L_{1i}) \in \mathbb{R}[X_1, \dots, X_N, \tau X_1, \dots, \tau X_N],$$

where $\tau^2 = x_0 + y_0 \tau$. Then by Lemma 5.4, we get $\|L_i\| \le |\tau| \|\mathbf{L}_i\| \le 1$ and $\|L'_i\| \le |\tau| \|\mathbf{L}_i\| \le 1$.

We can then apply [Hab08, Lemma 2] to the $2m$ forms $L_1, \dots, L_m$ and $L'_1, \dots, L'_m$ in $\mathbb{R}[X_1, \dots, X_N, \tau X_1, \dots, \tau X_N]$ with $n = 2N$ and his m twice the m appearing here. So for any real number $\rho \ge 1$ there exist linearly independent vectors $U_1, \dots, U_{2N} \in \mathbb{Z}^{2N}$ and positive reals $\lambda_1 \le \cdots \le \lambda_{2N}$ such that

$$\|U_i\| \le \lambda_i \quad \text{and} \quad \lambda_1 \cdots \lambda_{2N} \le 2(2N)^{2N} \rho^{2m}, \tag{5.7}$$

and for every $i \le m$ and $k \le 2N$,

$$\|L_i(U_k)\| \le \rho^{-1} \lambda_k \quad \text{and} \quad \|L'_i(U_k)\| \le \rho^{-1} \lambda_k. \tag{5.8}$$

For every $1 \le s \le N$, consider the writing of the vectors $U_1, \dots, U_{2s}$ as $U_1 = (A_{11}, A_{21}), \dots, U_{2s} = (A_{1,2s}, A_{2,2s})$ with $A_{ij} \in \mathbb{Z}^N$, and set $\mathbf{U}_i = A_{1i} + A_{2i}\tau$. Extract s vectors $\mathbf{u_i} = a_{1i} + \tau a_{2i}$ from the $\mathbf{U}_1, \dots, \mathbf{U}_{2s}$ such that the vectors $\mathbf{u}_1, \dots, \mathbf{u}_s$ are K-linearly independent and of minimal norm. We set $u_i = (a_{1i}, a_{2i})$. Remark that the vector space generated from the first $2i-1$ vectors u_j has dimension $2i-1$ over $\mathbb{Q}$ and therefore dimension at least i over K. Then $\|u_i\|^2 \le \|U_{2i-1}\| \|U_{2i}\|$. Moreover, from (5.7), we deduce

$$\|u_1\|^2 \cdots \|u_s\|^2 \le \|U_1\| \cdots \|U_{2s}\| \le \lambda_1 \cdots \lambda_{2s} \le (\lambda_1 \cdots \lambda_{2N})^{\frac{s}{N}} \le \left(2(2N)^{2N}\right)^{\frac{2s}{N}} \rho^{\frac{2ms}{N}}.$$

Choose ρ so that $T^2 := (2(2N)^{2N})^{\frac{2s}{N}} \rho^{\frac{2ms}{N}}$. Since $T > (2(2N)^{2N})^{\frac{s}{N}}$, $\rho \ge 1$.

Note that $\|\mathbf{u}_i\|^2 = \|a_{1,i}\|^2 + |\tau|^2 \|a_{2,i}\|^2 \le |\tau|^2 \|u_i\|^2$, because $|\tau| \ge 1$. Thus,

$$\|\mathbf{u}_1\| \cdots \|\mathbf{u}_s\| \le |\tau|^s \|u_1\| \cdots \|u_s\| \le |\tau|^s T,$$

which proves the first bound in the statement.

