mathematics

MDPI

Article

Lattices and Rational Points

Evelina Viada

Mathematisches Institut, Georg-August-Universität, Bunsenstraße 3–5, D-D-37073 Göttingen, Germany;
evelina.viada@math.ethz.ch

Received: 12 June 2017; Accepted: 4 July 2017; Published: 9 July 2017

Abstract: In this article, we show how to use the first and second Minkowski Theorems and some Diophantine geometry to bound explicitly the height of the points of rank $N-1$ on transverse curves in E^N, where E is an elliptic curve without Complex Multiplication (CM). We then apply our result to give a method for finding the rational points on such curves, when E has $\mathbb{Q}$-rank $\leq N-1$. We also give some explicit examples. This result generalises from rank 1 to rank $N-1$ previous results of S. Checcoli, F. Veneziano and the author.

Keywords: heights; rational points; curves; elliptic curves

1. Introduction

A classical question in the context of Diophantine geometry is to determine the points of a certain shape, for instance the rational points, on an algebraic curve. Much work has been done in this direction. By 'variety', we mean an algebraic variety defined over the algebraic numbers embedded in some projective space. For k, a number field and V a variety defined over k, we denote by $V(k)$ the set of k-rational points on V.

The genus of the curve distinguishes three quantitatively different behaviours for its rational points. For a curve of genus 0, either the set of k-rational points is empty or the curve is isomorphic to the projective line, whose k-rational points are infinitely many and well-understood. On the other hand, for genus of at least 2, we have the:

Mordell Conjecture. *A curve of genus at least 2 defined over a number field k has only finitely many k-rational points.*

This is a very deep result, first conjectured by Mordell in [1] and now known as Faltings Theorem after the ground-breaking proof in [2]. The curves of genus 1 can be endowed with the structure of an abelian group and the set of k-rational points, when not empty, is a finitely generated group. This is a famous theorem of Mordell, later generalised by Weil to the case of abelian varieties. The number of generators is called the k-rank of the abelian variety.

Vojta in [3] gave a new proof of the Mordell Conjecture and then Faltings, in [4,5], proved an analogous statement for rational points on subvarieties of abelian varieties, which generalises to points in a finitely generated subgroup Γ. Building on these results, Hindry [6] proved the case of Γ of finite rank, known as the Mordell–Lang Conjecture.

Mordell–Lang Conjecture. *Let Γ be a subgroup of finite rank of an abelian variety A. Let $V \subseteq A$ be a proper subvariety. Then, the set $\Gamma \cap V$ is contained in a finite union of translates of proper abelian subvarieties by elements of Γ.*

Unfortunately, even for curves, the different proofs of this theorem are not effective, in the sense that they prove the finiteness of the desired set, but do not hint at how this set could be determined.

One of the challenges of the last century has been the search for effective methods, but there is still no known general method for finding all the rational points on a curve. Most of the known examples are curves of small genus, often 2 or 3. They rely on the Chabauty-Coleman method (see the articles [7,8]) and on the Manin-Dem'janenko method (see [9,10]). An overview is given by J.P. Serre in his book [11] in Chapter 5. The Chabauty-Coleman method has been used by Flynn [12] to determine rational points on some families of hyperelliptic curves with special Jacobians of dimension 2 and rank one, respectively, of dimension 3 and rank 2. The Manin and Dem'janenko method 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 $A(k) < m$. Some explicit examples are, for instance, given by Kulesz [13] and Kulesz, Matera and Schost [14] for some families of algebraic curves of genus 2 with Jacobian isogenous to a product of special elliptic curves of $\mathbb{Q}$-rank one.

Unfortunately, these methods do not give an explicit dependence of the height of the k-rational points neither in terms of the curve nor in terms of the ambient variety. Thus, to apply the methods, such a dependence must be elaborated case by case with ad hoc strategies.

The theory of anomalous intersections introduced by Bombieri, Masser and Zannier [15] is well known to have implications on the Mordell–Lang Conjecture and leads to many new open conjectures, such as the Torsion Anomalous Conjecture (TAC), which remains open in its generality (see the book of Zannier [16] and the survey article [17]). The TAC implies the Zilber–Pink Conjecture, the Manin–Mumford and the Mordell–Lang Conjectures. There are also relations to model theory and to algebraic dynamics, in the context of the Morton Conjectures. The TAC is essentially only known for curves in abelian varieties (after work of Bombieri, Masser, Zannier, Rémond, Viada, Galateaux, Habbeger and Pila and others) and for varieties of codimension 2 embedded in tori (Bombieri, Masser and Zannier) and in E^N (Checcoli, Veneziano, Viada). Many of these results are proven in a non effective way. However, some methods in the context of anomalous intersections are effective, and this has some implications on the effective Mordell–Lang Conjecture.

In the last years, together with S. Checcoli and F. Veneziano, we have been working to approach the problem of anomalous intersections with explicit methods aiming to prove new cases of the explicit Mordell Conjecture and to eventually find all the rational points on some new families of algebraic curves. Our setting is compatible with the one of the Manin-Dem'janenko Theorem.

Let us introduce notation and definitions.

We denote by E an elliptic curve and, for any positive integer N, we denote by E^N the cartesian product of N copies of E. We say that a subvariety $V \subset E^N$ is a *translate*, respectively, a *torsion variety*, if it is a finite union of translates of proper algebraic subgroups of E^N by points, respectively by torsion points.

Furthermore, an irreducible variety $V \subset E^N$ is *transverse*, respectively *weak-transverse*, if it is not contained in any translate, respectively in any torsion variety.

We remember that the rank of an abelian group is the number of generators over $\mathbb{Z}$ of its free part and the k-rank of an elliptic curve E defined over k, for k a number field, is the rank of $E(k)$ as an abelian group. We introduce here a new concept of rank for a point on E^N.

Definition 1. *The rank of a point P in E^N is the minimal dimension of an algebraic subgroup of E^N containing the point.*

The following observation clarifies the definition: the rank of P is equal to the dimension of the Zariski-closure in E^N of the set of all multiples of P, i.e., of the set $\{[n]P : n \in \mathbb{Z}\}$.

In a joint paper with S. Checcoli and F. Veneziano (see [18]), we prove that the points of rank one on a weak-transverse curve of E^N have bounded height and we explicitly bound their height if E is non CM. We also give a non-density result for the points of rank one on a weak-transverse variety of E^N. In [19], the author extends the method for curves in E^N, where E has CM. Unfortunately, these bounds are much too big to be used to find the rational points on any curve.

