Forum of Mathematics, Sigma (2019), Vol. 7, e31, 62 pages
doi:10.1017/fms.2019.20

THE EXPLICIT MORDELL CONJECTURE FOR FAMILIES OF CURVES

SARA CHECCOLI[1], FRANCESCO VENEZIANO[2] and EVELINA VIADA[3]

[1] Institut Fourier, 100 rue des Maths, BP74 38402 Saint-Martin-d'Hères Cedex, France;
email: sara.checcoli@univ-grenoble-alpes.fr

[2] Collegio Puteano, Scuola Normale Superiore, Piazza dei Cavalieri, 3, I-56100 Pisa, Italy;
email: francesco.veneziano@sns.it

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

Received 22 October 2017; accepted 29 June 2019

(with an appendix by M. Stoll)

Abstract

In this article we prove the explicit Mordell Conjecture for large families of curves. In addition, we introduce a method, of easy application, to compute all rational points on curves of quite general shape and increasing genus. The method bases on some explicit and sharp estimates for the height of such rational points, and the bounds are small enough to successfully implement a computer search. As an evidence of the simplicity of its application, we present a variety of explicit examples and explain how to produce many others. In the appendix our method is compared in detail to the classical method of Manin–Demjanenko and the analysis of our explicit examples is carried to conclusion.

2010 Mathematics Subject Classification: 11G50 (primary); 14G40 (secondary)

1. Introduction

The Diophantine problem of finding integral or rational solutions to a set of polynomial equations has been investigated since ancient times. To this day there is no general method for finding such solutions and the techniques used to answer many fundamental questions are deep and complex. One of the leading principles

in arithmetic geometry is that the geometric structure of an algebraic variety determines the arithmetic structure of the set of points over the rational numbers. By *variety*, here and in the rest of the paper, we mean a closed algebraic variety defined over the algebraic numbers $\overline{\mathbb{Q}}$, and by *curve* a variety of dimension one. We identify a variety V with the set of its algebraic points $V(\overline{\mathbb{Q}})$.

A clear picture of how the arithmetic mirrors the geometry for varieties is given by irreducible curves defined over a number field k. For singular curves, we define the *genus* as the genus of the normalization. The genus of a curve is a geometric invariant, and it distinguishes three qualitatively different behaviours for the set of rational points. For a curve of genus 0, either the set of k-rational point 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 at least 2 we have the:

MORDELL CONJECTURE. *An irreducible algebraic 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 [30] and now known as Faltings Theorem after the ground-breaking proof in [14]. In between these two extremes, there are the curves of genus 1. They 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 generalized by Weil to the case of abelian varieties.

Vojta in [47] gave a new proof of the Mordell Conjecture and then Faltings, in [15, 16], proved an analogous statement for rational points on subvarieties of abelian varieties, which generalizes to points in a finitely generated subgroup Γ. Building on these results, Hindry [21] proved the case of Γ of finite rank, known as the Mordell–Lang Conjecture. This was later made quantitative by Rémond [35].

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. The few available

methods work under special assumptions and explicit examples are mainly given for curves of genus 2 or 3 as discussed below.

The method of Chabauty and Coleman [8, 10] provides a bound on the number of rational points on curves defined over a number field k with Jacobian of k-rank strictly smaller than the genus. In some examples the estimate gives the exact number of rational points. When this happens, possibly in combination with *ad hoc* descent arguments, one can manage to find them explicitly. See for example Flynn [17] for one of the first explicit applications of the Chabauty–Coleman method, Siksek [37] for investigations on possible extensions of the method, McCallum and Poonen [29] and Stoll [42] for general surveys and also their references for additional variations and applications of this method. For curves of genus 2, one can find the rational points using an implementation by Stoll based on [7, Section 4.4] of the Chabauty–Coleman method combined with the Mordell–Weil Sieve in the Magma computational algebra system [4]; this works when the Mordell–Weil rank of the Jacobian is one and an explicit point of infinite order is known.

The Manin–Demjanenko method [13, 26] is effective and applies to curves $\mathcal{C}$ defined over a number field k that admit m morphisms $f_1, \dots, f_m$ from $\mathcal{C}$ to an abelian variety A all defined over k and linearly independent modulo constants (in the sense that if $\sum_{i=1}^{m} n_i f_i$ is constant for some integers n_i, then $n_i = 0$ for all i). If $m > \operatorname{rank} A(k)$, then $\mathcal{C}(k)$ is finite and may be found effectively. However the method is far from being explicit in the sense that it does not give the dependence of the height of the rational points, neither on the curve nor on the morphisms; this makes it difficult for applications. See Serre [36] for a description of the method and a few applications. In the papers of Kulesz [24], Girard and Kulesz [19] and Kulesz *et al.* [25] this method has been used to find all rational points on some families of curves of genus 2 (respectively 3) with morphisms to special elliptic curves of rank 1 (respectively $\leqslant 2$). For instance, in [24] the curves have Jacobian with factors isogenous to $y^2 = x^3 + a^2 x$, with a a square-free integer and such that the Mordell–Weil group has rank one. We refer to Section A.1 of the appendix for a more detailed discussion on the Manin–Demjanenko method, including a comparison with the results of this article.

We also mention that Viada gave in [45] an effective method which is comparable with the setting of Manin–Demjanenko's result, although different in strategy. She obtains an effective height bound for the k-rational points on a transverse curve $\mathcal{C} \subseteq E^N$, where E is an elliptic curve with k-rank at most $N - 1$. Also in this case the bounds are not at all explicit and there are no examples.

A major shortcoming of these methods is that in general the bounds for the height must be worked out case by case and this is feasible in practice only when the equations of the curve are of a very special shape.

In this article we provide a good explicit upper bound for the height of the points in the intersection of a curve of genus at least 2 in E^N with the union of all algebraic subgroups of dimension one, where E is an elliptic curve without CM (Complex Multiplication), proving explicitly a particular case of the Mordell–Lang conjecture in an elliptic setting. With some further technical estimates, the method works also for the CM case. Our method can be easily applied to find the rational points on curves of a fairly general shape and growing genus. Moreover we present a variety of explicit examples, given by curves of genus at least 2 embedded in E^2, with E without CM and $E(k)$ of rank one. These are precisely the curves whose Jacobian has a factor isogenous to such an E^2. So the method can be easily applied to curves embedded in $E^2 \times A$, where A is an abelian variety. This is also the first nontrivial setting, as the case of $E(k)$ of rank zero can be easily treated (see Theorem 4.4 and Remark 4.5). Many explicit examples mentioned above can be covered by our method, but it also gives many new examples in which, differently from all previous examples, the genus of the curves tends to infinity (see also Appendix A, in particular Section A.4).

Compared to the other effective methods mentioned above, ours is easy to apply because it provides a simple formula for the bound for the height of the rational points. Finally, in our settings the method of Chabauty–Coleman cannot be directly applied, as the rank of the k-rational points of the ambient variety is not smaller than its dimension. Our assumption is instead compatible with the Manin–Demjanenko setting.

The importance of the result is that the dependence of our bound for the height is completely explicit both on the curve $\mathcal{C}$ and the elliptic curve E and it can be directly computed from the coefficients of the equations defining the curve. More precisely, it depends explicitly on the coefficients of a Weierstrass equation for E and on the degree and normalized height of $\mathcal{C}$.

To give some evidence of the power of our method we carry out in this paper the following applications:

- the proof of the explicit Mordell Conjecture for several families of curves;
- the list of all rational points for more than 10^4 explicit curves.

To state our main theorem, we first fix the setting (see Section 2 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 normalized height of $\mathcal{C}$, which is defined in terms of the Chow form of the ideal of $\mathcal{C}$, as done in [**33**, Section 2, page 346]. We let $\hat{h}$ be the Néron–Tate height on E^N (normalized as explained in Section 2.1).

We finally define the rank for a point of E^N as the $\mathrm{End}(E)$-rank of the ring generated by its coordinates or more in general:

DEFINITION 1.1. Let A be an abelian variety that is a projective variety with a (fixed) group structure. The rank of a point of A is the minimal dimension of an algebraic subgroup containing the point.

In particular, the points of rank 0 in A are precisely the torsion points. See also later the related Definition 4.1.

We can now state our main result:

THEOREM 1.2. *Let E be an elliptic curve without CM defined over a number field. Let $\mathcal{C}$ be an irreducible curve of genus at least 2 embedded in E^N. Then every point $P \in \mathcal{C}(\overline{\mathbb{Q}})$ of rank at most one has Néron–Tate height bounded as*

$$\hat{h}(P) \leqslant \gamma_1 \cdot h_2(\mathcal{C})(\deg \mathcal{C})^2 + \gamma_2(E)(\deg \mathcal{C})^3$$

where

$$\gamma_1 = 17 \cdot 3^N \cdot N!$$
$$\gamma_2(E) = 10 \cdot 3^{2N} \cdot N! \cdot c_1(E).$$

Moreover if $N = 2$

$$\hat{h}(P) \leqslant C_1 \cdot h_2(\mathcal{C}) \deg \mathcal{C} + C_2(E)(\deg \mathcal{C})^2 + C_3(E)$$

where

$$C_1 = 72.251$$
$$C_2(E) = C_1(6.019 + 4c_1(E))$$
$$C_3(E) = 4c_2(E),$$

and the constants $c_1(E)$ and $c_2(E)$ are defined in Table 1 and depend explicitly on the coefficients of E.

The case $N = 2$ of Theorem 1.2 is treated in Theorem 4.2, proved in Section 5, while the bound for $N \geqslant 3$ is a simplified form of that given in Theorem 4.3, proved in Section 4.

We remark that if $E(k)$ has rank one then the set of k-rational points of $\mathcal{C}$ is contained in the set of points of rank one and so it has height bounded as above. We underline that our method to bound the height of the rational points does not require the knowledge of a generator for $E(k)$ to work and that the bound we obtain is also independent on k. These aspects are rather important, specifically for applications.

Our search for effective and even explicit methods for the height of the k-rational points on curves started some years ago in the context of the Torsion Anomalous Conjecture (TAC), introduced by Bombieri *et al.* [3]. It is well known that this very general conjecture on the finiteness of the maximal torsion anomalous varieties implies the Mordell–Lang Conjecture and that effective results in the context of the TAC carry over to effective cases of the Mordell–Lang Conjecture (see [46] for a survey). Several of the methods used in this field are based on a long-established strategy of using theorems of diophantine approximation to obtain results about the solutions to diophantine equations. This general approach goes back at least to Thue and Siegel and has been often applied with success in the field of unlikely intersections as well as in number theory in general (see [48] and references there for a nice overview). Despite much effort there are few effective methods in this context and ours is probably the first explicit one in the setting of abelian varieties.

Our main theorem generalizes and drastically improves a previous result obtained in [9] where we considered only weak-transverse curves, that is curves not contained in any proper algebraic subgroup (see Definition 4.1), a stronger assumption which does not cover all curves of genus $\geqslant 2$ and we could only bound the height of the subset of points of rank one which are also torsion anomalous. From [9, Theorem 1.3] it is possible to deduce by a geometric argument a general result for all curves of genus $\geqslant 2$, but the numerical constants would not be explicit and the exponents in the degrees would be higher than necessary. Even in the weak-transverse case, in spite of the more restrictive setting, the bounds obtained in [9] are much worse than the present ones, both in the numerical constants and in the exponents, and they are beyond any hope of being implemented in any concrete case.

For instance, in this article, Theorem 4.3, for weak-transverse curves in E^N with $N \geqslant 3$ we obtain

$$\hat{h}(P) \leqslant 4(N-1)C_1 h_2(\mathcal{C}) \deg \mathcal{C} + (N-1)C_2(E)(\deg \mathcal{C})^2 + N^2 C_3(E),$$

while in [9] under the same hypothesis we got

$$\begin{aligned}\hat{h}(P) \leqslant\ & B_1(N) \cdot 2(N-1)C_1 h_2(\mathcal{C})(\deg \mathcal{C})^{N-1} \\ & + B_2(N) \cdot (N-1)C_2(E)(\deg \mathcal{C})^N + N^2 C_3(E)\end{aligned}$$

where $B_2(N) \geqslant B_1(N) \geqslant 10^{27} N^{N^2} (N!)^N$. Note that not only the constants here are linear instead of exponential in N, but also the exponents of $\deg \mathcal{C}$ are now independent of N and better already for $N = 3$.

By introducing new key elements in the proof, we go beyond what we could prove in [9]; this change in approach leads to improvements of the bounds crucial for the practical implementation.

In more details, this is a sketch of the proof of the main theorem given in Sections 4 and 5. At first instance we avoid to restrict ourselves to the concept of torsion anomalous points as done in [9] and study all points of rank one. To treat the case of a general N we use a geometric construction to reduce it to the case of $N = 2$. In this case we do a typical proof of diophantine approximation: if P is a point in E^2 of rank one, we construct a subgroup H of dimension 1 such that the height and the degree of the translate $H + P$ are well controlled. To this aim we use some classical results of the geometry of numbers, in a way that prevents the bounds from growing beyond the computational limits of a computer search. We then conclude the proof using the Arithmetic Bézout Theorem, Zhang's inequality and an optimal choice of the parameters.

Another significant feature of our main theorem is that it can easily be applied to find the rational points on curves of quite general shape. We present here some of these applications, remarking that, for instance, any curve of genus at least 2 in E^2 with $E(\mathbb{Q})$ of rank one is suitable for further examples of our method.

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

$$\begin{aligned} y_1^2 &= x_1^3 + Ax_1 + B \\ y_2^2 &= x_2^3 + Ax_2 + B \end{aligned} \tag{1.1}$$

for the equations of E^2 in $\mathbb{P}_2^2$ using affine coordinates $(x_1, y_1) \times (x_2, y_2)$ and we embed E^2 in $\mathbb{P}_8$ via the Segre embedding.