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

By (5.8) and from the fact that u_k is one vector among the U_j with $j \leq 2k-1$, we get that

$$\|L_i(u_k)\|^2 = \|L_i(U_j)\|^2 \leq \rho^{-2}\lambda_j^2 \leq \rho^{-2}\lambda_{2k-1}\lambda_{2k},$$

and similarly

$$\|L_i'(u_k)\|^2 \leq \rho^{-2}\lambda_{2k-1}\lambda_{2k}.$$

This, together with (5.7), gives that for all $i \leq m$, we have

$$\|u_1\|^2 \cdots \|u_s\|^2 \frac{|L_i(u_k)|^2}{\|u_k\|^2} \leq \rho^{-2}\lambda_1 \cdots \lambda_{2s} \leq \rho^{-2}T^2 = \left(2(2N)^{2N}\right)^{\frac{2}{m}} T^{2(1-\frac{N}{ms})},$$

$$\|u_1\|^2 \cdots \|u_s\|^2 \frac{|L_i'(u_k)|^2}{\|u_k\|^2} \leq \rho^{-2}\lambda_1 \cdots \lambda_{2s} \leq \rho^{-2}T^2 = \left(2(2N)^{2N}\right)^{\frac{2}{m}} T^{2(1-\frac{N}{ms})}.$$

By Lemma 5.4, we deduce that the K-linearly independent vectors

$$\mathbf{u_i} = a_{1i} + \tau a_{2i} \in \mathrm{End}(E)^N \quad \text{with} \quad u_i = (a_{1i}, a_{2i})$$

satisfy

$$\begin{aligned}\|\mathbf{u}_1\| \cdots \|\mathbf{u}_s\| \frac{|\mathbf{L}_i(\mathbf{u}_k)|}{\|\mathbf{u}_k\|} &\leq |\tau|^{s-1}\|u_1\| \cdots \|u_s\| \left(\frac{|L_i(u_k)| + |\tau||L'_i(u_k)|}{\|u_k\|} \right) \\ &\leq 2|\tau|^s (2(2N)^2 N)^{\frac{1}{m}} T^{1-\frac{N}{ms}}.\end{aligned}$$

This concludes the proof. ∎

We are now ready to prove Proposition 5.1.

Proof of Proposition 5.1 If E is non-CM, then this is proved in [CVV17, Proposition 3.1]. Note that there we used another normalization for the height functions (namely, the $\widehat{h}$ used in this paper is 3 times the one used in [CVV17]), however the bounds in that proposition are sharper than those presented here, which hold in both cases.

Assume now that E has CM. Let $\mathbf{L}_1, \ldots, \mathbf{L}_m \in K[X_1, \ldots, X_N]$ be the linear forms constructed in Lemma 5.3. Then

$$\widehat{h}(\mathbf{u}(P)) \leq C_2(m) f^r |D_K|^{\frac{r}{2}} |\tau|^2 \max_{1 \leq j \leq m} \{\|\mathbf{L}_j(\mathbf{u}_k)\|^2\} \widehat{h}(P) \tag{5.9}$$

for all $\mathbf{u} \in \mathrm{End}(E)^N$.

By Lemma 5.5 applied with $\sqrt{T}$, there exist s vectors $\mathbf{u}_1, \ldots, \mathbf{u}_s \in \mathrm{End}(E)^N$ such that

$$\|\mathbf{u}_1\|^2 \cdots \|\mathbf{u}_s\|^2 \leq |\tau|^{2s} T,$$

$$\|\mathbf{u}_1\|^2 \cdots \|\mathbf{u}_s\|^2 \frac{\|\mathbf{L}_j(\mathbf{u}_k)\|^2}{\|\mathbf{u}_k\|^2} \leq 4|\tau|^{2s} \left(2(2N)^{2N}\right)^{\frac{2}{m}} T^{1-\frac{N}{ms}},$$

and from (5.9), we have

$$\widehat{h}(\mathbf{u}_k(P)) \leq C_2(m) f^r |D_K|^{\frac{r}{2}} |\tau|^2 \max_{1 \leq j \leq m} \left\{ \|\mathbf{L}_j(\mathbf{u}_k)\|^2 \right\} \widehat{h}(P).$$

Consider the algebraic subgroup H of codimension s defined by $\mathbf{u}_1, \ldots, \mathbf{u}_s$. By (4.1), its degree is bounded as

$$\deg(H + P) \leq \left(3^N N! (12^{N-1}2)^s\right) |\tau|^{2s} T.$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