In [20], together with Checcoli and Veneziano we use a different apprach and we provide a new sharp explicit upper bound for the height of the points on a curve of genus at least 2 in E^2, where E is a non-CM elliptic curve. In particular, we prove the explicit Mordell-Conjecture for such curves, when E has $\mathbb{Q}$-rank 1. We also present a variety of explicit examples: we give two families of curves of growing genus in E^2, where E is non-CM and of $\mathbb{Q}$-rank 1, for which we can list all the rational points. Compared to the other effective methods, ours is easier to apply because it provides a simple formula for the bound for the height of the rational points. Moreover, it applies to curves of any genus and not only of small genus.

The assumptions in [20] represent the easiest setting in this context: points of rank one. We tested there the possibility of producing an explicit and even an implementable method for finding the rational points on some new families of algebraic curves in E^2.

In this article, we extend the method introduced in [20] for curves transverse in E^N and to points of rank $N-1$ instead of 1, where E is non-CM. We then give some new examples of curves for which we could determine all the rational points.

To state our main theorem, we first fix the setting (see Section 3 for more details). Let E be an elliptic curve given in the form:

$$y^2 = x^3 + Ax + B.$$

Via the given equation, we embed E^N into $\mathbb{P}_2^N$ and via the Segre embedding in $\mathbb{P}_{3^N-1}$.

The degree of a curve $\mathcal{C} \subseteq E^N$ is the degree of its image in $\mathbb{P}_{3^N-1}$ and $h_2(\mathcal{C})$ is the normalised height of $\mathcal{C}$, which is defined in terms of the Chow form of the ideal of $\mathcal{C}$, as done in [21]. We denote by $\hat{h}$ the canonical Néron–Tate height on E^N.

Our main theorem is:

Theorem 2. *Let E be an elliptic curve without CM. Let $\mathcal{C}$ be a curve transverse in E^N. Then, all the points P of rank at most $N-1$ on $\mathcal{C}$ have Néron–Tate height bounded as:*

$$\hat{h}(P) \leq C_1 \cdot h_2(\mathcal{C})(\deg \mathcal{C})^{N-1} + C_2(E)(\deg \mathcal{C})^N + NC(E),$$

where:

$$\begin{aligned} C_1 &= 2^{N+2}3^{N-1}(N-1)!c_2(N)^{N-1}, \\ C_2(E) &= 2^{N+2}3^{N-1}(N-1)!\,(NC(E)+C_0)\,c_2(N)^{N-1}, \\ c_2(N) &= \frac{3^{N-1}N^2(N-1)^3(N-1)!^5}{4^{N-2}}, \end{aligned}$$

and $C(E)$ depends only on A and B and is defined in Proposition 6 and $C_0 = C_0(1, N-1, 3^N-1)$ is defined in (8).

We remark that, for k, a number field of the definition of E, if E has k-rank $N-1$ (i.e., the rank of $E(k)$ as an abelian group), then the set of k-rational points $\mathcal{C}(k)$ of $\mathcal{C} \subset E^N$ is contained in the set of points of rank $N-1$ (in the sense of Definition 1) and so $\mathcal{C}(k)$ has a height bounded as above. This immediately gives the following:

Corollary 3. *Let E be an elliptic curve without CM defined over a number field k. Assume that E has k-rank $< N$. Let $\mathcal{C}$ be a curve transverse in E^N. Then, any k-rational point $P \in \mathcal{C}(k)$ has Néron–Tate height bounded as:*

$$\hat{h}(P) \leq C_1 \cdot h_2(\mathcal{C})(\deg \mathcal{C})^{N-1} + C_2(E)(\deg \mathcal{C})^N + NC(E),$$

where the constants are the same as in Theorem 2.

The proof of our main theorem relies basically on the first and second Minkowski theorems, on Zhang's inequality and on the Arithmetic Bézout Theorem. Precise estimates for different height functions must be used as well as computations of degree in some projective spaces.

The independence of the bound on k and on the generators of $E(k)$ is an interesting aspect, specifically for applications. In the following section, we present one of the possible applications of our Theorem. These are just examples and many others can be created using the same ideas.

2. An Application to Some Explicit Curves

An interesting feature of our main theorem is that it can be applied to find the rational points on some new curves. We present here an example. We remark that any curve transverse in E^3 with E of $\mathbb{Q}$-rank ≤ 2 is suitable for further examples of our method.

Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$. We write:

$$\begin{aligned} y_1^2 &= x_1^3 + Ax_1 + B, \\ y_2^2 &= x_2^3 + Ax_2 + B, \\ y_3^2 &= x_3^3 + Ax_2 + B, \end{aligned} \tag{1}$$

for the equations of E^3 in $\mathbb{P}_2^3$ using affine coordinates $(x_1, y_1) \times (x_2, y_2) \times (x_3, y_3)$, and we embed E^3 in $\mathbb{P}_{26}$ via the Segre embedding.

In order to apply our main theorem, the elliptic curve E shall be an elliptic curve over $\mathbb{Q}$ without CM and $\mathbb{Q}$-rank 2. Several examples of such E can be easily found in Cremona's tables [22]. For instance, we consider the following elliptic curves:

$$\begin{aligned} E_1 &: y^2 = x^3 - 7x + 10, \\ E_2 &: y^2 = x^3 - 4x + 1, \\ E_3 &: y^2 = x^3 - 19x + 34, \\ E_4 &: y^2 = x^3 - 28x + 52, \\ E_5 &: y^2 = x^3 - 4x + 16. \end{aligned} \tag{2}$$

These are five elliptic curves without CM, of rank two over $\mathbb{Q}$ and with trivial torsion. The generators are:

$(5, -10); (-2, 4)$	for E_1,
$(-1, 2); (0, 1)$	for E_2,
$(11, 34); (-3, 8)$	for E_3,
$(-4, 10); (-2, 10)$	for E_4,
$(-2, 4); (0, 4)$	for E_5.

While the constant $C(E)$ appearing in our main theorem is bounded as follows:

$$C(E_1) \leq 20; \quad C(E_2) \leq 16 \quad C(E_3) \leq 24; \quad C(E_4) \leq 24; \quad C(E_5) \leq 12.$$

We then consider the following family of curves that extend the one considered in [20]. There, however, we could only cut curves on E^2 with E of $\mathbb{Q}$-rank 1.