In Section 6 we give a method to construct several families of irreducible curves in E^2 of growing genus and we show how to compute bounds for their degree and normalized height. In Theorem 6.3 we prove a sharper version of the following result.

THEOREM 1.3. *Assume that E is without CM, defined over a number field k and that $E(k)$ has rank one. Let $\mathcal{C}$ be the projective closure of the curve given in E^2 by the additional equation*

$$p(x_1) = y_2,$$

with $p(X) \in k[X]$ a nonconstant polynomial of degree n. Then $\mathcal{C}$ is irreducible and for $P \in \mathcal{C}(k)$ we have

$$\hat{h}(P) \leqslant 1301(2n+3)^2(h_W(p) + \log n + 2c_6(E) + 3.01 + 2c_1(E)) + 4c_2(E)$$

where $h_W(p) = h_W(1 : p_0 : \ldots : p_n)$ is the height of the coefficients of $p(X)$, and the constants $c_6(E)$, $c_1(E)$ and $c_2(E)$ are defined in Table 1.

We then consider two specific families which have particularly small invariants. Clearly these are just examples and many similar others can be given.

DEFINITION 1.4. Let $\{\mathcal{C}_n\}_n$ be the family of the projective closures of the curves in E^2 defined for $n \geqslant 1$ via the additional equation

$$x_1^n = y_2.$$

Let $\{\mathcal{D}_n\}_n$ be the family of the projective closures of the curves in E^2 defined for $n \geqslant 1$ via the additional equation

$$\Phi_n(x_1) = y_2,$$

where $\Phi_n(x)$ is the nth cyclotomic polynomial.

In order to directly apply our main theorem we cut these curves on E^2, with E varying in the set of elliptic curves over $\mathbb{Q}$ without CM and $\mathbb{Q}$-rank one. Several examples of such E have been tabulated below and others can be easily found, for instance in Cremona's tables [**11**].

We consider the following elliptic curves:

$$\begin{aligned}
E_1 &: y^2 = x^3 + x - 1,\\
E_2 &: y^2 = x^3 - 26811x - 7320618,\\
E_3 &: y^2 = x^3 - 675243x - 213578586,\\
E_4 &: y^2 = x^3 - 110038419x + 12067837188462,\\
E_5 &: y^2 = x^3 - 2581990371x - 50433763600098.
\end{aligned}$$

These are five elliptic curves without CM and of rank one over $\mathbb{Q}$. The curves E_1, E_3, E_4, E_5 are, respectively, the curves 248c.1,10014b.1, 360009g.1 and 360006h.2 of [**11**]. The curve E_2 was considered by Silverman in [**41**, Example 3] and it does not appear in the Cremona tables because its conductor is too big. The curves E_3, E_4 and E_5 were chosen because they have generators of the Mordell–Weil group of large height. This choice may speed up the computations, but it is not necessary (see Section 9 for more details)

A remarkable application of our theorem is the following result, proven in Section 9. If E is an elliptic curve, we denote by O its neutral element.

THEOREM 1.5. *For the* 79600 *curves* $\mathcal{C}_n \subseteq E_i \times E_i$ *with* $1 \leqslant n \leqslant 19900$ *and* $i = 2, 3, 4, 5$, *we have*

$$\mathcal{C}_n(\mathbb{Q}) = \{O \times O\}.$$

For the 9900 *curves* $\mathcal{C}_n \subseteq E_1 \times E_1$ *with* $1 \leqslant n \leqslant 9900$, *we have*

$$\mathcal{C}_n(\mathbb{Q}) = \{O \times O, (1, \pm 1) \times (1, 1)\}.$$

For the 5600 *curves* $\mathcal{D}_n \subseteq E_i \times E_i$ *where* $1 \leqslant n \leqslant 1400$ *and* $i = 2, 3, 4, 5$ *we have*

$$\mathcal{D}_n(\mathbb{Q}) = \{O \times O\}.$$

For the 400 *curves* $\mathcal{D}_n \subseteq E_1 \times E_1$ *with* $1 \leqslant n \leqslant 400$ *we have*

$$\begin{aligned}
\mathcal{D}_1(\mathbb{Q}) &= \{O \times O, (2, \pm 3) \times (1, 1)\} \\
\mathcal{D}_2(\mathbb{Q}) &= \{O \times O, (2, \pm 3) \times (2, 3)\} \\
\mathcal{D}_{3^k}(\mathbb{Q}) &= \{O \times O, (1, \pm 1) \times (2, 3)\} \\
\mathcal{D}_{47^k}(\mathbb{Q}) &= \{O \times O, (1, \pm 1) \times (13, 47)\} \\
\mathcal{D}_{p^k}(\mathbb{Q}) &= \{O \times O\} \quad \text{if } p \neq 3, 47 \text{ or } p = 2 \text{ and } k > 1 \\
\mathcal{D}_6(\mathbb{Q}) &= \{O \times O, (1, \pm 1) \times (1, 1), (2, \pm 3) \times (2, 3)\} \\
\mathcal{D}_n(\mathbb{Q}) &= \{O \times O, (1, \pm 1) \times (1, 1)\} \\
&\qquad \text{if } n \neq 6 \text{ has at least two distinct prime factors.}
\end{aligned}$$

For these curves the bounds for the height of the rational points are very good especially for the $\mathcal{C}_n$; in fact they are so good that we can carry out a fast computer search and determine all their rational points for n quite large. The computations have been executed with the computer algebra system PARI/GP [**43**] using an algorithm by K. Belabas discussed in Section 9 based on a sieving method.

The computations for the 9900 curves $\mathcal{C}_n$ in E_1^2 took about 7 days. The 79600 curves $\mathcal{C}_n$ in E_i^2, $i = 2, \ldots, 5$ took about 11 days, while the computations on the 6000 curves $\mathcal{D}_n$ took about three weeks. A single curve in this range takes between a few seconds and a few minutes, for example $\mathcal{C}_{1000}$ in E_2^2 takes about 6.8 s.

In Appendix A M. Stoll completes the study of the rational points on the families $\mathcal{C}_n$ and $\mathcal{D}_n$ for all n. More precisely, he proves that for n large enough all rational points on the curves must be integral, by combining our upper bound for the height of the rational points with a lower bound obtained by studying the ℓ-adic behaviour of points on the curve close to the origin, see Sections A.3 and A.4. Thus our computations are required only for n small. However the data above give an idea of the time needed to find the rational points on other curves with

invariants similar to those considered in Theorem 1.5, even when the approach of the Appendix A does not apply.

For a few curves in which the bounds are particularly small, we first used a naive algorithm, which took about six weeks for each curve $\mathcal{C}_1$. Then we used a floating point algorithm suggested by J. Silverman: for each $i = 1, \dots, 5$ this algorithm took about one week for the 10 curves $\mathcal{C}_n \in E_i^2$ with $1 \leqslant n \leqslant 10$. The striking improvement in the running time is due to the idea of performing the computations after reducing modulo many primes; arithmetic operations in finite fields are much faster than exact arithmetic. More details on how to construct suitable new examples are given in Section 6.

The results of this article could be generalized in several ways. A possibility is to find rational points on new explicit examples of families of curves. One could also study curves in a product of abelian varieties or surfaces in a power of an elliptic curve. We intend to investigate in these directions. For instance, in [**44**] Viada applies the results obtained here to establish some generalizations.

The paper is organized as follows: Sections 2 and 3 contain the notations, definitions and some useful standard results. In Section 4 we state Theorem 4.2 which is a sharper version of our main result for curves in E^2. This is crucial for the applications and we use it to prove Theorem 1.2. Section 5 is dedicated to the proof of Theorem 4.2. Sections 6–9 are devoted to describe the families of examples and applications of our main method, proving in particular Theorems 1.3 and 1.5.

2. Notation and preliminaries

In this section we introduce the notations that we will use in the rest of the article. We define different heights and, among the main technical tools in the theory of height, we recall the Arithmetic Bézout Theorem and Zhang's inequality. We also recall some standard facts on subgroups of E^N and give some basic estimates for the degree of the kernel of morphisms on E^N.

2.1. Heights and degrees. In this article we deal only with varieties defined over the algebraic numbers. We will always identify a variety V with the set of its algebraic points $V(\overline{\mathbb{Q}})$. Throughout the article E will be an elliptic curve defined over the algebraic numbers and given by a fixed Weierstrass equation

$$E : y^2 = x^3 + Ax + B \tag{2.1}$$

with A and B algebraic integers (this assumption is not restrictive). If E is defined over a number field k we write in short E/k. As usual, we define the discriminant

of E as

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

(notice that $\Delta \neq 0$ because E is an elliptic curve) and the j-invariant

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

We also define

$$h_{\mathcal{W}}(E) = h_W(1 : A^{1/2} : B^{1/3}) \tag{2.2}$$

to be the absolute logarithmic Weil height of the projective point $(1 : A^{1/2} : B^{1/3})$. We recall that if k is a number field, $\mathcal{M}_k$ is the set of places of k and $P = (P_0 : \ldots : P_n) \in \mathbb{P}_n(k)$ 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 $[k_v : \mathbb{Q}_v]$ denotes, as usual, the local degree at v and the absolute values $|\cdot|_v$ are normalized in such a way that the product formula

$$\prod_{v \in \mathcal{M}_k} |x|_v^{[k_v:\mathbb{Q}_v]/[k:\mathbb{Q}]} = 1$$

holds for every nonzero element $x \in k$.

We also consider a modified version of the Weil height, differing from it at the Archimedean places

$$h_2(P) = \sum_{v \text{ finite}} \frac{[k_v : \mathbb{Q}_v]}{[k : \mathbb{Q}]} \log \max_i \{|P_i|_v\} + \sum_{v \text{ infinite}} \frac{[k_v : \mathbb{Q}_v]}{[k : \mathbb{Q}]} \log \left(\sum_i |P_i|_v^2 \right)^{1/2}. \tag{2.3}$$

If x is an algebraic number, we denote by $h_\infty(x)$ the contribution to the Weil height coming from the Archimedean places, more precisely

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

To compute heights and degrees of subvarieties of E^N, we consider them as embedded in $\mathbb{P}_{3^N-1}$ via the following composition of maps

$$E^N \hookrightarrow \mathbb{P}_2^N \hookrightarrow \mathbb{P}_{3^N-1}, \tag{2.4}$$

where the first map is, on each of the N factors, the embedding of E in $\mathbb{P}_2$ given by the Weierstrass form of E, while the second map is the Segre embedding.

For V a subvariety of E^N we consider the canonical height $h(V)$, as defined in [32, page 281]; when the variety V reduces to a point P, then $h(V) = \hat{h}(P)$ is the Néron–Tate height of the point (see [32, Proposition 9]) defined as

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h_W(2^n \cdot P)}{4^n}.$$

In general if $P = (P_1, \dots, P_N) \in E^N$, then we have

$$h(P) = \sum_{i=1}^{N} h(P_i) \tag{2.5}$$

for h equal to h_W, h_2 and $\hat{h}$ (see for instance [2, Proposition 2.4.4]).

For a subvariety $V \subseteq \mathbb{P}_m$ we denote by $h_2(V)$ the normalized height of V defined in terms of the Chow form of the ideal of V, as done in [33, Section 2, page 346]. This height extends the height h_2 defined for points by formula (2.3) (see [20, page 6] and [5, equation (3.1.6)]).

If V is defined as an irreducible component of the zero set in $\mathbb{P}_m$ of homogeneous polynomials $f_1, \dots, f_r$, then by the result at [33, page 347 and Proposition 4] and standard estimates, one can prove that

$$h(V) \leqslant \sum_{i=1}^{r} h_W(f_i) \prod_{j\neq i} \deg(f_j) + c \deg(f_1) \cdots \deg(f_r)$$

where $h_W(f_i)$ is the Weil height of the vector of coefficients of f_i, considered as a projective point and c is an explicit constant, which can be taken as $c = 4m \log m$.

The degree of an irreducible variety $V \subseteq \mathbb{P}_m$ 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; we show here how to do it for a curve $\mathcal{C} \subseteq \mathbb{P}_2^N$.

Let L be the class of a line in the Picard group of $\mathbb{P}_2$ and let $\pi_i : \mathbb{P}_2^N \to \mathbb{P}_2$ be the projection on the ith component. Set $\ell_i = \pi_i^*(L)$. The ℓ_i's have codimension 1 in $\mathbb{P}_2^N$ and they generate its Chow ring, which is isomorphic as a ring to $\mathbb{Z}[\ell_1, \dots, \ell_N]/(\ell_1^3, \dots, \ell_N^3)$.

The pullback through the Segre embedding of a hyperplane of $\mathbb{P}_{3^N-1}$ is given by $\ell_1 + \cdots + \ell_N$ as can be seen directly from the equation of a coordinate hyperplane in $\mathbb{P}_{3^N-1}$. The degree of $\mathcal{C}$ is therefore given by the intersection product $\mathcal{C}.(\ell_1 + \cdots + \ell_N)$ in the Chow ring of $\mathbb{P}_2^N$.

Assume now that $\mathcal{C}_i := \pi_i(\mathcal{C})$ is a curve for all i; by definition, $\deg \mathcal{C}_i = \deg(\mathcal{C}_i.L)$.