Substituting the above estimates in Proposition 4.1, we obtain that

$$h_2(H+P) \le \frac{C_1(N,s)C_2(m)s2^{N+2}(2(2N)^{2N})^{\frac{2}{m}}}{\omega_{2(N-s)}\omega_{2s}} f^{N+r}|D_K|^{\frac{N+r}{2}}|\tau|^{2s+2}T^{1-\frac{N}{ms}}\widehat{h}(P) + C_1(N,s)C(E)|\tau|^{2s}T. \qquad \blacksquare$$

6 The Proof of the Main Theorem

In this section we prove our main theorem. We divide the theorem into two parts. The first is the case of transverse curves; the second is the general case. At the end of the section we also prove Corollaries 1.5 and 1.6.

6.1 Transverse Curves

Theorem 6.1 *Let $\mathcal{C}$ be a curve transverse in E^N, let $K = \mathrm{frac}(\mathrm{End}(E))$ with discriminant D_K, and let $f = [\mathcal{O}_K : \mathrm{End}(E)]$. Then the set of points of $\mathcal{C}$ of rank $r \le N-1$ has Néron–Tate height bounded as*

$$\widehat{h}(P) \le \delta h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{N-r}} + \delta\big(N^2C(E)+C_0\big)(\deg\mathcal{C})^{\frac{N}{N-r}} + N^2C(E),$$

where

$$\delta = \delta(N,r,f,D_K) = c_1(N)c_2(N,r)Nf^{2+\frac{(N-r+4)r}{N-r}}|D_K|^{1+\frac{(N+r+4)r}{2(N-r)}},$$
$$c_1(N) = N(N!)6^{2N-1},$$
$$c_2(N,r) = \big(N!N^5 3^{2N-1}2^{4N-2}2^{\frac{4N+2}{r}}N^{\frac{4N}{r}}r^3(r!)^2((2r)!)^2(\omega_{2(N-1)}\omega_2)^{-1}\big)^{\frac{r}{N-r}},$$

$\omega_{2n} = \pi^n/n!$; $C(E)$ is the explicit constant defined in Proposition 2.1*, and depends only on the coefficients of E.*

Proof By assumption, the point P has rank $r \le N-1$; then $P \in B$ where B is a torsion variety with $\dim B = r$.

We apply Proposition 5.1 to P, with $m = r$, $s = 1$ and T as a free parameter that will be specified later. This gives a translate $H+P$ of dimension $N-1$, of degree explicitly bounded in terms of T and such that $h_2(H+P)$ is explicitly bounded in terms of $\deg H$ and $\widehat{h}(P)$ and T. Recall that $|\tau|^2 \le f^2|D_K|$. More precisely, for

$$\alpha = (N!)6^{2N-1}f^2|D_K|,$$
$$\beta = N!N^4 3^{2N-1}2^{4N-2}2^{\frac{4N+2}{r}}N^{\frac{4N}{r}}r^3((2r)!)^2(\omega_{2(N-1)}\omega_2)^{-1}f^{N+r+4}|D_K|^{\frac{N+r}{2}+2},$$
$$\gamma = N^2\alpha C(E),$$

the degree and the height of the translate $H+P$ are bounded by Proposition 5.1 with $m = r$ and $s = 1$, as

$$\deg(H+P) \le \alpha T, \tag{6.1}$$
$$h_2(H+P) \le \beta T^{1-\frac{N}{r}}\widehat{h}(P) + \gamma T. \tag{6.2}$$

We remark that P is a component of $\mathcal{C} \cap (H+P)$. Otherwise, $\mathcal{C} \subset H+P$, contradicting the transversality of $\mathcal{C}$. So, we apply the Arithmetic Bézout Theorem to