Definition 4. *Let $\{C_n\}_n$ be the family of projective curves in E^3 with affine part defined for $n \geq 1$ via the additional equations:*

$$x_1^n = y_2 \quad \text{and} \quad x_2 = y_3.$$

We remark that our curve $\mathcal{C}_n$ is the intersection in $\mathbb{P}_{26}$ of a hypersurface $X \subset \mathbb{P}_{26}$ and a surface $S_n \subset E^3$, where X is given in $\mathbb{P}_{26}$ by the linear equation $w_1 = w_2$ with $w_1 = x_1x_2z_3$ and $w_2 = x_1z_2y_3$ under the Segre embedding of $\mathbb{P}_2 \times \mathbb{P}_2 \times \mathbb{P}_2$ in $\mathbb{P}_{26}$. Thus:

$$\deg X = 1.$$

Moreover, S_n is the projective closures in E^3 of the surface defined for $n \geq 1$ via the additional equation $x_1^n = y_2$. Thus, the S_n are of the form $C_n \times E$ for C_n the curves defined in [20] (Definition 1.4), i.e., $C_n \subset E^2 \times 0$ given by the additional equation $x_1^n = y_2$. From [20] Corollary 7.1, we know that $\deg C_n = 6n + 9$. Thus, $\mathcal{C}_n$ has bidegree $(6n + 9, 3)$ in $\mathbb{P}_8 \times \mathbb{P}_2$. Recall that $\mathbb{P}_8 \times \mathbb{P}_2$ has degree $\frac{10!}{8!2!}$ in $\mathbb{P}_{26}$. Thus:

$$\deg S_n \leq 3(6n + 9)3^2 5.$$

By Bézout's Theorem:

$$\deg \mathcal{C}_n \leq \deg(S_n \cap X) \leq \deg(S_n) \deg X \leq 3^4 5(2n + 3).$$

We now want to estimate the height of $\mathcal{C}_n$. We use the same idea as in [20] (Theorem 6.2). By Zhang's inequality (9), we have $h_2(\mathcal{C}_n) \leq 2 \deg \mathcal{C}_n \mu_2(\mathcal{C}_n)$. An upper bound for $\mu_2(\mathcal{C}_n)$ is given by constructing an infinite set of points on $\mathcal{C}_n$ of bounded height. Let $Q_\zeta = ((\zeta, y_1), (x_2, y_2), (x_3, y_3)) \in \mathcal{C}_n$, where $\zeta \in \overline{\mathbb{Q}}$ is a root of unity. Clearly there exist infinitely many such points on $\mathcal{C}_n$. Using the equations of $\mathcal{C}_n$ and classical estimates on the Weil height, for all points Q_ζ, we have:

$$h_2(Q_\zeta) = h_2(\zeta, y_1) + h_2(x_2, \zeta^n) + h_2(x_3, x_2).$$

By the proof of [20] (Theorem 6.2), we know that:

$$h_2(\zeta, y_1) \leq c_6(E),$$
$$h_2(x_2, \zeta^n) \leq c_6(E),$$

where $c_6(E) = \frac{\log(3+|A|+|B|)}{2}$. By [20] (Lemma 3.1), we get:

$$h_2(x_3, x_2) \leq 2c_6(E).$$

Thus:

$$\mu_2(\mathcal{C}_n) \leq 2\log(3 + |A| + |B|)$$

and by Zhang's inequality:

$$h_2(C_n) \leq 2^2 3^4 5(2n + 3) \log(3 + |A| + |B|).$$

A similar argumentation as in [20], Lemma 7.2 shows that the genus of the curves $\mathcal{C}_n$ is increasing and it is greater than 1, so the $\mathcal{C}_n$ are not traslates of an elliptic curve. Unlike in [20], this is not sufficient to conclude that the curves are transverse. In fact, curves of any genus are contained in $E^2 \times 0$, and they are not even weak-transverse. Therefore, in order to apply our main Theorem, we shall now show that the $\mathcal{C}_n$ are transverse in E^3. We remark that, if not, then $\mathcal{C}_n \subset G + p$ for some algebraic subgroup G of dimension 2 and a point $p \in E^3$. Moreover, $\mathcal{C}_n - p$ is transverse in G because the genus of $\mathcal{C}_n$ is not 1. Thus, $\mathcal{C}_n + \mathcal{C}_n = G + 2p$ and $\deg G \leq 2^3(\deg \mathcal{C}_n)^2$, where 2^3 is a bound for the sum morphism. Therefore, G is defined by an equation $a_1X_1 + a_2X_2 + a_3X_3 = 0$ with $a_i \in \mathbb{Z}$. Let $a = (a_1, a_2, a_3) \in \mathbb{Z}^3$, and then $||a||^2 \leq \deg G \leq 2^3(\deg \mathcal{C}_n)^2$.

It follows that there are only finitely many possibilities for such an a and so for G. To check that $\mathcal{C}_n$ is not contained in any such $G + p$, it is then sufficient to show that the morphisms $a : E^3 \to E$ with $||a||^2 \leq 2^3(\deg \mathcal{C}_n)^2$ are not constant when restricted to $\mathcal{C}_n$. Remark that the fiber in $\mathcal{C}_n$ of a point is either $\mathcal{C}_n$ or at most $m = \deg \mathcal{C}_n \deg G$ points. Let $P_0, \dots P_m$ be $m+1$ distinct points on $\mathcal{C}_n$ (defined over any field). If there exists at least one index $1 \le i \le m$ such that the images $a(P_0 - P_i) \neq 0$, then the morphism a is not constant and $\mathcal{C}_n$ is transverse. For $n \le 100$, this is checked with an algorithmic implementation. Thus, for $n \le 100$, the $\mathcal{C}_n$ are transverse. We can now apply our Corollary 3 with $N = 3$ to the curves $\mathcal{C}_n$ for $n \le 100$. We obtain:

Theorem 5. *Let E be an elliptic curve without CM and such that E has $\mathbb{Q}$-rank 2. For $n \le 100$, the rational points on $\mathcal{C}_n \subset E^3$ have Néron–Tate height bounded as:*

$$\hat{h}(P) \le 2^{18}3^{11} \cdot h_2(\mathcal{C}_n)(\deg \mathcal{C}_n)^2 + 2^{18}3^{11}\Big(3C(E) + C_0\Big)(\deg \mathcal{C}_n)^3 + 3C(E),$$

where:

$$\begin{aligned}\deg \mathcal{C}_n &\le 3^4 5(2n+3),\\ h_2(\mathcal{C}_n) &\le 2^2 3^4 5(2n+3)\log(3 + |A| + |B|),\end{aligned}$$

and $C(E)$ is defined in Proposition 6 and $C_0 = C_0(1,2,26) \le 19$ is defined in (8).