We see that

$$\pi_{i*}(\mathcal{C}.\ell_i) = \pi_{i*}(\mathcal{C}.\pi_i^*(L)) = \pi_{i*}(\mathcal{C}).L = d_i\mathcal{C}_i.L$$

where d_i is the degree of the map $\mathcal{C} \to \mathcal{C}_i$ given by the restriction of π_i to $\mathcal{C}$, and the equality in the middle is given by the projection formula (see [18, Example 8.1.7]). Taking the degrees we have

$$\deg(\mathcal{C}.\ell_i) = \deg(\pi_{i*}(\mathcal{C}.\ell_i)) = d_i \deg \mathcal{C}_i$$

so that

$$\begin{aligned}\deg \mathcal{C} &= \deg(\mathcal{C}.(\ell_1 + \cdots + \ell_N)) = \deg(\mathcal{C}.\ell_1) + \cdots + \deg(\mathcal{C}.\ell_N)\\ &= d_1 \deg \mathcal{C}_1 + \cdots + d_N \deg \mathcal{C}_N.\end{aligned}$$

If in particular the curve $\mathcal{C}$ is contained in E^N, then all the $\mathcal{C}_i$'s are equal to E and have degree 3.

Notice that this formula remains true if for some of the i's the restriction of π_i to $\mathcal{C}$ is constant, provided that we take 0 as the degree of a constant map.

We recall now two classical results on heights that will be important in the proof of our theorems. The first is an explicit version of the Arithmetic Bézout Theorem, as proved in [33, Théorème 3]:

THEOREM 2.1 (Arithmetic Bézout theorem). *Let X and Y be irreducible 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*

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

where

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

The second result is Zhang's inequality. In order to state it, we define the essential minimum $\mu_2(X)$ of an irreducible algebraic subvariety $X \subseteq \mathbb{P}_m$ as

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

The following is a special case of [49, Theorem 5.2]:

THEOREM 2.2 (Zhang's inequality). *Let $X \subseteq \mathbb{P}_m$ be an irreducible subvariety. Then*

$$\mu_2(X) \leqslant \frac{h_2(X)}{\deg X} \leqslant (1 + \dim X)\mu_2(X). \tag{2.6}$$

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

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

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

$$\hat{\mu}(X) \leqslant \frac{h(X)}{\deg X} \leqslant (1 + \dim X)\hat{\mu}(X). \tag{2.7}$$

2.2. Algebraic Subgroups of E^N. We recall that the uniformization theorem implies that $E(\mathbb{C})$ is isomorphic, as complex Lie group, to $\mathbb{C}/\Lambda$ for a lattice $\Lambda \subset \mathbb{C}$ unique up to homothety. The Nth power of this isomorphism gives the analytic uniformization $\mathbb{C}^N/\Lambda^N \xrightarrow{\sim} E^N(\mathbb{C})$ of E^N (see for instance [38, Section VI, Theorem 5.1 and Corollary 5.1.1]). Through the exponential map from the tangent space of E^N at the origin to E^N, the Lie algebra of an abelian subvariety of E^N is identified with a complex vector subspace $W \subset \mathbb{C}^N$ for which $W \cap \Lambda^N$ is a lattice of full rank in W. The *orthogonal complement* $B^\perp$ of an abelian subvariety $B \subset E^N$ is the abelian subvariety with Lie algebra corresponding to the orthogonal complement of the Lie algebra of B with respect to the canonical Hermitian structure of $\mathbb{C}^N$ (see for instance [2, 8.2.27 and 8.9.8] for more details).

We end this section by recalling how the essential minimum $\hat{\mu}$ and the canonical height $\hat{h}$ behave with respect to orthogonality in E^N. This is an easy consequence of the main result of [34].

LEMMA 2.3. *Let H be a connected algebraic subgroup of E^N and let $H^\perp$ be its orthogonal complement. Then:*

(1) *if $P_1 \in H$ and $P_2 \in H^\perp$ then $\hat{h}(P_1 + P_2) = \hat{h}(P_1) + \hat{h}(P_2)$;*

(2) *if $V \subseteq H$ is an irreducible subvariety of E^N and $Q \in H^\perp$ then $\hat{\mu}(V + Q) = \hat{\mu}(V) + \hat{h}(Q)$.*

Proof. By [34] H and $H^\perp$ are orthogonal with respect to the Néron–Tate pairing, proving immediately part (1). To prove part (2), notice that

$$\begin{aligned}&\hat{\mu}(V+Q)\\&\quad=\inf\{\theta\in\mathbb{R}\mid \text{The set }\{P'+Q\in V+Q\mid P'\in V,\hat{h}(P'+Q)\leqslant\theta\}\\&\qquad\text{is Zariski dense in } V+Q\}\\&\quad=\inf\{\theta\in\mathbb{R}\mid \text{The set }\{P'\in V\mid \hat{h}(P')\leqslant\theta-\hat{h}(Q)\}\\&\qquad\text{is Zariski dense in } V\}=\hat{\mu}(V)+\hat{h}(Q).\end{aligned}$$ □

3. Basic estimates for heights

This is a self-contained technical section in which we give several explicit estimates on heights, used later. The readers who wish to skip these technical results may refer to the following table for the definition of the relevant constants. The notation was introduced in Section 2.

Summary of Constants. For ease of reference, we collect here the definition of the constants $c_1,\dots,c_7$ that will intervene in our computations. Some of these quantities have a sharper expression when the curve E is defined over $\mathbb{Q}$ and we deal with rational points.

Table 1. Table of constants.

	For $E/\overline{\mathbb{Q}}$ and $P\in E(\overline{\mathbb{Q}})$	For $E/\mathbb{Q}$ and $P\in E(\mathbb{Q})$
$c_1(E)$	$\dfrac{h_W(\Delta)+h_\infty(j)}{4}+\dfrac{h_W(j)}{8}+\dfrac{h_W(A)+h_W(B)}{2}+3.724$	$\min\Big(\dfrac{\log\lvert\Delta\rvert+h_\infty(j)}{4}+\dfrac{h_W(j)}{8}+\dfrac{\log(\lvert A\rvert+\lvert B\rvert+3)}{2}+2.919,\,3h_{\mathcal{W}}(E)+4.709\Big)$
$c_2(E)$	$\dfrac{h_W(\Delta)+h_\infty(j)}{4}+\dfrac{h_W(A)+h_W(B)}{2}+4.015$	$\min\Big(\dfrac{\log\lvert\Delta\rvert+h_\infty(j)}{4}+\dfrac{\log(\lvert A\rvert+\lvert B\rvert+3)}{2}+3.21,\,\dfrac{3h_{\mathcal{W}}(E)}{2}+2.427\Big)$
$c_3(E)$	$\dfrac{h_W(\Delta)}{12}+\dfrac{h_\infty(j)}{12}+1.07$	
$c_4(E)$	$\dfrac{h_W(j)}{24}+\dfrac{h_W(\Delta)}{12}+\dfrac{h_\infty(j)}{12}+0.973$	
$c_5(E)$	$c_1(E)$	$3h_{\mathcal{W}}(E)+6\log 2$
$c_6(E)$	$\dfrac{h_W(A)+h_W(B)+\log 5}{2}$	$\dfrac{\log(3+\lvert A\rvert+\lvert B\rvert)}{2}$
$c_7(E)$	$\dfrac{h_W(A)+h_W(B)+\log 3}{2}$	$\dfrac{\log(1+\lvert A\rvert+\lvert B\rvert)}{2}$

All the above constants are computed below. More precisely, the constants $c_1(E)$ and $c_2(E)$, first appearing in Theorem 1.2, are computed in Proposition 3.2,

by combining bounds of Silverman and Zimmer. The constants $c_3(E)$ and $c_4(E)$ come from formula (3.2) proved in [40, Theorem 1.1]. Moreover $c_5(E)$ is given in Zimmer's bound [50, page 40] recalled in (3.3). We remark that, more recently, algorithms by Cremona *et al.* [12] and by Bruin [6] have been given to bound the difference in (3.2). These algorithms give better bounds in many numerical examples, but they do not provide explicit general formulae for the bounds in terms of the coefficients of a Weierstrass equation for the elliptic curve E, as done in [40, 50]. Moreover, in the available implementations of [12], the Weierstrass model for E is required to be minimal. Therefore we cannot use these bounds for our general theorem.

Finally the constants $c_6(E)$ and $c_7(E)$ are computed in Lemma 3.1.

We now give the details for determining these constants.

If P is a point in $\mathbb{P}_m$, from the definition of h_W and h_2, we have

$$h_W(P) \leqslant h_2(P) \leqslant h_W(P) + \log(m+1)/2. \tag{3.1}$$

If $P \in E$, then, from [40, Theorem 1.1], we have

$$-c_4(E) \leqslant \frac{\hat{h}(P)}{3} - \frac{h_W(x(P))}{2} \leqslant c_3(E) \tag{3.2}$$

where

$$c_3(E) = \frac{h_W(\Delta)}{12} + \frac{h_\infty(j)}{12} + 1.07$$

and

$$c_4(E) = \frac{h_W(j)}{24} + \frac{h_W(\Delta)}{12} + \frac{h_\infty(j)}{12} + 0.973$$

(notice that the Néron–Tate height used by Silverman in [40] is one third of our $\hat{h}$, as defined in [32]).

If E is defined over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$, Zimmer [50, page 40], proved that:

$$-\frac{3h_{\mathcal{W}}(E)}{2} - \frac{7}{2}\log 2 \leqslant h_W(P) - \hat{h}(P) \leqslant 3h_{\mathcal{W}}(E) + 6\log 2. \tag{3.3}$$

We remark that Silverman's bound is better than Zimmer's one for elliptic curves with big coefficients. Nevertheless we included here Zimmer's estimates because they are sharper in some of our examples.

In the following lemma we compare h_2 and h_W for points in E.

LEMMA 3.1. *For every point $P \in E$ we have*

$$|h_2(P) - \tfrac{3}{2}h_W(x(P))| \leqslant c_6(E),$$

$$|h_2(P) - h_W(y(P))| \leqslant c_6(E),$$
$$|h_W(y(P)) - \tfrac{3}{2}h_W(x(P))| \leqslant c_7(E)$$

where

$$c_6(E) = \frac{h_W(A) + h_W(B) + \log 5}{2}$$

and

$$c_7(E) = \frac{h_W(A) + h_W(B) + \log 3}{2}.$$

If moreover E is defined over $\mathbb{Q}$ we may take the sharper values

$$c_6(E) = \frac{\log(|A| + |B| + 3)}{2}$$

and

$$c_7(E) = \frac{\log(|A| + |B| + 1)}{2}.$$

Proof. We write both h_W and h_2 in terms of local contributions and bound each of them. Let $P = (x, y) \in E$ and let k be a number field of definition for P and E. Let us first compare $h_2(P)$ and $h_W(x(P))$.

For every place v of k, we set $\lambda_v = [k_v : \mathbb{Q}_v]/[k : \mathbb{Q}]$.

By the definitions of h_W and h_2, if v is a non-Archimedean place, then the contribution to the difference $h_2(P) - \frac{3}{2}h_W(x(P))$ coming from v is

$$\lambda_v(\log \max(1, |x|_v, |y|_v) - \tfrac{3}{2}\log \max(1, |x|_v)).$$

We see that if $|x|_v \leqslant 1$ then $|y|_v \leqslant 1$ as well, because A and B are algebraic integers, and this contribution is 0. If instead $|x|_v > 1$, then $|y|_v^2 = |x^3 + Ax + B|_v = |x|_v^3$ thanks to the ultrametric inequality, and the contribution is again 0.

If v is an Archimedean place, then the contribution coming from v is

$$\lambda_v\left(\frac{1}{2}\log(1 + |x|_v^2 + |y|_v^2) - \frac{3}{2}\log \max(1, |x|_v)\right)$$
$$= \frac{\lambda_v}{2}(\log(1 + |x|_v^2 + |x^3 + Ax + B|_v) - 3\log \max(1, |x|_v)).$$

If $|x|_v \leqslant 1$ this quantity is at most $(\lambda_v/2)\log(3 + |A|_v + |B|_v)$. If $|x|_v > 1$ we write

$$\frac{\lambda_v}{2}(\log(1+|x|_v^2+|x^3+Ax+B|_v)-3\log|x|_v)$$
$$=\frac{\lambda_v}{2}\left(\log\left(\frac{1}{|x|_v^3}+\frac{1}{|x|_v}+\left|1+\frac{A}{x^2}+\frac{B}{x^3}\right|_v\right)\right),$$

which is again at most $(\lambda_v/2)\log(3+|A|_v+|B|_v)$. If E is defined over $\mathbb{Q}$, then the sum of all λ_v, for v ranging in the Archimedean places, is 1 (as the sum of the local degrees is the global degree) and we get the bound in the statement. If this is not the case, then we check that

$$\log(3+a+b)\leqslant\log 5+\max(0,\log a)+\max(0,\log b)\quad\forall a,b>0$$

so that the quantity $|h_2(P)-\frac{3}{2}h_W(x(P))|$ is bounded by

$$\sum_{v\text{ Archimedean}}\lambda_v\frac{\max(0,\log|A|_v)+\max(0,\log|B|_v)+\log 5}{2}$$
$$=\frac{h_W(A)+h_W(B)+\log 5}{2}.$$

Let us now compare $h_2(P)$ and $h_W(y(P))$. Just as in the case discussed above, the non-Archimedean absolute values give no contribution. Let v be an Archimedean absolute value. The quantity to bound is

$$\lambda_v(\tfrac{1}{2}\log(1+|x|_v^2+|y|_v^2)-\log\max(1,|y|_v)).$$

We consider two cases:

If $|x|_v^2\leqslant 1+|A|_v+|B|_v$ then one easily checks that

$$\tfrac{1}{2}\log(1+|x|_v^2+|y|_v^2)-\log\max(1,|y|_v)\leqslant\tfrac{1}{2}\log(3+|A|_v+|B|_v)$$

for all values of $|y|_v$.