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

$\mathcal{C} \cap (H + P)$ to bound the height of P. We have

$$h_2(P) \le h_2(\mathcal{C}) \deg H + \deg \mathcal{C} h_2(H + P) + C_0 \deg \mathcal{C} \deg H,$$

where

$$C_0 = \Big(\frac{H_N + \log 2(2(3^N - 1) - N)}{2} \Big) \tag{6.3}$$

is given in (2.3) and H_N denotes the N-th harmonic number. Substituting the estimates from (6.1) and (6.2) above, we obtain

$$h_2(P) \le h_2(\mathcal{C})\alpha T + \deg \mathcal{C}\Big(\frac{\beta}{T^{(N-r)/r}} \widehat{h}(P) + \gamma T \Big) + C_0 \alpha T \deg \mathcal{C}. \tag{6.4}$$

We now choose

$$T = \Big(\frac{N}{N-1} \beta \deg C \Big)^{\frac{r}{N-r}},$$

so that the coefficient of $\widehat{h}(P)$ at the right-hand side of (6.4) becomes $(N-1)/N < 1$.

Recall that by Proposition 2.1 we have

$$\widehat{h}(P) \le h_2(P) + NC(E),$$

where

$$C(E) = \frac{h_W(\Delta) + 3h(j)}{4} + \frac{h_W(A) + h_W(B)}{2} + 4$$

where A and B are the coefficients of the Weierstrass equation for E, and Δ and j are the discriminant and the j-invariant of E. Then we get

$$\widehat{h}(P) \le \frac{(N-1)}{N} \widehat{h}(P) + h_2(\mathcal{C})\alpha T + \deg \mathcal{C} \gamma T + C_0 \alpha T \deg \mathcal{C} + NC(E),$$

and hence

$$\begin{aligned} \widehat{h}(P) &\le N h_2(\mathcal{C})\alpha T + N(\gamma + C_0\alpha) T \deg \mathcal{C} + N^2 C(E) \\ &\le \delta h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{N-r}} + \delta(N^2 C(E) + C_0)(\deg \mathcal{C})^{\frac{N}{N-r}} + N^2 C(E), \end{aligned}$$

where

$$\delta = N\alpha \Big(\frac{N}{N-1} \beta \Big)^{\frac{r}{N-r}}. \qquad \blacksquare$$

6.2 The General Case

We can now conclude the proof of Theorem 1.3, reducing the case of a general curve to the transverse case with a geometric induction.

Theorem 6.2 *Let $\mathcal{C}$ be a curve of genus at least 2 embedded in E^N, and let $K = \mathrm{frac}(\mathrm{End}(E))$ with discriminant D_K and $f = [\mathcal{O}_K : \mathrm{End}(E)]$. Then the set of points of $\mathcal{C}$ of rank $r < \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}})$ has Néron-Tate height bounded as*

$$\widehat{h}(P) \le D_1 h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{t_{\mathcal{C}} - r}} + D_1\Big(t_{\mathcal{C}}^2 C(E) + C_0 \Big)(\deg \mathcal{C})^{\frac{t_{\mathcal{C}}}{t_{\mathcal{C}} - r}} + (N-r) t_{\mathcal{C}}^2 C(E) + \frac{h(\mathcal{C})}{\deg \mathcal{C}},$$

where

$$D_1 = (N-r)\delta\big(t_{\mathcal{C}}, r, f, |D_K| \big),$$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

and δ is defined in Theorem 6.1*; $C(E)$ is the explicit constant defined in Proposition* 2.1 *and depends only on the coefficients of E.*

Proof Let $H_0 + Q$ be a translate of minimal dimension $t_{\mathcal{C}}$ containing $\mathcal{C}$, with H_0 an abelian subvariety of E^N and Q a point in $H_0^{\perp}$. Then $\mathcal{C} = \mathcal{C}_0 + Q$ with $\mathcal{C}_0$ transverse in H_0, and so the rank of any point of $\mathcal{C}$ is at least rank Q. Thus, there are no points on $\mathcal{C}$ of rank less than rank Q. Moreover, rank $Q = r_{\mathcal{C}} - t_{\mathcal{C}}$. Indeed, if B_Q is the torsion variety of minimal dimension containing Q, then by definition of rank $\dim B_Q$ = rank Q. Thus, $\mathcal{C}$ is contained in the torsion variety $H_0 + B_Q$ of dimension $t_{\mathcal{C}} + \operatorname{rank} Q$. On the other hand, if B is the torsion variety of minimal dimension containing $\mathcal{C}$, then $\mathcal{C} - Q = \mathcal{C}_0 \subset B - Q$. Thus, $H_0 \subset B - Q$ and $H_0 + Q \subset B$. Since H_0 is an abelian variety, $Q \in B$. Thus, $H_0 + B_Q \subset B$. And equality follows by the minimality of B. So $r_{\mathcal{C}} = t_{\mathcal{C}} + \operatorname{rank} Q$.