With an algorithm similar to the one presented in [20], we can finally check if any rational point of height bounded as above belongs to the curve $\mathcal{C}_n \subset E_i^3$, where E_i for $i = 1,2,3,4,5$ are the elliptic curves given in relation (2) above. For any i, we obtain bounds for the height of the rational points between $2^{23}3^{23}5^3$ for the curves of lowest degree and $2^{25}3^{23}5^9$ for the ones of largest degree.

3. 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, such as the Arithmetic Bézout Theorem and the Zhang Inequality.

The word *rank* is used with several different meanings. For clarity, we remember that the rank of an abelian group is the number of generators over $\mathbb{Z}$ of its free part; the rank of an R-module M for R a ring with field of franction $\mathrm{frac}(R)$ 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.

Let E be an elliptic curve defined over a number field k by a fixed Weierstrass equation:

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

with A and B in the ring of integers of k (this assumption is not restrictive). We denote the discriminant of E by:

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

and the j-invariant by:

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

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

$$E^N \hookrightarrow \mathbb{P}_2^N \hookrightarrow \mathbb{P}_{3^N-1}, \tag{4}$$

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.

3.1. Algebraic Subgroups

By the uniformisation theorem, there exists a unique lattice $\Lambda_0 \subset \mathbb{C}$ such that $\mathbb{C}/\Lambda_0 \xrightarrow{\sim} E(\mathbb{C})$ as complex Lie groups.

By [23] (Chapter 8), the set of abelian subvarieties of E^N of codimension r is in natural bijection with the set of complex vector subspaces $W \subset \mathbb{C}^N$ of codimension r for which $W \cap {\Lambda_0}^N$ is a lattice of full rank in W. Therefore, W is given by a linear system of rank r with matrix of the coefficients φ_B in $\mathrm{Mat}_{r\times N}(\mathrm{End}(E))$. We identify φ_B with the induced morphism $\varphi_B : E^N \to E^r$. On the other hand, a matrix in $\mathrm{Mat}_{r\times N}(\mathrm{End}(E))$ of rank r defines an algebraic subgroup of codimension r. Recall that in the non-CM case $\mathrm{End}(E) \cong \mathbb{Z}$.

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 $\mathbb{C}^N$.

3.2. Heights of Points

If $P = (P_1 : \ldots : P_n) \in \mathbb{P}_n(\overline{\mathbb{Q}})$ 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:

$$h_2(P) = \sum_{v \text{ finite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max_i\{|P_i|_v\} + \sum_{v \text{ infinite}} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \left(\sum_i |P_i|_v^2\right)^{1/2}. \tag{5}$$

For a point $P \in E$, we denote by $\hat{h}(P)$ its Néron–Tate height as defined in [24] (which is one third of the usual Néron–Tate height used also in [18]).

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

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

The following proposition directly follows from [25], Theorem 1.1 and [20], Proposition 3.2.

Proposition 6. *For $P \in E^N$, then:*

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

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 [20], Section 3.

3.3. 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 done in [21]. This height extends the height h_2 defined for points by formula (5) (see [26], Equation (3.1.6)). We also consider the canonical height $h(V)$, as defined in [24]; when the variety V reduces to a point P, then $h(P) = \hat{h}(P)$ (see [24], Proposition 9).

3.4. The Degree of Varieties

The degree of an irreducible variety $V \subset \mathbb{P}_m$ is the maximal cardinality of a finite intersection $V \cap L$, with L 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 [18], Lemma 2.1, we have:

$$\deg X(E,N) = 3^N N!. \tag{6}$$

In [20] Section 2.1, it is shown that the degree of an algebraic subgroup H of E^N defined by $\alpha_1 X_1 + \cdots \alpha_N X_N = O$ is given as the sum of the degrees of the projections of H to the coordinates elliptic curves E, that is, the sum of the intersection numbers of H with the coordinate hyperplanes in E^N. In view of (6), we see that the degree of such projections is $3^{N-1}(N-1)!|\alpha_i|^2$. This gives:

$$\deg H = 3^{N-1}(N-1)! \sum_{i=1}^{N} |\alpha_i|^2 . \tag{7}$$

3.5. The Arithmetic Bézout Theorem

The following explicit result is proven by Philippon in [21], Théorème 3. It describes the behavior of the height for intersections.

Theorem 7 (Arithmetic Bézout theorem)**.** *Let X and Y be irreducible closed subvarieties of $\mathbb{P}_m$ defined over the algebraic numbers. If $Z_1, \ldots, Z_g$ are the irreducible components of $X \cap Y$, then:*

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

where:

$$C_0(d_1, d_2, m) = \left(\sum_{i=0}^{d_1} \sum_{j=0}^{d_2} \frac{1}{2(i+j+1)} \right) + \left(m - \frac{d_1 + d_2}{2} \right) \log 2. \tag{8}$$

3.6. 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:

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

The following result is due to Zhang [27], Theorem 5.2:

Theorem 8 (Zhang inequality)**.** *Let $X \subset \mathbb{P}_m$ be an irreducible algebraic subvariety. Then:*

$$\mu_2(X) \leq \frac{h_2(X)}{\deg X} \leq (1 + \dim X) \mu_2(X). \tag{9}$$

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

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

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

$$\hat{\mu}(X) \leq \frac{h(X)}{\deg X} \leq (1 + \dim X) \hat{\mu}(X). \tag{10}$$

If X is an irreducible subvariety in E^N, using Proposition 6, we have:

$$-NC(E) \leq \mu_2(X) - \hat{\mu}(X) \leq NC(E), \tag{11}$$

where the constant $C(E)$ is defined in Proposition 6.

4. Bounds for the Height and the Degree of the Auxiliary Translate

In this section, we want to produce an auxiliary translate H that has a bounded degree and is close to our point P, where close means that the height of $H+P$ is not too big with respect to the height of P. This is proven in Proposition 13, which follows from the Proposition and Lemmas presented below.

4.1. Bounds for the Height and Degree of a Translate

Here, we prove some general bounds for the degree and the height of a proper translate $H+P$ in E^N of codimension 1 in terms of $\hat{h}(P)$ and of the coefficients of the equation defining the algebraic subgroup H. We use some linear algebra, the Cauchy–Binet formula and some bounds on heights from Section 3. When not otherwise specified, we use the canonical basis. We now extend [20] Proposition 5.1 for an arbitrary N.