If $|x|_v^2>1+|A|_v+|B|_v$ then

$$|y|_v^2\geqslant|x|_v^2|x|_v-|Ax|_v-|B|_v>|x|_v+|B|_v|x|_v-|B|_v>|x|_v>1$$

and therefore the quantity to bound is

$$\frac{\lambda_v}{2}\log\left(1+\frac{|x|_v^2+1}{|x^3+Ax+B|_v}\right).$$

To see that

$$|x|_v^2+1\leqslant(2+|A|_v+|B|_v)\cdot|x^3+Ax+B|_v$$

we write

$$\begin{aligned}
&(2+|A|_v+|B|_v)\cdot|x^3+Ax+B|_v\\
&\quad\geqslant (2+|A|_v+|B|_v)|x|_v^3-(2+|A|_v+|B|_v)(|Ax|_v+|B|_v)\\
&\quad> |x|_v^3+(1+|A|_v+|B|_v)^2|x|_v-(2+|A|_v+|B|_v)(|Ax|_v+|B|_v)\\
&\quad\geqslant |x|_v^2+1.
\end{aligned}$$

The bound in the statement now follows as in the first case. The bound between $h_W(x(P))$ and $h_W(y(P))$ is proved analogously. □

The following proposition combines in a single statement the bounds by Silverman and Zimmer that we recalled before and Lemma 3.1. It gives a bound between $\hat{h}$ and h_2 for a point in E^N. This estimate is used in the proof of our main theorem.

PROPOSITION 3.2. *Let $P\in E^N$. Then*

$$-Nc_2(E)\leqslant h_2(P)-\hat{h}(P)\leqslant Nc_1(E),$$

where

$$\begin{aligned}
c_1(E)&=\frac{h_W(\Delta)+h_\infty(j)}{4}+\frac{h_W(j)}{8}+\frac{h_W(A)+h_W(B)}{2}+3.724,\\
c_2(E)&=\frac{h_W(\Delta)+h_\infty(j)}{4}+\frac{h_W(A)+h_W(B)}{2}+4.015.
\end{aligned}$$

Moreover, if E is defined over $\mathbb{Q}$ and $P\in E(\mathbb{Q})$ one can take

$$\begin{aligned}
c_1(E)&=\min\Bigg(\frac{\log|\Delta|+h_\infty(j)}{4}+\frac{h_W(j)}{8}+\frac{\log(|A|+|B|+3)}{2}\\
&\qquad+2.919,\,3h_{\mathcal{W}}(E)+4.709\Bigg),\\
c_2(E)&=\min\Bigg(\frac{\log|\Delta|+h_\infty(j)}{4}+\frac{\log(|A|+|B|+3)}{2}\\
&\qquad+3.21,\,\frac{3h_{\mathcal{W}}(E)}{2}+2.427\Bigg).
\end{aligned}$$

Proof. The general bounds are obtained by (3.2) combined with Lemma 3.1. When E is defined over $\mathbb{Q}$ and the point $P\in E(\mathbb{Q})$, they can be sharpened by taking the minimum between the bounds obtained combining (3.2) with Lemma 3.1 and the ones obtained combining (3.3) with (3.1). □

Using Proposition 3.2 we immediately deduce the following relation between the two essential minima $\mu_2(X)$ and $\hat{\mu}(X)$ introduced in Section 2, for any irreducible subvariety X of E^N. We have

$$-Nc_2(E) \leqslant \mu_2(X) - \hat{\mu}(X) \leqslant Nc_1(E) \tag{3.4}$$

where the constants are defined in Proposition 3.2.

Finally, using (3.4), (2.6) and (2.7) we get:

$$\frac{h_2(X)}{1+\dim X} - Nc_1(E)\deg X \leqslant h(X) \leqslant (1+\dim X)(h_2(X) + Nc_2(E)\deg X). \tag{3.5}$$

4. Main results and consequences

In this section we prove a sharper version of Theorem 1.2. The proof relies on a geometrical induction on the dimension N of the ambient variety. We split the statement and the proof in two parts: the base of the induction given by $N = 2$ is Theorem 4.2, and we postpone its proof to Section 5; the inductive step given for $N \geqslant 3$ is Theorem 4.3. Finally we give some more general formulations of our main theorem and additional remarks.

It is evident that our Theorem 1.2 in the Introduction is a direct consequence of Theorems 4.2 and 4.3, where the bounds in Theorem 1.2 are less sharp. This sharper version and the finer constants for points overs $\mathbb{Q}$ are used in the applications to keep the bounds for the height of the rational points on a curve as small as possible.

In our context, we characterize arithmetically points by their rank (see Definition 1.1), while geometrically we characterize a curve by its transversality property.

DEFINITION 4.1. A curve $\mathcal{C}$ in an abelian variety A is transverse (respectively weak-transverse) if it is irreducible and it is not contained in any translate (respectively in any torsion variety).

Here by translate (respectively torsion variety) we mean a finite union of translates of proper algebraic subgroups of A by points (respectively by torsion points).

We remark that curves of genus 1 are translates of an elliptic curve and that, in an abelian variety A of dimension 2, a curve has genus at least 2 if and only if it is transverse. Thus, for $\mathcal{C}$ in E^2 assuming transversality is equivalent to the assumption that the genus is at least 2. Then it is equivalent to state the following theorem for transverse curves.

THEOREM 4.2 (Base of the reduction). *Let E be an elliptic curve without CM. Let $\mathcal{C}$ be an irreducible curve in E^2 of genus $\geqslant 2$. Then every point P on $\mathcal{C}$ of rank $\leqslant 1$ has height bounded as:*

$$\hat{h}(P) \leqslant C_1 \cdot h_2(\mathcal{C}) \deg \mathcal{C} + C_2(E)(\deg \mathcal{C})^2 + C_3(E)$$

where

$$\begin{aligned} C_1 &= 72.251 \\ C_2(E) &= C_1(6.019 + 4c_1(E)) \\ C_3(E) &= 4c_2(E), \end{aligned}$$

and the constants $c_1(E)$ and $c_2(E)$ are defined in Table 1.

The proof of this theorem is the content of the following Section 5.

We now show how to use Theorem 4.2 to prove the following sharper version of our main Theorem 1.2 for $N \geqslant 3$. The central idea is to argue by induction and project $\mathcal{C}$ from E^N to E^n for $n < N$ in such a way that the projection is transverse and its height and degree are well controlled. In order to obtain better bounds, we study different cases according to the geometric conditions satisfied by $\mathcal{C}$.

THEOREM 4.3 (Reduction step). *Let E be an elliptic curve without CM. Let $N \geqslant 3$ be an integer. If $\mathcal{C}$ is an irreducible curve of genus at least 2 embedded in E^N, then every point P of rank at most one in $\mathcal{C}$ has Néron–Tate height bounded as*

$$\begin{aligned} \hat{h}(P) \leqslant{}& 2 \cdot 3^{N-2} N! C_1 h_2(\mathcal{C})(\deg \mathcal{C})^2 + \frac{3^{N-2} N!}{2} C_2(E)(\deg \mathcal{C})^3 \\ &+ 3^{N-2}(N-2)! h_2(\mathcal{C}) \\ &+ \deg \mathcal{C}(3^{N-2}(N-2)!)\left(N(N-1)\left(\frac{C_3(E)}{2} + c_1(E)\right) + C_0(N)\right) \\ &+ N c_2(E). \end{aligned}$$

If $\mathcal{C}$ is weak-transverse we get

$$\hat{h}(P) \leqslant 4(N-1) C_1 h_2(\mathcal{C}) \deg \mathcal{C} + (N-1) C_2(E)(\deg \mathcal{C})^2 + N^2 C_3(E).$$

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

$$\hat{h}(P) \leqslant N C_1 h_2(\mathcal{C}) \deg \mathcal{C} + \frac{N}{2} C_2(E)(\deg \mathcal{C})^2 + \frac{N}{2} C_3(E).$$

Here

$$C_0(N) = (3^N - 3/2) \log 2 + \sum_{i=1}^{N-1} \frac{1}{i} - \frac{1}{2N}$$

$$\begin{aligned} C_1 &= 72.251 \\ C_2(E) &= C_1(6.019 + 4c_1(E)) \\ C_3(E) &= 4c_2(E), \end{aligned}$$

and the constants $c_1(E)$ and $c_2(E)$ are defined in Table 1.

Proof. If P has rank 0 then it is a torsion point and its height is trivial. So we assume that P has rank one.

We first suppose that $\mathcal{C}$ is also transverse in E^N. Let $\pi : E^N \to E^2$ be the projection on any two coordinates. Since $\mathcal{C}$ is transverse in E^N, then $\pi(\mathcal{C})$ is a transverse curve in E^2.

By [27, Lemma 2.1] we have that $\deg \pi(\mathcal{C}) \leqslant \deg \mathcal{C}$. Clearly $h_2(\pi(P)) \leqslant h_2(P)$ for every point P in E^N, therefore $\mu_2(\pi(\mathcal{C})) \leqslant \mu_2(\mathcal{C})$. By Theorem 2.2 with $\pi(\mathcal{C}) \subseteq E^2$ embedded in $\mathbb{P}_8$ as in formula (2.4), we have that

$$h_2(\pi(\mathcal{C})) \leqslant 2\mu_2(\pi(\mathcal{C})) \deg \pi(\mathcal{C}) \leqslant 2\mu_2(\mathcal{C}) \deg \mathcal{C} \leqslant 2h_2(\mathcal{C}).$$

Let now $P = (P_1, \dots, P_N) \in \mathcal{C}$ be a point of rank one. Up to a reordering of the factors of E^N we may assume that $\hat{h}(P_1) \geqslant \hat{h}(P_2) \geqslant \cdots \geqslant \hat{h}(P_N)$ and let π be the projection on the first two coordinates. Then

$$\hat{h}(P) \leqslant \hat{h}(P_1) + (N-1)\hat{h}(P_2) \leqslant \frac{N}{2}\hat{h}(\pi(P)). \tag{4.1}$$

We apply Theorem 4.2 to bound the height of $\pi(P)$ on $\pi(\mathcal{C})$ in E^2, obtaining

$$\begin{aligned} \hat{h}(\pi(P)) &\leqslant C_1 \cdot h_2(\pi(\mathcal{C})) \deg \pi(\mathcal{C}) + C_2(E)(\deg \pi(\mathcal{C}))^2 + C_3(E) \\ &\leqslant 2C_1 \cdot h_2(\mathcal{C}) \deg \mathcal{C} + C_2(E)(\deg \mathcal{C})^2 + C_3(E). \end{aligned}$$

Substituting this estimate in formula (4.1) we get the wished bound for $\mathcal{C}$ transverse.

Suppose now that $\mathcal{C}$ is weak-transverse, but it is not transverse. If the set of points of $\mathcal{C}$ of rank one is empty nothing has to be proven. We show that if it is not empty, then we can reduce to the case of a transverse curve in E^{N-1}.

Since $\mathcal{C}$ is not transverse, but weak-transverse, it is contained in a proper nontorsion translate of minimal dimension $H + Q$, where H is a proper abelian subvariety of E^N and Q is a point in the orthogonal complement $H^\perp$ of H, defined in Section 2.2.

We now prove that $\dim H^\perp = 1$. Let P be a point of $\mathcal{C}$ of rank one. Since Q is the component of P in $H^\perp$, we deduce that Q has rank at most one. But Q cannot be torsion, so it has rank one and $\dim H^\perp = 1$.

Up to a reordering of the coordinates of $P = (P_1, \dots, P_N)$, we can assume that $\hat{h}(P_1) \geqslant \hat{h}(P_i)$ for all $i = 1, \dots, N$. We denote by $\pi_i : E^N \to E^{N-1}$ the natural projection which omits the ith coordinate.

Assume first that there exists an index $i \neq 1$ such that the restriction of π_i to H is surjective. In this case $\pi_i(\mathcal{C})$ is a transverse curve in E^{N-1}. We easily see that $\mu_2(\pi_i(\mathcal{C})) \leqslant \mu_2(\mathcal{C})$; by [27, Lemma 2.1] $\deg \pi_i(\mathcal{C}) \leqslant \deg \mathcal{C}$; by Zhang's inequality $h_2(\pi_i(\mathcal{C})) \leqslant 2h_2(\mathcal{C})$.

So if $N = 3$ we apply Theorem 4.2 and if $N > 3$ we apply the first part of the proof to $\pi_i(\mathcal{C})$ transverse in E^{N-1} obtaining

$$\begin{aligned}\hat{h}(\pi_i(P)) &\leqslant (N-1)C_1 \cdot h_2(\pi_i(\mathcal{C})) \deg \pi_i(\mathcal{C}) + \frac{N-1}{2} C_2(E)(\deg \pi_i(\mathcal{C}))^2 \\ &\quad + \frac{N-1}{2} C_3(E) \\ &\leqslant 2(N-1)C_1 \cdot h_2(\mathcal{C}) \deg \mathcal{C} + \frac{N-1}{2} C_2(E)(\deg \mathcal{C})^2 + \frac{N-1}{2} C_3(E).\end{aligned}$$

Moreover, the height of P is easily bounded as $\hat{h}(P) \leqslant 2\hat{h}(\pi_i(P))$, because the first coordinate has maximal height for P and it is in the projection as $i \neq 1$. This gives the desired bound for $\mathcal{C}$ weak-transverse.

We are left with the case where the restriction of π_i to H is not surjective for all $i \neq 1$. Then $H \supseteq \ker \pi_i$ for all $i \neq 1$ and by counting dimensions $H = \{O\} \times E^{N-1}$. Therefore Q is, up to a torsion point, the first component P_1 of the point P and

$$\hat{h}(P) \leqslant N\hat{h}(P_1) = N\hat{h}(Q). \tag{4.2}$$

By Lemma 2.3 we obtain $\hat{h}(Q) = \hat{\mu}(\mathcal{C}) - \hat{\mu}(\mathcal{C} - Q) \leqslant \hat{\mu}(\mathcal{C}) \leqslant h(\mathcal{C})/\deg \mathcal{C}$. Substituting this in (4.2) and using (3.5) we have

$$\hat{h}(P) \leqslant N \frac{h(\mathcal{C})}{\deg \mathcal{C}} \leqslant 2N \left(\frac{h_2(\mathcal{C})}{\deg \mathcal{C}} + N c_2(E) \right),$$

where $c_2(E)$ is defined in Table 1. This concludes the weak-transverse case as this bound is smaller then the one in the statement.