In conclusion, there are no points of rank $<$ rank $Q = r_{\mathcal{C}} - t_{\mathcal{C}}$. This solves the case $r_{\mathcal{C}} - t_{\mathcal{C}} \geq t_{\mathcal{C}}$.

We now assume that $t_{\mathcal{C}} > r_{\mathcal{C}} - t_{\mathcal{C}}$. The torsion variety H_0 is a component of the kernel of a morphism given by an $(N - t_{\mathcal{C}}) \times N$-matrix Φ with entries in $\operatorname{End}(E)$ and of rank $N - t_{\mathcal{C}}$, as described in Section 2.8. Then there exists an orthogonal complement matrix $\Phi^{\perp}$ with entries in $\operatorname{End}(E)$. Let $P \in \mathcal{C}$ be a point of rank r; then $P = P_0 + Q$ with $P_0 \in H_0$ and $\widehat{h}(P) = \widehat{h}(P_0 + Q) = \widehat{h}(P_0) + \widehat{h}(Q)$ by [Phi12]. This also shows that every point in $\mathcal{C}$ has height at least $\widehat{h}(Q)$, and therefore by definition of essential minimum we get that $\widehat{\mu}(\mathcal{C}) \geq \widehat{h}(Q)$. If P_0 is a torsion point, then we can directly conclude the proof; indeed, $\widehat{h}(P) = \widehat{h}(Q) \leq \widehat{\mu}(\mathcal{C}) \leq h(\mathcal{C})/\deg \mathcal{C}$ by Zhang's inequality. We can then assume that P_0 is non-torsion. Let P_{i_0} be the coordinate of P_0 of maximal height; then P_{i_0} is non-torsion.

Using basic arguments of linear algebra and a Gauss-reduction process (which might also determine a reordering of the coordinates), we can reduce the matrix Φ to the form

$$M = \begin{pmatrix} a_1 & \cdots & 0 & a_{1,N-t_{\mathcal{C}}} & \cdots & a_{1,N} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & a_{N-t_{\mathcal{C}}} & a_{N-t_{\mathcal{C}},N-t_{\mathcal{C}}+1} & \cdots & a_{N-t_{\mathcal{C}},N} \end{pmatrix},$$

with $a_i \neq 0$ for all i and the matrix $\Phi^{\perp}$ to the form

$$M^{\perp} = \begin{pmatrix} b_{1,1} & \cdots & b_{1,t_{\mathcal{C}}} & b_1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ b_{t_{\mathcal{C}},1} & \cdots & b_{t_{\mathcal{C}},t_{\mathcal{C}}} & 0 & \cdots & b_{t_{\mathcal{C}}} \end{pmatrix},$$

with $b_i \neq 0$ for all i.

In addition, we can assume that the $(N - t_{\mathcal{C}} + 1)$-th column of the reduced matrices M and $M^{\perp}$ corresponds to the i_0 coordinate of the starting order of the factors in E^N. For, if not, then if the i_0 coordinate corresponds to one of the last $t_{\mathcal{C}}$ columns it is sufficient to apply a reordering of the columns (which corresponds to a permutation of the factors of E^N) and of the rows of $M^{\perp}$. Suppose now that the i_0-th coordinate corresponds to the column $j \leq N - t_{\mathcal{C}}$; then since P_{i_0} is a non torsion point, there exists a non-trivial entry $M_{jk} \neq 0$ with $N - t_{\mathcal{C}} < k \leq N$. In addition, $b_k \neq 0$, and by the orthogonality assumption $M^{\perp}_{jk} \neq 0$. Thus, we can exchange the j-th and k-th

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

columns of M and $M^\perp$ and apply a new Gauss reduction to obtain the matrix M and $M^\perp$ with the desired properties.