Proposition 9. *Let P be a point in E^N, where E is without CM. Let H be a component of the algebraic subgroup in E^N defined by the equation $\alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_N X_N = O$, with $u = (\alpha_1, \ldots, \alpha_N) \in \mathbb{Z}^N \setminus \{0\}$. Then:*

$$\deg(H+P) \leq 3^{N-1}(N-1)! ||u||^2,$$

where $\|u\|$ denotes the Euclidean norm of u, and:

$$h_2(H+P) \leq 3^{N-1} N! \left(\hat{h}(u(P)) + NC(E) \|u\|^2\right),$$

where $u(P) = \alpha_1 P_1 + \cdots + \alpha_N P_N$.

Proof. Let $u = u_1 \in \mathbb{Z}^N$. Let $\Lambda = \langle u \rangle_{\mathbb{Z}} \subseteq \mathbb{R}^N$ be a lattice and let $\Lambda^\perp$ be its orthogonal lattice in $\mathbb{R}^N$.

Let $u_2, \ldots, u_N$ be a basis of $\Lambda^\perp$. The $(N-1) \times N$ matrix with rows $u_2, \ldots, u_N$ defines an algebraic subgroup $H^\perp$, given by the $N-1$ equations $u_i(X) = O$ for $i = 2, \ldots, N$. Then, 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 $u = u_1, \ldots, u_N$, and let Δ be its determinant.

Notice that, for u^t the transpose of u, we have:

$$\det \Lambda = \sqrt{u \cdot u^t} = \|u\|$$

and:

$$|\Delta| = \det \Lambda \cdot \det \Lambda^\perp \tag{12}$$

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

We remark that $u(P_0) = 0$ because $P_0 \in H$, and $u_i(P^\perp) = 0$ for all $i = 2, \ldots, N$ because $P^\perp \in H^\perp$.

Therefore:

$$UP^\perp = \begin{pmatrix} u(P^\perp) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} u(P_0 + P^\perp) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} u(P) \\ 0 \\ \vdots \\ 0 \end{pmatrix};$$

hence:

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

where U^{*} is the adjugate matrix of U.

Computing canonical heights and applying the Cauchy–Binet formula, we obtain:

$$|\Delta|^{2}\,\hat{h}(P^{\perp}) = \hat{h}([\Delta]P^{\perp}) = \det(\Lambda^{\perp})^{2}\hat{h}(u(P)),$$

so by (12):

$$\hat{h}(P^{\perp}) = \frac{\hat{h}(u(P))}{\|u\|^{2}}.$$

Recall inequality (11), which gives:

$$\mu_2(H+P) \leq \hat{\mu}(H+P) + NC(E).$$

By [28], we know that:

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

and, therefore, by Zhang's inequality:

$$\begin{aligned} h_2(H+P) &\leq N(\deg H)\mu_2(H+P) \leq \\ &\leq N(\deg H)(\hat{\mu}(H+P) + NC(E)) = \\ &= N(\deg H)(\hat{h}(P^{\perp}) + NC(E)) = \\ &= N(\deg H)\left(\frac{\hat{h}(u(P))}{\|u\|^{2}} + NC(E)\right). \end{aligned} \tag{13}$$

By (7), we get:

$$\deg H \leq 3^{N-1}(N-1)!\,\|u\|^{2},$$

so (13) becomes:

$$h_2(H+P) \leq 3^{N-1}N!\left(\hat{h}(u(P)) + NC(E)\,\|u\|^{2}\right). \quad \square$$

4.2. Geometry of Numbers

In this section, the geometry of numbers plays a central role. It is thanks to Minkowski's first and second Theorems that one can prove the existence of an auxiliary translate passing through our starting point P of rank $N-1$, so that both its degree and height are "small". As usual in diophantine approximation, "small" means depending on some parameters. At the end, we will show that a good choice of the parameters gives the desired bound on the height of P.

A central result in our approach is Lemma 7.5 of [18], which, in turn, is a consequence of [29], Lemma 3. This is a typical application of the second Minkowski Theorem to the lattice given by the group Γ_P generated by the coordinates of the point P. Similar results have been introduced by Bombieri, Masser and Zannier in [15]. For clarity, we recall these results here.

Lemma 10. *Let Γ be a finitely generated subgroup of E of rank m over $\mathbb{Z}$. Then, there are elements $g_1, \ldots, g_m \in \Gamma$ that generate a subgroup isomorphic to $\Gamma/\mathrm{Tor}(\Gamma)$ and such that:*

$$\hat{h}\left(\sum a_i g_i\right) \geq c(m)\left(\sum |a_i|^{2}\hat{h}(g_i)\right),$$

with $a_i \in \mathbb{Z}$ and $c(m) = 2^{2m-2}/m^2(m!)^4$.

Proof. From [30] Proposition 9.6, we know that the height function $\hat{h}$ extends on $\Gamma_{\mathbb{R}} := \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ to the square of a norm. In particular there is an inner product $\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ and $||P||^2 = 2\hat{h}(P)$. The group $\Gamma/\mathrm{Tor}(\Gamma)$ is a lattice in $\Gamma_{\mathbb{R}}$. Let $\tilde{p}_1, \dots, \tilde{p}_m$ be liftings on Γ of integral generators $p_1, \dots, p_m$ of $\Gamma/\mathrm{Tor}(\Gamma)$. We identify $\mathbb{R}^m$ and $\Gamma_{\mathbb{R}}$ via the isomorphism defined by the choice of the basis $p_1, \dots, p_m$. Let $V := \mathrm{vol}(p_1, \dots p_m)$ be the volume of a fundamental domain of $\Gamma/\mathrm{Tor}(\Gamma)$. Let $B := \{x \in \mathbb{R}^m : ||x|| \le 1\}$ be the closed ball of radius 1. Let $\lambda_1, \dots \lambda_m$ be the successive minima of B with respect to the lattice $\Gamma/\mathrm{Tor}(\Gamma)$. By Minkowski's second fundamental Theorem, we have:

$$\lambda_1, \dots \lambda_m \mathrm{vol}(B) \le 2^m V. \tag{14}$$

A Theorem of Mahler, [31] §V, Lemma 8, shows that there is a basis $v_1, \dots, v_m$ of $\Gamma/\mathrm{Tor}(\Gamma)$ such that:

$$\lambda_i \le ||v_i|| \le \max(1, i/2)\lambda_i. \tag{15}$$

Let $v_i = \sum_{j=1}^m v_{ij} p_i = (v_{i1}, \dots, v_{im})$. Since $v_1, \dots, v_m$ is a basis, we have:

$$|\det(v_1, \dots, v_m)| = V. \tag{16}$$

We write:

$$w_i = \frac{v_i}{||v_i||} \tag{17}$$

and we define B^* to be:

$$B^* = \{y \in \mathbb{R}^m : ||y_1 w_1 + y_2 w_2 + \dots + y_m w_m|| \le 1\}, \tag{18}$$

where $y = y_1 p_1 + y_2 p_2 + \dots + y_m p_m$. Since B is the image of B^* by the linear map $y = y_1 p_1 + y_2 p_2 + \dots + y_m p_m \mapsto y_1 w_1 + y_2 w_2 + \dots + y_m w_m$, we have, by (14)–(17), the upper bound:

$$\mathrm{vol}(B^*) = \frac{\mathrm{vol}(B)}{|\det(w_1, w_2, \dots, w_m)|} = \frac{\mathrm{vol}(B)}{V} \prod_{i=1}^m ||v_i|| \le 2m!. \tag{19}$$

A lower bound is obtained as follows.

Let e_j, $j = 1, \dots, m$ be the standard basis in $\mathbb{R}^m$. Let y be a boundary point of B^*, then, for each i, the set B^* contains the convex closure of the points $\pm y$ and $\pm e_j$, $j = 1, \dots, i-1, i+1, \dots m$. This set is the union of 2^m simplices of volume $|y_i|/m!$. Therefore, we get the lower bound:

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

which, combined with (19), gives:

$$\sum_{i=1}^m |y_i| \le 2^{-m+1} m (m!)^2 \left|\left| \sum_{i=1}^m y_i w_i \right|\right|, \tag{20}$$

where the norm on the right is 1 because y is a boundary point of B^*. Now, from (17), we may rewrite (20) as:

$$\left|\left| \sum_{i=1}^m x_i v_i \right|\right| \ge c_0(m) \sum_{i=1}^m |x_i| \cdot ||v_i||, \tag{21}$$

where $x_i = y_i/||v_i||$ and $c_0(m) = 2^{m-1}/m(m!)^2$. Finally, we define generators g_i for a subgroup $\overline{\Gamma}$ of Γ isomorphic to $\Gamma/\mathrm{Tor}(\Gamma)$, by setting:

$$g_i = \sum_{j=1}^{m} v_{ij}\tilde{p}_j,$$

where $v_i = (v_{i1}, \ldots, v_{im})$ and $\tilde{p}_1, \ldots, \tilde{p}_m$ are liftings on Γ of the generators $p_1, \ldots, p_m$ of $\Gamma/\mathrm{Tor}(\Gamma)$. Thus, we have:

$$2\hat{h}(\sum_{i=1}^{m} a_i g_i) = ||a_i v_1 + \cdots + a_m v_m||^2.$$

Since $||v_i||^2 = 2\hat{h}(g_i)$, Lemma 10 follows from (21). □

We now apply this basic Lemma to our situation. We obtain:

Lemma 11. *Let $1 \leq m \leq N$ be integers and let $P = (P_1, \ldots, P_N) \in B \subseteq E^N$, where B is a torsion variety of dimension $\leq m$ and E is non CM.*

There exist linear forms $L_1, \ldots, L_m \in \mathbb{R}[X_1, \ldots, X_N]$ 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:

$$\hat{h}(t_1P_1 + \cdots + t_NP_N) \leq c_1(N, m) \max_{1\leq j\leq m} \{|L_j(\mathbf{t})|^2\}\hat{h}(P)$$

for all $\mathbf{t} = (t_1, \ldots, t_N) \in \mathbb{Z}^N$. The constant $c_1(N, m)$ is given by:

$$c_1(N, m) = \frac{m^3(m!)^4N}{4^{m-1}}.$$

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

By Lemma 10, there are elements $g_1, \ldots, g_m \in E$, and torsion points $\zeta_1, \ldots, \zeta_N \in E$, such that:

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

and:

$$\hat{h}(b_1g_1 + \cdots + b_mg_m) \geq \frac{2^{2m-2}}{m^2(m!)^4} \max_{1\leq i\leq m} \{|b_i|^2\hat{h}(g_i)\} \quad \forall \mathbf{b} \in \mathbb{Z}^m.$$

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

$$\tilde{L}_j = v_{1j}X_1 + \cdots + v_{Nj}X_N, \qquad j = 1, \ldots, m,$$
$$L_j = \left(\frac{\hat{h}(g_j)}{NA}\right)^{\frac{1}{2}} \tilde{L}_j, \qquad j = 1, \ldots, m.$$

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:

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

where ξ is a torsion point. Therefore:

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

$$= NA\sum_{j=1}^{m} |L_j(\mathbf{t})|^2 \leq mNA \max_{1\leq j\leq m} \{|L_j(\mathbf{t})|^2\}. \tag{22}$$

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

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

We conclude combining this with inequality (22). □

We now extend the use of Minkowski's first Theorem as done in [20] for the case of dimension 2 to the case of dimension N.

Lemma 12. *Let $L_i \in \mathbb{R}[X_1, \ldots, X_N], i = 1, \ldots, N-1$ be $N-1$ independent linear form and let $\kappa \geq 2^{\frac{1}{N-1}}$ and $T \geq 4$. Then, there exists $u \in \mathbb{Z}^N \setminus \{0\}$ such that:*

$$||u||^2 \leq T^2,$$
$$|L_i(u)| \leq \frac{\kappa}{T^{\frac{1}{N-1}}}\,||L_i||\,,$$

where $||u||$ denotes the Euclidean norm of u, $||L||$ the Euclidean norm of the vector of the coefficients of L and $|L(u)|$ is the absolute value of $L(u)$.

Proof. Let $\mathcal{S}_T \subseteq \mathbb{R}^N$ be the set of points $(x_1, \ldots, x_N)$ satisfying the inequalities:

$$x_1^2 + \cdots + x_N^2 \leq T^2,$$
$$|L_i(x_1 \ldots, x_N)| \leq \kappa||L_i||/T^{\frac{1}{N-1}}.$$

Geometrically, $\mathcal{S}_T$ is the intersection between a ball and the $N-1$ "slices" determined by the $\kappa/T^{\frac{1}{N-1}}$-neighbourhoods of the hyperplanes defined by the L_i. We shall show that $\mathcal{S}_T \cap \mathbb{Z}^N \neq \{0\}$. $\mathcal{S}_T$ is clearly convex and symmetric with respect to the origin, so by Minkowski's Convex Body Theorem if the set $\mathcal{S}_T$ has a volume bigger than 2^N, then the intersection $\mathcal{S}_T \cap \mathbb{Z}^N$ contains points other than the origin.