We finally treat the case of $\mathcal{C}$ of genus at least 2, but not weak-transverse.

Then $\mathcal{C}$ is contained in a translate $H + Q$ of minimal dimension with $Q \in H^{\perp}$, where this time there are no conditions on the rank of Q. We first notice that the translate $H + Q$ is unique. Indeed, suppose that $H' + Q'$ is another such translate and let $P \in \mathcal{C}$ be a point. Then $H + P = H + Q$ and $H' + P = H' + Q'$, thus $\mathcal{C} \subseteq (H \cap H') + P$. The hypothesis on the minimality of the dimension implies then $H + Q = H' + Q'$.

We also notice that $\mathcal{C} - Q$ is transverse in H and the dimension of H is at least 2 otherwise $\mathcal{C} = H + Q$ would have genus 1. Consider the natural projections

$\pi : E^N \to E^{\dim H}$ that omit some $d = N - \dim H$ coordinates. For a question of dimensions, at least one projection π is surjective when restricted to H. Thus the image $\pi(\mathcal{C})$ is transverse in $E^{\dim H}$. Moreover, like in the previous cases, we have $\deg \pi(\mathcal{C}) \leqslant \deg \mathcal{C}$ and $h_2(\pi(\mathcal{C})) \leqslant 2h_2(\mathcal{C})$. We can then apply the first part of the proof to $\pi(\mathcal{C})$ transverse in $E^{\dim H}$ to get

$$\hat{h}(\pi(P)) \leqslant 2(N-d)C_1 h_2(\mathcal{C}) \deg \mathcal{C} + \frac{N-d}{2} C_2(E) (\deg \mathcal{C})^2 + \frac{N-d}{2} C_3(E). \tag{4.3}$$

To bound $h_2(P)$ we first remark that P is a component of $\mathcal{C} \cap (\ker \pi + \pi(P))$, otherwise $\mathcal{C} - Q \subseteq \ker \pi + \pi(P) \cap H \subsetneq H$ would not be transverse in H. We then use the Arithmetic Bézout Theorem for $\mathcal{C} \cap (\ker \pi + \pi(P))$, where we bound $h_2(\ker \pi + \pi(P))$ using Zhang's inequality, equation (3.4) and the fact that $\hat{\mu}(\ker \pi + \pi(P)) = \hat{h}(\pi(P))$ by Lemma 2.3. All of this gives

$$\begin{aligned} h_2(P) \leqslant{}& (1+d)(\deg \ker \pi)\hat{h}(\pi(P)) \deg \mathcal{C} + (\deg \ker \pi) h_2(\mathcal{C}) \\ &+ ((1+d)Nc_1(E) + C_0(1, d, 3^N - 1))(\deg \ker \pi) \deg \mathcal{C}, \end{aligned} \tag{4.4}$$

where

$$C_0(1, d, 3^N - 1) = \sum_{i=1}^{d+2} \frac{1}{i} - \frac{d+3}{2(d+2)} + \left(3^N - \frac{d+3}{2}\right) \log 2$$

is the constant appearing in the Arithmetic Bézout Theorem 2.1 by choosing $d_1 = 1$, $d_2 = d$ and $m = 3^N - 1$.

Clearly $d \leqslant N - 2$ and $\deg \ker \pi = 3^d d! \leqslant 3^{N-2}(N-2)!$, so setting

$$C_0(N) = (3^N - 3/2) \log 2 + \sum_{i=1}^{N-1} \frac{1}{i} - \frac{1}{2N}$$

we have

$$C_0(1, d, 3^N - 1) \leqslant C_0(N)$$

and

$$\begin{aligned} h_2(P) \leqslant{}& 3^{N-2}(N-1)!\hat{h}(\pi(P)) \deg \mathcal{C} + 3^{N-2}(N-2)! h_2(\mathcal{C}) \\ &+ 3^{N-2}(N-2)!(N(N-1)c_1(E) + C_0(N)) \deg \mathcal{C}. \end{aligned} \tag{4.5}$$

Finally, substituting (4.3) into (4.5) and using Proposition 3.2 to compare $\hat{h}(P)$ and $h_2(P)$, we get the bound in the statement. □

Clearly, if E and $\mathcal{C}$ are defined over k and $E(k)$ has rank one then the set $\mathcal{C}(k)$ of k-rational points of $\mathcal{C}$ is a subset of the set of points on $\mathcal{C}$ of rank one, thus of

height bounded as above. We now show how a similar strategy applies to curves transverse in an abelian variety with a factor E^2. The bounds are explicit when an embedding of the abelian variety in some projective space is given, even though this happens rarely for abelian varieties of higher dimension.

PROPOSITION 4.4. *Let E be an elliptic curve and A an abelian variety, both defined over a number field k; let E be embedded in $\mathbb{P}_2$ through equation (2.1) and let us fix an embedding of A in some projective space.*

(a) *Assume that E is without CM. Let $\mathcal{C}$ be a curve transverse in $E^2 \times A$. Then every point P in $\mathcal{C}$ of rank at most one has:*

$$\begin{aligned} h_2(P) \leqslant\ & h_2(A)(1+\dim A)\deg \mathcal{C} + \deg A(h_2(\mathcal{C}) + C_0 \deg \mathcal{C}) \\ & + (1+\dim A)\deg A \\ & \times ((C_3(E) + 2c_1(E))\deg \mathcal{C} + 2C_1(E)h_2(\mathcal{C})(\deg \mathcal{C})^2 \\ & + C_2(E)(\deg \mathcal{C})^3). \end{aligned}$$

(b) *Assume that $E(k)$ has rank zero. Let $\mathcal{C}$ be a curve over k weak-transverse in $E \times A$. Then for every point $P \in \mathcal{C}(k)$ we have:*

$$\begin{aligned} h_2(P) \leqslant\ & (1+\dim A)(2c_1(E)\deg A + h_2(A))\deg \mathcal{C} + \deg A h_2(\mathcal{C}) \\ & + C_0 \deg A \deg \mathcal{C}. \end{aligned}$$

(c) *Assume that E is without CM and that $E(k)$ has rank one. Let $\mathcal{C}$ be a curve over k transverse in $E^2 \times A$. Then for every point $P \in \mathcal{C}(k)$ we have:*

$$\begin{aligned} h_2(P) \leqslant\ & h_2(A)(1+\dim A)\deg \mathcal{C} + \deg A(h_2(\mathcal{C}) + C_0 \deg \mathcal{C}) \\ & + (1+\dim A)\deg A \\ & \times ((C_3(E) + 2c_1(E))\deg \mathcal{C} + 2C_1(E)h_2(\mathcal{C})(\deg \mathcal{C})^2 \\ & + C_2(E)(\deg \mathcal{C})^3). \end{aligned}$$

Here the constants $C_1, C_2(E), C_3(E)$ are defined in Theorem 1.2, C_0 in Theorem 2.1 and $c_1(E)$ in Table 1.

Proof. Part (c) is an immediate corollary of part (a).

To prove parts (a) and (b), we use Theorem 4.2 and the same strategy as in the proof of Theorem 4.3.

Let P be a point in $\mathcal{C}$ of rank one in case (a), respectively, a k-rational point in case (b), and let $\pi : E^2 \times A \to E^2$ be the natural projection on E^2 for the case (a) and let $\pi : E \times A \to E$ be the natural projection on E for the case (b).

The point P is a component of $\mathcal{C}$ intersected with $A' = \{\pi(P)\} \times A$, in case (a) because the curve $\mathcal{C}$ is transverse, in case (b) because $\mathcal{C}$ is weak-transverse and $\pi(P)$ is a torsion point. By the Arithmetic Bézout Theorem we deduce

$$h_2(P) \leqslant h_2(A') \deg \mathcal{C} + h_2(\mathcal{C}) \deg A' + C_0 \deg \mathcal{C} \deg A' \tag{4.6}$$

where the constant C_0 is explicitly given in Theorem 2.1.

Clearly $\deg A' = \deg A$, so we are left to bound $h_2(A')$.

Using Zhang's inequality we get

$$h_2(A') \leqslant (1 + \dim A) \deg A \mu_2(A') = (1 + \dim A) \deg A (h_2(\pi(P)) + \mu_2(A)). \tag{4.7}$$

Moreover $\mu_2(A) \leqslant h_2(A)/\deg A$ and $h_2(\pi(P)) \leqslant \hat{h}(\pi(P)) + 2c_1(E)$ by Proposition 3.2. Thus

$$h_2(A') \leqslant (1 + \dim A)(\deg A(\hat{h}(\pi(P)) + 2c_1(E)) + h_2(A)). \tag{4.8}$$

In case (b), $\pi(P)$ is a torsion point, so $\hat{h}(\pi(P)) = 0$ and we directly deduce the bound.

To bound $\hat{h}(\pi(P))$ in case (a), we apply Theorem 4.2 to the curve $\pi(\mathcal{C})$ transverse in E^2 and we use that $\deg \pi(\mathcal{C}) \leqslant \deg \mathcal{C}$ by [27, Lemma 2.1] and $\mu_2(\pi(\mathcal{C})) \leqslant \mu_2(\mathcal{C})$ by the definition of essential minimum and thus $h_2(\pi(\mathcal{C})) \leqslant 2h_2(\mathcal{C})$ by Zhang's inequality. We obtain

$$\hat{h}(\pi(P)) \leqslant 2C_1 \cdot h_2(\mathcal{C}) \deg \mathcal{C} + C_2(E)(\deg \mathcal{C})^2 + C_3(E). \tag{4.9}$$

Combining (4.9), (4.8) and (4.6) we get the bound in part (a). □

REMARK 4.5. Using the universal property of the Jacobian one can extend the above argument to any curve such that the Jacobian has a factor E of rank zero or E^2 with E of rank one.

In addition in Proposition 4.4 case (b), with $k = \mathbb{Q}$, the number of rational points of $\mathcal{C}$ is easily bounded using Mazur's theorem [28, Theorem 8] and Bézout's theorem, giving

$$\#\mathcal{C}(\mathbb{Q}) \leqslant 16 \deg A \deg \mathcal{C}.$$

Similarly, a bound for the number of k-rational points can be given using Bézout Theorem and the bound of Parent [31] for the size of the torsion group in terms of the degree of k.

As a final remark in this section we notice that the bounds given in Theorem 4.2 use, among others, the estimates of Proposition 3.2. We give here a more intrinsic formulation of our result, where the dependence on the height bounds of Proposition 3.2 is explicitly given.

THEOREM 4.2′. *Let E be an elliptic curve without CM. Let $\mathcal{C}$ be a transverse curve in E^2. Let $d_2(E), d_1(E) > 0$ be two constants such that*

$$-d_2(E) \leqslant h_2(Q) - \hat{h}(Q) \leqslant d_1(E) \quad \forall Q \in E(\overline{\mathbb{Q}}). \tag{4.10}$$

Then for every point P in $\mathcal{C}$ of rank at most one, we have:

$$\hat{h}(P) \leqslant D_1 \cdot h_2(\mathcal{C}) \deg \mathcal{C} + D_2(E)(\deg \mathcal{C})^2 + D_3(E)$$

where

$$\begin{aligned} D_1 &= 72.251 \\ D_2(E) &= D_1(6.019 + 4d_2(E)) \\ D_3(E) &= 4d_1(E). \end{aligned}$$

This formulation might help for potential future applications; indeed for specific elliptic curves one can prove different versions of the bounds in (4.10) (using, for instance, the algorithms in [**12**] or [**6**] instead of the more explicit bounds in [**40**]) and possibly improve, in those cases, the bounds in our main theorem.

5. The proof of the main theorem for $N = 2$

In this section we first prove the new key estimate at the base of the bound in Theorem 4.2 and then we show how to conclude its proof.

5.1. Bounds for the degree and the height of a translate. Here we prove some general bounds for the degree and the height of a proper translate $H + P$ in E^2 in terms of $\hat{h}(P)$ and of the coefficients of the equation defining the algebraic subgroup H.

PROPOSITION 5.1. *Let $P = (P_1, P_2)$ be a point in E^2, where E is without CM. Let H be a component of the algebraic subgroup in E^2 defined by the equation $\alpha X_1 + \beta X_2 = O$, where O is the neutral element of E and $u = (\alpha, \beta) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Then*

$$\deg(H + P) \leqslant 3\|u\|^2$$

where $\|u\|$ denotes the euclidean norm of u,

$$h(H+P) \leqslant 6\hat{h}(u(P)),$$

and

$$h_2(H+P) \leqslant 6\hat{h}(u(P)) + 12\|u\|^2 c_1(E)$$

where $u(P) = \alpha P_1 + \beta P_2$ and $c_1(E)$ is defined in Table 1.

Proof. A bound for the degree of $H+P$.