Passing to the Lie algebras, the kernels of these matrices determine the Lie algebra of H_0 and $H_0^\perp$ as sub-Lie algebras of E^N. Thus the rows of $M^\perp$ are a basis of the Lie algebra of H_0. Since the last $t_{\mathcal{C}}$ columns of $M^\perp$ form an invertible minor, the projection of the last $t_{\mathcal{C}}$ coordinates of $\mathrm{Lie}(H_0)$ on $\mathbb{C}^{t_{\mathcal{C}}}$ is surjective. Thus, the projection $\pi\colon E^N \to E^{t_{\mathcal{C}}}$ on the last $t_{\mathcal{C}}$ coordinates is surjective when restricted to H_0 and consequently $\pi(\mathcal{C}) = \pi(\mathcal{C}_0)$ is transverse in $E^{t_{\mathcal{C}}}$. By a result of Masser and Wüstholz [MW90, Lemma 2.1], we have that $\deg \pi(\mathcal{C}) \le \deg \mathcal{C}$. In addition, $h(\pi(\mathcal{C})) \le h(\mathcal{C})$.

We can now apply Theorem 6.1 to the curve $\pi(\mathcal{C})$ in $E^{t_{\mathcal{C}}}$, obtaining

$$\widehat{h}(\pi(P)) \le \delta h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{t_{\mathcal{C}}-r}} + \delta\big(t_{\mathcal{C}}^2 C(E) + C_0\big)(\deg \mathcal{C})^{\frac{t_{\mathcal{C}}}{t_{\mathcal{C}}-r}} + t_{\mathcal{C}}^2 C(E), \tag{6.5}$$

where $\delta = \delta(t_{\mathcal{C}}, r, f, D_K)$ is given in Theorem 6.1 and $C(E)$ is defined in Proposition 2.1.

We finally remark that

$$\widehat{h}(P) = \widehat{h}(P_0 + Q) = \widehat{h}(P_0) + \widehat{h}(Q) \le (N-r)\widehat{h}(\pi(P)) + \widehat{h}(Q),$$

where the last inequality is due to the fact that the $(N - t_{\mathcal{C}} + 1)$-th coordinate of P_0 has maximal height. Recall that, as clarified above, $\widehat{h}(Q) \le \widehat{\mu}(\mathcal{C})$, and by Zhang's inequality $\widehat{\mu}(\mathcal{C}) \le h(\mathcal{C})/\deg \mathcal{C}$. So $\widehat{h}(Q) \le h(\mathcal{C})/\deg \mathcal{C}$, and so

$$\widehat{h}(P) \le \widehat{h}(P_0) + \widehat{h}(Q) \le (N-r)\widehat{h}(\pi(P)) + \frac{h(\mathcal{C})}{\deg \mathcal{C}}.$$

Replacing (6.5) we obtain the bound

$$\widehat{h}(P) \le (N-r)\delta h_2(\mathcal{C})(\deg \mathcal{C})^{\frac{r}{t_{\mathcal{C}}-r}} + (N-r)\delta\big(t_{\mathcal{C}}^2 C(E) + C_0\big)(\deg \mathcal{C})^{\frac{t_{\mathcal{C}}}{t_{\mathcal{C}}-r}} + (N-r)t_{\mathcal{C}}^2 C(E) + \frac{h(\mathcal{C})}{\deg \mathcal{C}}. \qquad \blacksquare$$