The volume of $\mathcal{S}_T$ is lower bounded by the volume of 2^N hyperprismas with $N-1$ sides of length $\kappa/T^{1/N-1}$ and one of length $T\sin\theta$, where $\cos\theta = \kappa/T^{1/N-1}$ Therefore, for $T \geq 2\kappa^{N-1}$, the whole volume can be bounded from below as:

$$2^{N-1}\kappa^{N-1},$$

and the hypothesis of Minkowski's theorem are satisfied as soon as $\kappa \geq 2^{\frac{1}{N-1}}$. □

4.3. Bounds for the Auxiliary Translate

We can now sum up all our Lemmas to construct the auxiliary translate and prove the central proposition of this section. This will play a crucial role in the proof of our main theorem.

Proposition 13. *Let E be an elliptic curve without CM. Let $P = (P_1, \ldots, P_N) \in B \subset E^N$, where B is a torsion variety of dimension $N-1$. Let $T \geq 2^4, \kappa \geq 2^{\frac{2}{N-1}}$ be real numbers.*

Then, there exists an abelian subvariety $H \subset E^N$ of codimension 1 such that:

$$\begin{aligned}\deg(H+P) &\leq 3^{N-1}(N-1)!T,\\ h_2(H+P) &\leq c_2(N)\frac{\kappa}{T^{\frac{1}{N-1}}}\hat{h}(P)+c_3(N,E)T,\end{aligned}$$

where:

$$\begin{aligned}c_2(N) &= \frac{3^{N-1}N^2(N-1)^3(N-1)!^5}{4^{N-2}},\\ c_3(N,E) &= N3^{N-1}(N-1)!C(E),\end{aligned}$$

and $C(E)$ is defined in Proposition 6.

Proof. Let $L_1,\dots,L_{N-1}$ be the linear forms obtained from Lemma 11 with $m=N-1$. Then, for all j, we have:

$$||L_j|| \leq 1$$

and for all $\mathbf{t}=(t_1,\dots,t_N)\in\mathbb{Z}^N$, we have:

$$\hat{h}(t_1P_1+\cdots+t_NP_N) \leq \frac{(N-1)^3(N-1)!^4N}{4^{N-2}}\max_j\{|L_j(\mathbf{t})|^2\}\hat{h}(P). \tag{23}$$

Apply Lemma 12 with the just constructed L_i and κ and T equal to the square roots of the κ and T in the statement. Let $u=(\alpha_1,\dots,\alpha_N)\in\mathbb{Z}^N$ be the vector obtained from Lemma 12. Then:

$$\begin{aligned}&||u||^2 \leq T,\\ &|L_i(u)| \leq \frac{\kappa^{1/2}}{T^{\frac{1}{2N-2}}}\,\|L_i\| \leq \frac{\kappa^{1/2}}{T^{\frac{1}{2N-2}}},\end{aligned}$$

where the last bound is due to the fact that the L_j have norm at most 1. Therefore, the relation (23) implies:

$$\hat{h}(u(P)) \leq \frac{(N-1)^3(N-1)!^4N}{4^{N-2}}\frac{\kappa}{T^{\frac{1}{N-1}}}\hat{h}(P). \tag{24}$$

Let H the zero component of the algebraic subgroup defined by the equation $\alpha_1X_1+\cdots+\alpha_NX_N=O$. The thesis follows from Proposition 9 and the above estimate. □

5. The Proof of the Main Theorem 2

We can now proceed to the proof of our main theorem and compute all the constants. For simplicity, we recall the statement here.

Theorem 14. *Let E be an elliptic curve without CM. Let $\mathcal{C}$ be a curve transverse in E^N. Then, all the points P of rank at most $N-1$ on $\mathcal{C}$ have Néron–Tate height bounded as:*

$$\hat{h}(P) \leq C_1\cdot h_2(\mathcal{C})(\deg\mathcal{C})^{N-1}+C_2(E)(\deg\mathcal{C})^N+NC(E),$$

where:

$$\begin{aligned}C_1 &= 2^{N+2}3^{N-1}(N-1)!c_2(N)^{N-1},\\ C_2(E) &= 2^{N+2}3^{N-1}(N-1)!\,(NC(E)+C_0)\,c_2(N)^{N-1},\\ c_2(N) &= \frac{3^{N-1}N^2(N-1)^3(N-1)!^5}{4^{N-2}},\end{aligned}$$

and $C(E)$ is defined in Proposition 6 and $C_0=C_0(1,N-1,3^N-1)$ is defined in (8).

Proof. If P has rank zero, then its height is zero and the statement is true.

Let $T \geq 2^4, \kappa \geq 2^{2/N-1}$ be real numbers. We apply Proposition 13 to the point P of rank $\leq N-1$. Thus, we obtain a abelian variety H of codimension 1 in E^N with:

$$\begin{aligned} \deg(H+P) \leq& 3^{N-1}(N-1)!T \quad \text{, and} \\ h_2(H+P) \leq& c_2(N)\frac{\kappa}{T^{\frac{1}{N-1}}}\hat{h}(P) + c_3(N,E)T, \end{aligned} \tag{25}$$

where:

$$c_2(N) = \frac{3^{N-1}N^2(N-1)^3(N-1)!^5}{4^{N-2}},$$

$$c_3(N,E) = N3^{N-1}(N-1)!C(E),$$

and $C(E)$ is defined in Proposition 6.

We now want to bound $\hat{h}(P)$ in terms of $\deg(H+P)$ and $h_2(H+P)$.