We compute the degree of $H+P$ as explained in Section 2.1. We have $H+P \subseteq E^2$, with E^2 embedded in $\mathbb{P}_2^2$ via the Weierstrass form of E (see formula (2.4)). For $1 \leqslant i \leqslant 2$, let $\pi_i : \mathbb{P}_2^2 \to \mathbb{P}_2$ be the projection on the ith component and let ℓ_i be the pullback via π_i of the class of a line in the Picard group of $\mathbb{P}_2$. The maps π_1 and π_2 have degree, respectively, β^2 and α^2, thus

$$\deg((H+P).\ell_1) = \beta^2 \deg E = 3\beta^2,$$
$$\deg((H+P).\ell_2) = \alpha^2 \deg E = 3\alpha^2.$$

Therefore computing the degree as intersection product we get

$$\deg(H+P) = 3(\alpha^2+\beta^2) = 3\|u\|^2. \tag{5.1}$$

A bound for the height of $H+P$. Let $P = (P_1, P_2)$ be a point in E^2. Let H be a component of the algebraic subgroup defined by the vector $u = (\alpha, \beta) \in \mathbb{Z}^2$. Let $u^\perp = (-\beta, \alpha)$. Then $u^\perp$ defines an algebraic subgroup $H^\perp$, and for any point $P \in E^2$ there exist 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

$$U = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$$

be the 2×2 matrix with rows u and $u^\perp$.

We remark that $u(P_0) = 0$ because $P_0 \in H$, and $u^\perp(P^\perp) = 0$ as $P^\perp \in H^\perp$. Therefore

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

We have that $UU^t = U^tU = (\det U) I_2$; hence

$$[\det U]P^\perp = U^tUP^\perp = U^t \begin{pmatrix} u(P) \\ 0 \end{pmatrix}.$$

Computing canonical heights we have

$$(\det U)^2\hat{h}(P^\perp) = \hat{h}([\det U]P^\perp) = \hat{h}\left(U^t\begin{pmatrix}u(P)\\0\end{pmatrix}\right) = \hat{h}\left(\begin{pmatrix}\alpha & -\beta\\ \beta & \alpha\end{pmatrix}\begin{pmatrix}u(P)\\0\end{pmatrix}\right)$$
$$= (\alpha^2+\beta^2)\hat{h}(u(P)) = (\det U)\hat{h}(u(P)),$$

and so

$$\hat{h}(P^\perp) = \frac{\hat{h}(u(P))}{\det U}.$$

By Lemma 2.3 we know that

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

and therefore, by Zhang's inequality (2.7)

$$h(H+P) \leqslant 2(\deg H)\hat{\mu}(H+P) = 2(\deg H)\hat{h}(P^\perp)$$
$$= 2\frac{(\deg H)}{\det U}\hat{h}(u(P)) = 2\frac{(\deg H)}{\|u\|^2}\hat{h}(u(P)).$$

Analogously for h_2 using (2.6) and (3.4) we obtain

$$h_2(H+P) \leqslant 2(\deg H)\mu_2(H+P) \leqslant 2\deg H(\hat{\mu}(H+P)+2c_1(E))$$
$$= 2\deg H\left(\frac{\hat{h}(u(P))}{\det U}+2c_1(E)\right) = 2\deg H\left(\frac{\hat{h}(u(P))}{\|u\|^2}+2c_1(E)\right).$$

By (5.1) we get

$$\deg H \leqslant 3\|u\|^2,$$

which leads to the bounds for $h(H+P)$ and $h_2(H+P)$ in the statement. □

5.2. Geometry of numbers. In this section we use a classical result from the Geometry of Numbers to prove a sharp technical lemma that will be used to build an auxiliary translate so that both its degree and height are small.

LEMMA 5.2. *Let $L \in \mathbb{R}[X_1, X_2]$ be a linear form and let $1 < \kappa$. If*

$$T \geqslant \frac{\kappa}{\sqrt{2}(\kappa-1)^{1/4}},$$

then there exists $u \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that

$$\|u\| \leqslant T$$
$$|L(u)| \leqslant \frac{\kappa\|L\|}{T},$$

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 $\mathscr{S}_T \subseteq \mathbb{R}^2$ be the set of points (x, y) satisfying the two inequalities

$$\sqrt{x^2 + y^2} \leqslant T$$
$$|L(x, y)| \leqslant \kappa \|L\| / T.$$

Geometrically $\mathscr{S}_T$ is the intersection between a circle of radius T and a strip of width $2\kappa/T$, as presented in the following figure (the set $\mathscr{S}_T$ is lightly shaded).

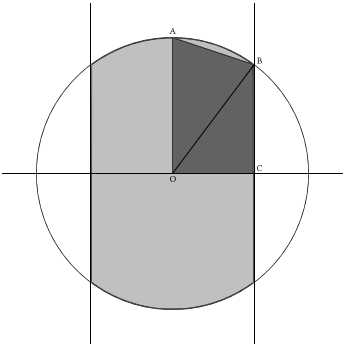

Figure 1. The set $\mathscr{S}_T$.

The statement of the theorem is equivalent to $\mathscr{S}_T \cap \mathbb{Z}^2 \neq \{(0, 0)\}$. By Minkowski's Convex Body Theorem if the set $\mathscr{S}_T$ has an area bigger than 4, then the intersection $\mathscr{S}_T \cap \mathbb{Z}^2$ contains points other than the origin.

The area of $\mathscr{S}_T$ is bigger than four times the area of the dark grey trapezoid in the picture, which can be easily computed as

$$\frac{\kappa}{2T}\left(T + \sqrt{T^2 - \frac{\kappa^2}{T^2}}\right).$$

Therefore we need to check that

$$\frac{\kappa}{2T}\left(T + \sqrt{T^2 - \frac{\kappa^2}{T^2}}\right) \geqslant 1.$$

This is trivially true for all $\kappa \geqslant 2$ (notice that $\kappa/\sqrt{2}(\kappa - 1)^{1/4} \geqslant \sqrt{\kappa}$). If $1 < \kappa < 2$ an easy computation shows that the inequality holds as soon as $T \geqslant \kappa/\sqrt{2}(\kappa - 1)^{1/4}$. □

5.3. The auxiliary subgroup. In Proposition 5.4 we apply our Lemma 5.2 to construct the auxiliary translate $H + P$ used in the proof of Theorem 4.2.

LEMMA 5.3. *Let E be without CM. Let $P = (P_1, P_2) \in E^2$ be a point of rank one. Then there exists a linear form $L \in \mathbb{R}[X_1, X_2]$ with $\|L\| = 1$ and*

$$\hat{h}(t_1P_1 + t_2P_2) = |L(\mathbf{t})|^2\hat{h}(P)$$

for all $\mathbf{t} = (t_1, t_2) \in \mathbb{Z}^2$.

Proof. Let g be a generator for $\langle P_1, P_2\rangle_{\mathbb{Z}}$ and let $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ and T_1, T_2 torsion points such that $P_1 = [a]g + T_1$ and $P_2 = [b]g + T_2$. Thus $\hat{h}(P) = \hat{h}(ag) + \hat{h}(bg) = (a^2 + b^2)\hat{h}(g)$. Consider the linear form

$$L(X_1, X_2) = \frac{aX_1 + bX_2}{\sqrt{a^2 + b^2}}.$$

Then for all $\mathbf{t} = (t_1, t_2) \in \mathbb{Z}^2$ we have:

$$\begin{aligned}\hat{h}(t_1P_1 + t_2P_2) &= \hat{h}([at_1 + bt_2]g) = (at_1 + bt_2)^2\hat{h}(g)\\ &= \frac{(at_1 + bt_2)^2}{a^2 + b^2}\hat{h}(P) = |L(\mathbf{t})|^2\hat{h}(P).\end{aligned}$$

□

We can now construct the auxiliary translate.

PROPOSITION 5.4. *Let E be without CM. Let $P \in E^2$ be a point of rank one. Let $1 < \kappa$ and $T \geqslant \kappa^2/2(\kappa - 1)^{1/2}$.*

Then there exists an elliptic curve $H \subseteq E^2$ such that

$$\begin{aligned}\deg(H + P) &\leqslant 3T,\\ h_2(H + P) &\leqslant \frac{6\kappa^2}{T}\hat{h}(P) + 12Tc_1(E)\end{aligned}$$

where $c_1(E)$ is defined in Table 1.

Proof. By Lemma 5.3, there exists a linear form $L \in \mathbb{R}[X_1, X_2]$ with $\|L\| = 1$ such that $\hat{h}(t_1P_1 + t_2P_2) = |L(\mathbf{t})|^2\hat{h}(P)$ for all vectors $t = (t_1, t_2) \in \mathbb{Z}^2$.

By Lemma 5.2, applied to L, κ and $\sqrt{T}$, there exists $u \in \mathbb{Z}^2$ such that $\|u\| \leqslant \sqrt{T}$ and $|L(u)| \leqslant \kappa\|L\|/\sqrt{T} = \kappa/\sqrt{T}$.

Consider the subgroup defined by the equation $u(X) = O$ and denote by H the irreducible component containing O. By Proposition 5.1, we have that

$$\deg(H + P) \leqslant 3\|u\|^2$$

and

$$h_2(H+P) \leqslant 6\hat{h}(u(P)) + 12\|u\|^2 c_1(E).$$

Combining these bounds with the above inequalities, we get that

$$\begin{aligned} \deg(H+P) &\leqslant 3T, \\ h_2(H+P) &\leqslant \frac{6\kappa^2}{T}\hat{h}(P) + 12Tc_1(E). \end{aligned}$$

□

5.4. Conclusion of the proof of Theorem 4.2. In this section we conclude the proof of Theorem 4.2. We shall approximate a point of rank one with a translate constructed as above. Combining the Arithmetic Bézout Theorem and a good choice of the parameters we conclude that the height of P is bounded.

Proof of Theorem 4.2. If P has rank zero then its height is zero and the statement is true.

Let T and κ be real numbers with $\kappa > 1$ and $\sqrt{T} \geqslant \kappa/\sqrt{2}(\kappa-1)^{1/4}$. We apply Proposition 5.4 to the point P of rank one, thus obtaining an elliptic curve H with

$$\begin{aligned} \deg(H+P) &\leqslant 3T, \\ h_2(H+P) &\leqslant \frac{6\kappa^2}{T}\hat{h}(P) + 12Tc_1(E). \end{aligned} \tag{5.2}$$

The values of the free parameters T and κ will be chosen later.

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 $\mathcal{C} = H + P$, contradicting the fact that $\mathcal{C}$ has genus $\geqslant 2$. Therefore we can apply the Arithmetic Bézout Theorem to the intersection $\mathcal{C} \cap (H+P)$, obtaining:

$$h_2(P) \leqslant h_2(\mathcal{C}) \deg H + h_2(H+P) \deg \mathcal{C} + C_0(1,1,8) \deg H \deg \mathcal{C}$$

where $C_0(1,1,8) = \frac{7}{6}(1+6\log 2) \leqslant 6.019$.

By Proposition 3.2 we have $\hat{h}(P) \leqslant h_2(P) + 2c_2(E)$ so, using the bounds in formula (5.2), we get

$$\begin{aligned} \hat{h}(P) \leqslant 3Th_2(\mathcal{C}) + \frac{6\kappa^2}{T}\hat{h}(P)\deg\mathcal{C} \\ + 3T\deg\mathcal{C}(4c_1(E) + C_0(1,1,8)) + 2c_2(E). \end{aligned}$$

Let now

$$c_8(\mathcal{C}) = 6\deg\mathcal{C},$$

$$c_9(\mathcal{C}, E) = 3h_2(\mathcal{C}) + 3\deg \mathcal{C}(4c_1(E) + C_0(1, 1, 8)),$$
$$c_{10}(\mathcal{C}, E) = 2c_2(E),$$

so that

$$\hat{h}(P) \leqslant c_8 \frac{\kappa^2}{T} \hat{h}(P) + c_9 T + c_{10}. \tag{5.3}$$

We set

$$\kappa = 1 + \frac{1}{16c_8^2}$$
$$T = c_8\kappa^2\left(1 + \sqrt{1 + \frac{c_{10}}{c_8 c_9 \kappa^2}}\right).$$

Notice that $1 < \kappa$, $T \geqslant \kappa^2/2\sqrt{\kappa - 1}$, so our assumptions on κ and T are satisfied. Furthermore

$$2c_8\kappa^2 \leqslant T \leqslant 2c_8\kappa^2 + \frac{c_{10}}{2c_9} \tag{5.4}$$

and the coefficient of $\hat{h}(P)$ on the right hand side of (5.3) is smaller than 1, so we can bring it to the left hand side and express $\hat{h}(P)$ in terms of the rest. After simplification, and using the definition of T, (5.3) becomes

$$\hat{h}(P) \leqslant 2c_9 T + c_{10} = \frac{c_9 T^2}{c_8 \kappa^2}.$$

Using (5.4) this simplifies to

$$\hat{h}(P) \leqslant 4c_8 c_9 \kappa^2 + 2c_{10}. \tag{5.5}$$

After substituting everything back and noticing that $\kappa \leqslant 1 + \frac{1}{576}$, the last inequality (5.5) becomes the bound in the statement of the theorem. □

REMARK 5.5. Theorem 4.2′ is proven in an analogous way, replacing Proposition 3.2 and the constants $c_1(E), c_2(E)$ with relation (4.10) and the constants $d_1(E), d_2(E)$, respectively.

6. Transversality and invariants for a large family of curves in E^2

In this section we give a simple criterion to prove the transversality of a curve in E^2. We also show an easy argument to explicitly bound the height and the degree of a large class of curves.

LEMMA 6.1. *Let $\mathcal{C} \subseteq E^2$ be an irreducible curve. Assume that:*

(i) *$\mathcal{C}$ is not of the form $\{P\} \times E$ or $E \times \{P\}$ for some point $P \in E$;*

(ii) *for every point $(P_1, P_2) \in \mathcal{C}$ the point $(-P_1, P_2)$ also belongs to $\mathcal{C}$.*

Then $\mathcal{C}$ is transverse.