6.3 The Proof of Corollary 1.5

In [CVV16, Theorem 6.2], we proved that the curve $\mathcal{C}$ is transverse in E^2 and its degree and height are bounded as

$$\deg \mathcal{C} = 6n + 9, \quad h_2(\mathcal{C}) \le 6(2n+3)\big(h_W(p) + \log m + 2C(E)\big),$$

where $h_W(p) = h_W(1 : p_0 : \cdots : p_n)$ is the height of the polynomial $p(X)$ and $C(E)$ is given in Proposition 2.1. Applying Theorem 6.1 to $\mathcal{C}$ in E^2 (with $N = 2$ and $r = 1$), we get that

$$\widehat{h}(P) \le f^9 |D_K|^{\frac{9}{2}} 2^{39}\big(h_2(\mathcal{C})(\deg \mathcal{C}) + (4C(E) + 5.61)(\deg \mathcal{C})^2\big) + 4C(E).$$

Substituting the values of $\deg \mathcal{C}$ and $h_2(\mathcal{C})$, we conclude the proof. $\blacksquare$

https://doi.org/10.4153/CJM-2017-045-0 Published online by Cambridge University Press

6.4 The Proof of Corollary 1.6

To prove our corollary we use the same projection $\pi\colon E^N \to E^{t_{\mathcal{C}}}$ used in the proof of Theorem 6.2. Then $\pi(\mathcal{C})$ is transverse in $E^{t_{\mathcal{C}}}$. In addition, $\deg \pi(\mathcal{C}) \leq \deg \mathcal{C}$ and $h(\pi(\mathcal{C})) \leq h(\mathcal{C})$. The proof of Theorem 6.2 also shows that there are no points on $\mathcal{C}$ of rank $< r_{\mathcal{C}} - t_{\mathcal{C}}$. We then apply Theorem 6.1 and [Via08, Theorem 1.3] to the curve $\pi(\mathcal{C})$ in $E^{t_{\mathcal{C}}}$ to bound the number of points of rank $< t_{\mathcal{C}} - 1$ on $\pi(\mathcal{C})$. Note that the rank of the projection of a point is less than or equal to the rank of the point. Moreover, the fiber of π restricted to $\mathcal{C}$ has cardinality $\leq \deg \mathcal{C} \deg E^{N-t_{\mathcal{C}}}$ by Bézout's theorem. This bounds the number of points on $\mathcal{C}$ of rank $< \max(r_{\mathcal{C}} - t_{\mathcal{C}}, t_{\mathcal{C}} - 1)$ in terms of $\deg \mathcal{C}$, $\deg \pi(\mathcal{C})$, $h_2(\pi(\mathcal{C}))$, E and N. We finally use $\deg \pi(\mathcal{C}) \leq \deg \mathcal{C}$ and $h(\pi(\mathcal{C})) \leq h(\mathcal{C})$ to conclude.

Acknowledgments I kindly thank the referee for his accurate and valuable comments. I thank Sara Checcoli for her contribution on some computations. I also thank Özlem Imamoglu for some nice discussions.