Notice that the point P is a component of the intersection $\mathcal{C} \cap (H+P)$ because, otherwise, $\mathcal{C} \subseteq H+P$, contradicting the fact that $\mathcal{C}$ is transverse. We apply the Arithmetic Bézout Theorem 7 to the intersection $\mathcal{C} \cap (H+P)$ in $\mathbb{P}_{3^N-1}$, obtaining:

$$h_2(P) \leq h_2(\mathcal{C}) \deg H + h_2(H+P) \deg \mathcal{C} + C_0(1, N-1, 3^N-1) \deg H \deg \mathcal{C}.$$

By Proposition 6, we have $\hat{h}(P) \leq h_2(P) + 2C(E)$ so, using the bounds in formula (25), we get:

$$\hat{h}(P) \leq c_5 \frac{\kappa}{T^{\frac{1}{N-1}}}\hat{h}(P) + c_6 T + c_7 \tag{26}$$

with:

$$\begin{aligned} c_5(\mathcal{C}) &= c_2(N) \deg \mathcal{C}, \\ c_6(\mathcal{C}, E) &= 3^{N-1}(N-1)!h_2(\mathcal{C}) + c_3(N,E) \deg \mathcal{C} + C_0 3^{N-1}(N-1)! \deg \mathcal{C}, \\ c_7(\mathcal{C}, E) &= NC(E). \end{aligned}$$

We set:

$$T = (2c_5\kappa)^{N-1} \text{ and } \kappa = 2^{\frac{2}{N-1}},$$

so that the conditions on T, κ are largely satisfied. Moreover, the choice of T is done to make the coefficient of $\hat{h}(P)$ on the right-hand side of (26) equal to $1/2$. Thus, we can bring it to the left-hand side and express $\hat{h}(P)$ in terms of the rest. After simplification, (26) becomes:

$$\hat{h}(P) \leq 2^{N+2}c_5^{N-1}c_6\kappa + 2c_7, \tag{27}$$

which gives the bound in the theorem. □

Conflicts of Interest: The author declares no conflict of interest.

References

1. Mordell, L.J. On the rational solutions of the indeterminate equation of the third and fourth degrees. *Proc. Camb. Philos. Soc.* **1922**, *21*, 179–192.
2. Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **1983**, *73*, 349–366.
3. Vojta, P. Siegel's theorem in the compact case. *Ann. Math.* **1991**, *133*, 509–548.
4. Faltings, G. Diophantine approximation on abelian varieties. *Ann. Math.* **1991**, *133*, 549–576.
5. Faltings, G. The general case of S. Lang's conjecture. In *Barsotti Symposium in Algebraic Geometry*; Academic Press: San Diego, CA, USA, 1994; pp. 175–182.

6. Hindry, M. Autour d'une conjecture de Serge Lang. *Invent. Math.* **1988**, *94*, 575–603.
7. Chabauty, C. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci. Paris* **1941**, *212*, 882–885.
8. Coleman, R.F. Effective Chabauty. *Duke Math. J.* **1985**, *52*, 765–780.
9. Dem'janenko, V. Rational points on a class of algebraic curves. *Am. Math. Soc. Transl.* **1968**, *66*, 246–272.
10. Manin, J. The p-torsion of elliptic curves is uniformly bounded. *Am. Math. Soc. Transl.* **1969**, *33*, 433–438.
11. Serre, J.P. *Lectures on the Mordell-Weil Theorem*; Aspects of Mathematics, E15, Friedr; Vieweg & Sohn: Braunschweig, Germany, 1989.
12. Flynn, E.V. A flexible method for applying Chabauty's theorem. *Compos. Math.* **1997**, *105*, 79–94.
13. Kulesz, L. Application de la méthode de Dem′janenko-Manin à certaines familles de courbes de genre 2 et 3. *J. Number Theory* **1999**, *76*, 130–146.
14. Kulesz, L.; Matera, G.; Schost, E. Uniform bounds for the number of rational points of families of curves of genus 2. *J. Number Theory* **2004**, *108*, 241–267.
15. Bombieri, E.; Masser, D.; Zannier, U. Intersecting a Curve with Algebraic Subgroups of Multiplicative Groups. *Int. Math. Res. Not.* **1999**, *20*, 1119–1140.
16. Zannier, U. *Some Problems of Unlikely Intersections in Arithmetic and Geometry (with Appendixes by D. Masser)*; Princeton University Press: Princeton, NJ, USA, 2012; p. 181.
17. Viada, E. Explicit height bounds and the effective Mordell–Lang Conjecture. In Proceedings of the "Third Italian Number Theory Meeting", Pisa, Italy, 21–24 September 2015.
18. Checcoli, S.; Veneziano, F.; Viada, E. On the explicit Torsion Anomalous Conjecture. *Trans. AMS* **2016**, *369*, 6465–6491.
19. Viada, E. An explicit Manin-Dem'janenko Theorem in Elliptic Curves. *arXiv* **2016**, arXiv:1609.04615. Available online: https://arxiv.org/abs/1609.04615 (accessed on 5 July 2017).
20. Checcoli, S.; Veneziano, F.; Viada, E. The explicit Mordell Conjecture for families of curves. *arXiv* **2016**, arXiv:1602.04097. Available online: https://arxiv.org/abs/1602.04097 (accessed on 5 July 2017).
21. Philippon, P. Sur des hauteurs alternatives. III. *J. Math. Pures Appl.* **1995**, *74*, 345–365.
22. Cremona, J.E. Elliptic Curve Data, 2015. Available online: http://johncremona.github.io/ecdata/ (accessed on 5 July 2017).
23. Bombieri, E.; Gubler, W. *Heights in Diophantine Geometry*; Cambridge University Press: Cambridge, UK, 2006.
24. Philippon, P. Sur des hauteurs alternatives. I. *Math. Ann.* **1991**, *289*, 255–284.
25. Silverman, J.H. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.* **1990**, *55*, 723–743.
26. Bost, J.-B.; Gillet, H.; Soulé, C. Heights of projective varieties and positive Green forms. *J. Am. Math. Soc.* **1994**, *7*, 903–1027.
27. Zhang, S. Positive line bundles on arithmetic varieties. *J. Am. Math. Soc.* **1995**, *8*, 159–165.
28. Philippon, P. Sur une Question D'orthogonalité dans les Puissances de Courbes Elliptiques. **2012**, hal-00801376. Available online: https://hal.archives-ouvertes.fr/hal-00801376 (accessed on 5 July 2017).
29. Viada, E. The intersection of a curve with algebraic subgroups in a product of elliptic curves. *Ann. Sc. Norm. Super. Pisa Cl. Sci.* **2003**, *2*, 47–75.
30. Silverman, J.H. *The Arithmetic of Elliptic Curves*; Graduate Texts in Mathematics; Springer: New York, NY, USA, 1986; Volume 106.
31. Cassels, J.W.S. *An Introduction to the Geometry of Numbers*; Springer: New York, NY, USA, 1971.