Proof. By (i), the curve $\mathcal{C}$ is not $\{P\} \times E$, so the natural projection $\mathcal{C} \to E$ on the first coordinate is surjective. Thus $\mathcal{C}$ contains at least one point (P_1, P_2) with P_1 not a torsion point in E. By (ii), then $\mathcal{C}$ contains also the point $(-P_1, P_2)$. Observe that the only nontransverse curves in E^2 are translates. So if $\mathcal{C}$ were not transverse, then it would be a translate $H + Q$ of an elliptic curve H by a point $Q = (Q_1, Q_2)$. Therefore the difference $(P_1, P_2) - (-P_1, P_2) = (2P_1, 0)$ would belong to H, and so would all its multiples. This implies that $H = E \times \{0\}$ and $\mathcal{C} = E \times \{Q_2\}$, contradicting (i). □

This last lemma is useful to show the transversality of the following curves.

THEOREM 6.2. *Let E be defined over a number field k. Let E^2 be given as in (1.1) and let $\mathcal{C}$ be the projective closure of the curve in E^2 given by the additional equation*

$$p(x_1) = y_2,$$

where $p(X) = p_0 X^n + p_1 X^{n-1} + \cdots + p_n$ is a nonconstant polynomial in $k[X]$ of degree n having m coefficients different from zero.

Then $\mathcal{C}$ is transverse and its degree and normalized height are bounded as

$$\deg \mathcal{C} = 6n + 9$$

and

$$h_2(\mathcal{C}) \leqslant 6(2n+3)(h_W(p) + \log m + 2c_6(E))$$

where $h_W(p) = h_W(1 : p_0 : \ldots : p_n)$ is the height of the polynomial $p(X)$ and $c_6(E)$ is defined in Table 1.

Proof. Clearly the curve $\mathcal{C}$ is not of the form $E \times \{P\}$ or $\{P\} \times E$ for some point $P \in E$. Moreover, as the equation $p(x_1) = y_2$ does not involve the coordinate y_1, we have that if $(P_1, P_2) \in \mathcal{C}$, then also $(-P_1, P_2) \in \mathcal{C}$. The transversality of $\mathcal{C}$ then follows from Lemma 6.1, once we have proved that $\mathcal{C}$ is irreducible. To this aim, it is enough to check that the ideal generated by $y_1^2 - x_1^3 - Ax_1 - B$ and $x_2^3 - Ax_2 + B - p(x_1)^2$ is a prime ideal in $k(x_1)[x_2, y_1]$. This follows by observing that both polynomials are irreducible over $k(x_1)$ and involve only one

of the two unknowns, with coprime exponents. To check the irreducibility of $x_2^3 - Ax_2 + B - p(x_1)^2$ we observe that a root $f(x_1)$ of this polynomial over $k(x_1)$ gives a morphism $x_1 \mapsto (f(x_1), p(x_1))$ from $\mathbb{P}_1$ to E which is not constant as $\deg p(x) \geqslant 1$. Such a morphism cannot exist.

The degree of $\mathcal{C}$ is computed as an intersection product as explained in Section 2.1. The preimage in $\mathcal{C}$ of a generic point of E through the projection on the first component consists of three points. The preimage through the projection on the second component has generically $2n$ points. Therefore $\deg \mathcal{C} = 3(2n+3)$.

We now want to estimate the height of $\mathcal{C}$. By Zhang's inequality we have $h_2(\mathcal{C}) \leqslant 2 \deg \mathcal{C} \mu_2(\mathcal{C})$. We compute an upper bound for $\mu_2(\mathcal{C})$ by constructing an infinite set of points on $\mathcal{C}$ of bounded height. Let $Q_\zeta = ((\zeta, y_1), (x_2, y_2)) \in \mathcal{C}$, where $\zeta \in \overline{\mathbb{Q}}$ is a root of unity. Clearly there exist infinitely many such points on $\mathcal{C}$. Using the equations of $\mathcal{C}$ and classical estimates on the Weil height we have:

$$h_W(\zeta) = 0,$$
$$h_W(y_2) \leqslant h_W(1 : p_0 : \ldots : p_n) + \log m.$$

By Lemma 3.1 we get:

$$h_2(\zeta, y_1) \leqslant c_6(E),$$
$$h_2(x_2, y_2) \leqslant h_W(1 : p_0 : \ldots : p_n) + \log m + c_6(E)$$

where $c_6(E)$ is defined in Table 1. Thus for all points Q_ζ we have

$$h_2(Q_\zeta) = h_2(x_1, y_1) + h_2(\zeta, y_2) \leqslant h_W(1 : p_0 : \ldots : p_n) + \log m + 2c_6(E).$$

By the definition of essential minimum, we deduce

$$\mu_2(\mathcal{C}) \leqslant h_W(1 : p_0 : \ldots : p_n) + \log m + 2c_6(E).$$

Finally, by Zhang's inequality (2.6)

$$h_2(\mathcal{C}) \leqslant 2 \deg \mathcal{C} \mu_2(\mathcal{C}) \leqslant 6(2n+3)(h_W(1 : p_0 : \ldots : p_n) + \log m + 2c_6(E))$$

as wished. □

We now apply Theorem 4.2 in order to prove an effective Mordell theorem for the large family of curves defined above. The following theorem is a sharper version of Theorem 1.3 in the Introduction. If P is a rational point on one of our curves, we also give bounds for the integers a, b such that $P = ([a]g, [b]g)$, where g generates $E(k)$. These bounds are used in the algorithm in Section 9 to list all the rational points and their shape explains why a g with large height is advantageous for us.

THEOREM 6.3. *Assume that E is without CM, defined over a number field k and that $E(k)$ has rank one. Let $\mathcal{C}$ be the projective closure of the curve given in E^2 by the additional equation*

$$p(x_1) = y_2,$$

with $p(X) \in k[X]$ a nonconstant polynomial of degree n having m nonzero coefficients.

Then $\mathcal{C}$ is irreducible and for $P \in \mathcal{C}(k)$ we have

$$\hat{h}(P) \leqslant 1300.518(2n+3)^2(h_W(p) + \log m + 2c_6(E) + 3.01 + 2c_1(E)) + 4c_2(E)$$

where $h_W(p) = h_W(1 : p_0 : \ldots : p_n)$ is the height of the polynomial $p(X)$ and the constants $c_6(E)$, $c_1(E)$ and $c_2(E)$ are defined in Table 1.

Writing $P = ([a]g, [b]g)$ where a and b are integers and g is a generator of $E(k)$ we have that

$$\max(|a|, |b|) \leqslant \left(\frac{\hat{h}(P)}{\hat{h}(g)}\right)^{1/2}.$$

Proof. Let $P \in \mathcal{C}(k)$. In view of Theorem 6.2, $\mathcal{C}$ is transverse in E^2, thus irreducible. We can apply Theorem 4.2 to $\mathcal{C}$ in E^2 and use the bounds for $\deg \mathcal{C}$ and $h_2(\mathcal{C})$ computed in Theorem 6.2 to obtain the desired upper bound for $\hat{h}(P)$. The bound on $|a|$ and $|b|$ follows from the equality $(a^2 + b^2)\hat{h}(g) = \hat{h}(P)$. □

7. Estimates for the family $\mathcal{C}_n$

In the following two sections we study two special families of curves. The rough idea is to cut a transverse curve in E^2 with an equation with few small integral coefficients and choosing E without CM defined by a Weierstrass equation with small integral coefficients and with $E(\mathbb{Q})$ of rank one. A generator of large height can help in the implementation, but it does not play any role in the height bounds. Such a choice of the curve keeps the bound for the height of its rational points very small, so small that we can implement a computer search and list them all.

In this section we investigate the family $\{\mathcal{C}_n\}_n$ of curves given in Definition 1.4, that is cut in E^2 by the additional equation $x_1^n = y_2$.

As a direct application of Theorem 6.2 with $p(x_1) := x_1^n$ we have:

COROLLARY 7.1. *For every $n \geqslant 1$, the curve $\mathcal{C}_n$ is transverse in E^2 and its degree and normalized height are bounded as*

$$\deg \mathcal{C}_n = 6n + 9,$$
$$h_2(\mathcal{C}_n) \leqslant 6(2n+3)\log(3 + |A| + |B|).$$

Even if it is not necessary for the results of this paper, it is interesting to remark that the genus of the curves in the family $\{\mathcal{C}_n\}_n$ is unbounded for generic rational integers A and B, as shown by the following lemma.

LEMMA 7.2. *Suppose that the coefficients A and B of the elliptic curve E are rational integers such that $-3A$ and -3Δ are not squares, where Δ is the discriminant of E, and $B(2A^3 + B^2)(3A^3 + 8B^2) \neq 0$. Then the curve $\mathcal{C}_n$ of Definition 1.4 has genus $4n + 2$.*

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

Let $\alpha_1, \alpha_2, \alpha_3$ be the three distinct roots of the polynomial $f(T) = T^3 + AT + B$; let also $\beta_1, \beta_2, \beta_3, \beta_4$ be the roots of the polynomial $g(T) = 27T^4 - 54BT^2 + 4A^3 + 27B^2$, which are the values such that $f(T) - \beta_i^2$ has multiple roots. If $-3A$ and -3Δ are not squares then the polynomial $g(T)$ is irreducible over $\mathbb{Q}$ [**23**, Theorem 2]; in particular, the β_i are all distinct.

The β_i have degree 4 over $\mathbb{Q}$, and therefore they cannot be equal to any of the α_j^n, which have degree at most 3. Also for all $n \geqslant 1$ the three α_j^n are distinct, otherwise the ratio α_i/α_j would be a root of 1 inside the splitting field of a polynomial of degree 3, which is easily discarded (if the ratio is 1, then $\Delta = 0$, if the ratio is -1 then $B = 0$, if the ratio is i then $2A^3 + B^2 = 0$, if the ratio is a primitive third root of unity, then $A = 0$, if the ratio is a primitive sixth root of unity, then $3A^3 + 8B^2 = 0$).

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

By Hurwitz formula

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

□

We remark that the five curves $E_1, \ldots, E_5$ satisfy the hypotheses of Lemma 7.2.

We now prove an effective Mordell theorem for the family $\{\mathcal{C}_n\}_n \subseteq E^2$.

The bound for the canonical height of a point $P \in \mathcal{C}_n(k)$ is a simple corollary of Theorem 6.3 while, for this specific family, we sharpen the bounds for the integers a, b such that $P = ([a]g, [b]g)$, where g generates $E(k)$. This improvement

speeds up the computer search. We use here some technical height bounds proved in Section 3.

THEOREM 7.3. *Let E be an elliptic curve defined over a number field k, without CM and such that $E(k)$ has rank one. Let $\{\mathcal{C}_n\}_n$ be the family of curves of Definition 1.4. For every $n \geqslant 1$ and every point $P \in \mathcal{C}_n(k)$ we have*

$$\hat{h}(P) \leqslant 1300.518(2c_6(E) + 3.01 + 2c_1(E))(2n+3)^2 + 4c_2(E).$$

Writing $P = ([a]g, [b]g)$ where a and b integers and g is a generator of $E(k)$, we have that

$$|a| \leqslant \left(\frac{3\hat{h}(P) + 3c_5(E) + 6nc_3(E)}{(2n+3)\hat{h}(g)}\right)^{1/2}$$

and

$$|b| \leqslant \left(\frac{2n\hat{h}(P) + 6nc_4(E) + 9c_3(E) + 3c_7(E)}{(2n+3)\hat{h}(g)}\right)^{1/2}.$$

Here the constants $c_1(E), \ldots, c_7(E)$ are defined in Table 1.

Proof. From Theorem 6.3 applied to $p(x_1) := x_1^n$ we have

$$\hat{h}(P) \leqslant 1300.518(2c_6(E) + 3.01 + 2c_1(E))(2n+3)^2 + 4c_2(E).$$

By the definition of $\hat{h}$ on E^2 (see formula (2.5)) and the standard properties of the Néron–Tate height, we have

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

and

$$(x([a]g))^n = y([b]g) \tag{7.1}$$

because P is on the curve with equation $x_1^n = y_2$.

Combining the bounds (7.1) with (3.2), (3.1) (respectively (3.3) if $k = \mathbb{Q}$) and Proposition 3.2, proved in Section 3, we get

$$\begin{aligned}
\tfrac{2}{3}na^2\hat{h}(g) &\leqslant nh_W(x([a]g)) + 2nc_3(E) = h_W(y([b]g)) + 2nc_3(E) \\
&\leqslant h_W([b]g) + 2nc_3(E) \\
&\leqslant h_2([b]g) + 2nc_3(E) \leqslant \hat{h}([b]g) + c_5(E) + 2nc_3(E) \\
&= b^2\hat{h}(g) + c_5(E) + 2nc_3(E)
\end{aligned}$$

where $c_5(E) = c_1(E)$ in general, while if $k = \mathbb{Q}$ one can take $c_5(E) = 3h_{\mathcal{W}}(E) + 6\log 2$. Therefore

$$\frac{2n+3}{3}a^2\hat{h}(g) \leqslant \hat{h}(P) + c_5(E) + 2nc_3(E),$$

which gives the bound in the statement.

Using (3.2) and Lemma 3.1, proved in Section 3, we get

$$\begin{aligned} b^2\hat{h}(g) &\leqslant \frac{3}{2}h_W(x([b]g)) + 3c_3(E) \leqslant h_W(y([b]g)) + c_7(E) + 3c_3(E) \\ &= nh_W(x([a]g)) + c_7(E) + 3c_3(E) \\ &\leqslant \frac{2na^2}{3}\hat{h}(g) + 2nc_4(E) + c_7(E) + 3c_3(E) \end{aligned}$$

where $c_7(E) = (h_W(A) + h_W(B) + \log 3)/2$ and, if $k = \mathbb{Q}$ one can take $c_7(E) = \log(1 + |A| + |B|)/2$. Therefore

$$\frac{2n+3}{3}b^2\hat{h}(g) \leqslant \frac{2n}{3}\hat{h}(P) + 2nc_4(E) + c_7(E) + 3c_3(E)$$

which gives the desired bound. □

We remark that the bound for $|a|$ in Theorem 7.3 grows like $\sqrt{n}$ (while the one for $|b|$ grows like n).