References

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*. New Mathematical Monographs, 4, Cambridge University Press, Cambridge, 2006.
[BMZ99] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*. Internat. Math. Res. Notices **20**(1999), 1119–1140.
[BV83] E. Bombieri and J. Vaaler, *On Siegel's lemma*. Invent. Math. **73**(1983), no. 1, 11–32. http://dx.doi.org/10.1007/BF01393823
[BGS94] J.-B. Bost, H. Gillet, and C. Soulé, *Heights of projective varieties and positive Green forms*. J. Amer. Math. Soc. **7**(1994), no. 4, 903–1027. http://dx.doi.org/10.1090/S0894-0347-1994-1260106-X
[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*. C. R. Acad. Sci. Paris **212**(1941), 882–885.
[CVV17] S. Checcoli, F. Veneziano, and E. Viada, *On the explicit torsion anomalous conjecture*. Trans. Amer. Math. Soc. **369**(2017), 6465–6491. http://dx.doi.org/10.1090/tran/6893
[CVV16] ———, *The explicit Mordell conjecture for families of curves*. 2016. arxiv:1602.04097
[CV14] S. Checcoli and E. Viada, *On the torsion anomalous conjecture in CM abelian varieties*. Pacific J. Math. **271**(2014), no. 2, 321–345. http://dx.doi.org/10.2140/pjm.2014.271.321
[Col85] R. F. Coleman, *Effective Chabauty*. Duke Math. J. **52**(1985), 765–780. http://dx.doi.org/10.1215/S0012-7094-85-05240-8
[Cox89] D. A. Cox, *Primes of the form $x^2 + ny^2$*. Wiley, New York, 1989.
[Dem68] V. Dem'janenko, *Rational points on a class of algebraic curves*, Amer. Math. Soc. Transl. **66**(1968), 246–272.
[Hab08] P. Habegger, *Intersecting subvarieties of $\mathbb{G}_m^n$ with algebraic subgroups*. Math. Ann. **342**(2008), no. 2, 449–466. http://dx.doi.org/10.1007/s00208-008-0242-3
[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73**(1983), 349–366. http://dx.doi.org/10.1007/BF01388432
[Kul99] L. 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.
[KMS04] L. Kulesz, G. Matera, and E. Schost, *Uniform bounds for the number of rational points of families of curves of genus 2*. J. Number Theory **108**, (2004), 241–267.
[Man69] J. Manin, *The p-torsion of elliptic curves is uniformly bounded*. Isv. Akad. Nauk. SSSR Ser. Mat. **33**(1969), 459–465. http://dx.doi.org/10.1006/jnth.1998.2339
[MP10] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*. In: Explicit methods in number theory; rational points and diophantine equations, Panoramas et Synthèses, 36, Soc. Math. France, Paris, 2012, pp. 99–117.
[MW90] D. Masser and G. Wüstholz, *Estimating isogenies on elliptic curves*. Invent. Math. **100**(1990), 1–24.

[MW93] D. Masser and G. Wüstholz, *Periods and minimal abelian subvarieties*. Ann. of Math. (2) **137**(1993), no. 2, 407–458. http://dx.doi.org/10.2307/2946542
[Neu99] J. Neukirch, *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin, 1999.
[Phi91] P. Philippon, *Sur des hauteurs alternatives. I*. Math. Ann. **289**(1991), no. 2, 255–284. http://dx.doi.org/10.1007/BF01446571
[Phi95] _____, *Sur des hauteurs alternatives. III*. J. Math. Pures Appl. (9) **74**(1995), no. 4, 345–365.
[Phi12] _____, *Sur une question d'orthogonalité dans les puissances de courbes elliptiques*. 2012. https://hal.archives-ouvertes.fr/hal-00801376/document
[Ser89] J.-P. Serre, *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989.
[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.
[Sil90] _____, *The difference between the Weil height and the canonical height on elliptic curves*. Math. Comp. **55**(1990), no. 192, 723–743. http://dx.doi.org/10.1090/S0025-5718-1990-1035944-5
[Sto11] M. Stoll, *Rational points on curves*. J. Théor. Nombres Bordeaux **23**(2011), 257–277. http://dx.doi.org/10.5802/jtnb.760
[Via03] E. 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.
[Via08] _____, *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. http://dx.doi.org/10.2140/ant.2008.2.249
[Via15] _____, *Explicit height bounds and the effective Mordell-Lang Conjecture*. Riv. Math. Univ. Parma (N.S.) **7**(2016), no. 1, 101–131.
[Win17] B. Winckler. *Probléme de Lehmer sur les courbes elliptiques à multiplications complexes*. 2017. https://hal.archives-ouvertes.fr/hal-01493577
[Zan12] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry (with appendixes by D. Masser)*. Annals of Mathematics Studies, 181, Princeton University Press, Princeton, NJ, 2012.
[Zha95] S. Zhang, *Positive line bundles on arithmetic varieties*. J. Amer. Math. Soc. **8**(1995), no. 1, 187–221. http://dx.doi.org/10.1090/S0894-0347-1995-1254133-7

Mathematisches Institut, Georg-August-Universität, Bunsenstraße 3-5, D-D-37073, Göttingen, Germany
e-mail: evelina.viada@mathematik.uni-goettingen.de