8. Estimates for the family $\mathcal{D}_n$

We can do similar computations for the family $\mathcal{D}_n$ of Definition 1.4. Thanks to the arithmetic properties of the cyclotomic polynomials we can prove a better bound for $h_2(\mathcal{D}_n)$ than the one that follows directly from Theorem 6.2.

PROPOSITION 8.1. *For every $n \geqslant 2$, the curve $\mathcal{D}_n$ is transverse in E^2 and its degree and normalized height are bounded as*

$$\begin{aligned} &\deg \mathcal{D}_n = 6\varphi(n) + 9, \\ &h_2(\mathcal{D}_n) \leqslant 6(2\varphi(n) + 3)(2^{\omega_2(n)}\log 2 + 2c_6(E)), \end{aligned}$$

where $\varphi(n)$ is the Euler function, $\omega_2(n)$ is the number of distinct odd prime factors of n, and $c_6(E)$ is defined in Table 1.

Proof. Transversality and the bound for the degree follow directly from Theorem 6.2.

Now we follow the same strategy as in the proof of Theorem 6.2 and we construct an infinite set of points on $\mathcal{D}_n$ of bounded height, getting an upper bound for $\mu_2(\mathcal{D}_n)$.

Let $Q_\zeta = ((\zeta, y_1), (x_2, y_2)) \in \mathcal{D}_n$, where $\zeta \in \overline{\mathbb{Q}}$ is a root of unity. Clearly there exist infinitely many such points on $\mathcal{D}_n$.

We claim that for every root of unity ζ and for every $n \geqslant 1$ we have:

$$h_W(\Phi(\zeta)) \leqslant 2^{\omega_2(n)} \log 2,$$

where $\omega_2(n)$ is the number of distinct odd prime factors of n. To show this, we first show that we can assume n to be square-free.

Let r be the product of the distinct prime divisors of n. Then we have that $\Phi_n(x) = \Phi_r(x^{n/r})$ and if ζ is a root of 1 so is $\zeta^{n/r}$.

We can also assume n to be odd, because if $n = 2d$ with d odd, then $\Phi_n(x) = \Phi_d(-x)$.

Now we write

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

where $\mu(n)$ is the Möbius function, and we observe that when n is odd and square-free then there are exactly $2^{\omega_2(n)}$ factors in the product, and that $h_W(\zeta^d - 1) \leqslant \log 2$ for all ζ and d.

Using the equations of $\mathcal{D}_n$ we have:

$$h_W(y_2) \leqslant 2^{\omega_2(n)} \log 2.$$

Thus by Lemma 3.1

$$h_2(\zeta, y_1) \leqslant c_6(E), \quad h(x_2, y_2) \leqslant 2^{\omega_2(n)} \log 2 + c_6(E)$$

and, using (3.1), for all points Q_ζ we have

$$h_2(Q_\zeta) = h_2(x_1, y_1) + h_2(\zeta, y_2) \leqslant 2^{\omega_2(n)} \log 2 + 2c_6(E).$$

By the definition of essential minimum, we deduce

$$\mu_2(\mathcal{D}_n) \leqslant 2^{\omega_2(n)} \log 2 + 2c_6(E).$$

and by Zhang's inequality $h_2(\mathcal{D}_n) \leqslant 2 \deg \mathcal{D}_n \mu_2(\mathcal{D}_n)$ which gives the bounds in the statement. □

To give an idea of the growth of the bounds above in terms of n when n tends to $+\infty$, we recall that $n/(\log\log n) \ll \varphi(n) \ll n$ and that $\omega_2(n)$ has a normal value of $\log\log n$.

Now a direct application of Theorem 4.2 gives the following:

COROLLARY 8.2. *Let E be an elliptic curve without CM such that $E(k)$ has rank one. Let $\{\mathcal{D}_n\}_n$ be the family of curves of Definition 1.4. For every $n \geqslant 2$ and every point $P \in \mathcal{D}_n(k)$ we have*

$$\hat{h}(P) \leqslant 1300.518(2^{\omega_2(n)} \log 2 + 2c_6(E) + 3.01 + 2c_1(E))(2\varphi(n) + 3)^2 + 4c_2(E)$$

where the constants $c_1(E)$, $c_2(E)$ and $c_6(E)$ are defined in Table 1. Writing $P = ([a]g, [b]g)$ where a and b are integers and g is a generator of $E(k)$ we have that

$$\max(|a|, |b|) \leqslant \left(\frac{\hat{h}(P)}{\hat{h}(g)}\right)^{1/2}.$$

Proof. The bound on $\hat{h}(P)$ is a direct application of Theorem 4.2 and the bound on a and b follows from Theorem 6.3. □

9. Rational points on explicit curves

In this section we prove Theorem 1.5 from the Introduction, which gives all the rational points of several curves. The strategy here is to build many examples by keeping fixed the equation

$$x_1^n = y_2$$

or

$$\Phi_n(x_1) = y_2$$

in $\mathbb{P}_2 \times \mathbb{P}_2$ and taking many different elliptic curves E in order to define the curves $\mathcal{C}_n$ and $\mathcal{D}_n$ in E^2; see Definition 1.4. We also recall that for $i = 1, 2, 3, 4, 5$ we defined:

$$\begin{aligned}
E_1 &: y^2 = x^3 + x - 1\\
E_2 &: y^2 = x^3 - 26811x - 7320618\\
E_3 &: y^2 = x^3 - 675243x - 213578586\\
E_4 &: y^2 = x^3 - 110038419x + 12067837188462\\
E_5 &: y^2 = x^3 - 2581990371x - 50433763600098.
\end{aligned}$$

For these elliptic curves the discriminant and the j-invariant are the following:

$$\begin{aligned}
\Delta(E_1) &= -496, \quad j(E_1) = \frac{6912}{31},\\
\Delta(E_2) &= -21918062700048384, \quad j(E_2) = -\frac{979146657}{10069019},
\end{aligned} \tag{9.1}$$

$$\Delta(E_3) = -1765662163329024, \quad j(E_3) = -\frac{15641881075729}{811134},$$
$$\Delta(E_4) = -628280506977238548985268920 32,$$
$$j(E_4) = -\frac{2507136440062325499}{1068992890181390681},$$
$$\Delta(E_5) = 28306136758818947305580789 76,$$
$$j(E_5) = \frac{87452567124229040056941 7}{1300365970941935616}.$$

We recall that all CM elliptic curves have an integral j-invariant; this shows that the curves E_i are without CM for $i = 1, \dots, 5$.

Using databases of elliptic curve data such as [11] or [1], we checked that for every $i \neq 2$, E_i has no torsion points defined over $\mathbb{Q}$ and that $E_i(\mathbb{Q})$ has rank one. We also found in the tables an explicit generator g_i for $E_i(\mathbb{Q})$ and we computed $\hat{h}(g_i)$ using the function `ellheight` of PARI/GP [43] (notice that the canonical height of PARI/GP is two thirds of ours). A generator for the curve E_2, which has a conductor too big to appear in Cremona's tables, was given in [41, Example 3]. Collecting these informations we have that the generators of $E_i(\mathbb{Q})$ are:

$$g_1 = (1, 1),$$
$$g_2 = \left(\frac{290083549425751}{23921262225}, \frac{4940195839487330160124}{3699782022029625}\right),$$
$$g_3 = \left(\frac{930273}{484}, -\frac{796052583}{10648}\right),$$
$$g_4 = \left(\frac{3228005993902971489}{128791448271424}, \frac{731604286912918204872444 8529}{1461606751179427091968}\right),$$
$$g_5 = \left(\frac{-9750023890880795040300239250862047101114}{335283704622805743122062106485469025},\right.$$
$$\left.\frac{4720299314015853285822735334948965561389290542826702671986 6}{1941416291460247234773656944025320301414670590910926 25}\right),$$

where

$$\hat{h}(g_1) \geqslant 0.377, \quad \hat{h}(g_2) \geqslant 47.888, \quad \hat{h}(g_3) \geqslant 17.649, \tag{9.2}$$
$$\hat{h}(g_4) \geqslant 60.674, \quad \hat{h}(g_5) \geqslant 136.823.$$

We can now state our bounds for the five families of curves $\{\mathcal{C}_n\}_n$ in E_i^2.

THEOREM 9.1. *Let $P \in \mathcal{C}_n(\mathbb{Q}) \subseteq E^2$ where E is one of the curves E_i for $i = 1, \dots, 5$. We write P in terms of the generator g_i as $P = ([a]g_i, [b]g_i)$. Then:*

(1) *If* $E = E_1$ *we have*

$$\hat{h}(P) \leqslant 73027 \cdot n^2 + 219081 \cdot n + 164320,$$
$$|a| \leqslant \left(\frac{581115 \cdot n^2 + 1743376 \cdot n + 1307618}{2n+3}\right)^{1/2},$$
$$|b| \leqslant \left(\frac{387410 \cdot n^3 + 1162229 \cdot n^2 + 871760 \cdot n + 54}{2n+3}\right)^{1/2}.$$

(2) *If* $E = E_2$ *we have*

$$\hat{h}(P) \leqslant 311345 \cdot n^2 + 934033 \cdot n + 700566,$$
$$|a| \leqslant \left(\frac{19505 \cdot n^2 + 58515 \cdot n + 43889}{2n+3}\right)^{1/2},$$
$$|b| \leqslant \left(\frac{13004 \cdot n^3 + 39010 \cdot n^2 + 29260 \cdot n + 2}{2n+3}\right)^{1/2}.$$

(3) *If* $E = E_3$ *we have*

$$\hat{h}(P) \leqslant 373925 \cdot n^2 + 1121775 \cdot n + 841382,$$
$$|a| \leqslant \left(\frac{63561 \cdot n^2 + 190683 \cdot n + 143021}{2n+3}\right)^{1/2},$$
$$|b| \leqslant \left(\frac{42374 \cdot n^3 + 127121 \cdot n^2 + 95349 \cdot n + 5}{2n+3}\right)^{1/2}.$$

(4) *If* $E = E_4$ *we have*

$$\hat{h}(P) \leqslant 534732 \cdot n^2 + 1604195 \cdot n + 1203216,$$
$$|a| \leqslant \left(\frac{26440 \cdot n^2 + 79320 \cdot n + 59494}{2n+3}\right)^{1/2},$$
$$|b| \leqslant \left(\frac{17627 \cdot n^3 + 52880 \cdot n^2 + 39663 \cdot n + 2}{2n+3}\right)^{1/2}.$$

(5) *If* $E = E_5$ *we have*

$$\hat{h}(P) \leqslant 566995 \cdot n^2 + 1700984 \cdot n + 1275813,$$
$$|a| \leqslant \left(\frac{12433 \cdot n^2 + 37297 \cdot n + 27974}{2n+3}\right)^{1/2},$$
$$|b| \leqslant \left(\frac{8289 \cdot n^3 + 24865 \cdot n^2 + 18650 \cdot n + 1}{2n+3}\right)^{1/2}.$$

Proof. The proof is an application of Theorem 7.3. First, we need to compute all the invariants intervening in the bounds. Notice that $\deg \mathcal{C}_n$, $h_2(\mathcal{C}_n)$ are bounded in Corollary 7.1, while $\Delta(E_i)$ and $j(E_i)$ are bounded in (9.1) and a lower bound for $\hat{h}(g_i)$ is given in (9.2).

We are left to estimate $h_{\mathcal{W}}(E_i) = h_W(1 : A_i^{1/2} : B_i^{1/3})$ as defined in (2.2). We obtain:

$$h_{\mathcal{W}}(E_1) = 0, \quad h_{\mathcal{W}}(E_2) \leqslant 5.269, \quad h_{\mathcal{W}}(E_3) \leqslant 6.712,$$
$$h_{\mathcal{W}}(E_4) \leqslant 10.041, \quad h_{\mathcal{W}}(E_5) \leqslant 10.836.$$

In addition, by Table 1 we get:

$$c_1(E_1) \leqslant 4.709, \quad c_2(E_1) \leqslant 2.423, \quad c_3(E_1) \leqslant 2.037, \quad c_4(E_1) \leqslant 2.31,$$
$$c_1(E_2) \leqslant 20.515, \quad c_2(E_2) \leqslant 10.33, \quad c_3(E_2) \leqslant 4.587, \quad c_4(E_2) \leqslant 5.353,$$
$$c_1(E_3) \leqslant 24.843, \quad c_2(E_3) \leqslant 12.494, \quad c_3(E_3) \leqslant 5.394, \quad c_4(E_3) \leqslant 6.563,$$
$$c_1(E_4) \leqslant 34.83, \quad c_2(E_4) \leqslant 17.487, \quad c_3(E_4) \leqslant 6.667, \quad c_4(E_4) \leqslant 8.336,$$
$$c_1(E_5) \leqslant 37.216, \quad c_2(E_5) \leqslant 18.68, \quad c_3(E_5) \leqslant 7.456, \quad c_4(E_5) \leqslant 9.656,$$

and

$$c_5(E_1) \leqslant 4.159, \quad c_6(E_1) \leqslant 0.805, \quad c_7(E_1) \leqslant 0.55,$$
$$c_5(E_2) \leqslant 9.428, \quad c_6(E_2) \leqslant 7.905, \quad c_7(E_2) \leqslant 7.904,$$
$$c_5(E_3) \leqslant 10.871, \quad c_6(E_3) \leqslant 9.592, \quad c_7(E_3) \leqslant 9.592,$$
$$c_5(E_4) \leqslant 14.2, \quad c_6(E_4) \leqslant 15.061, \quad c_7(E_4) \leqslant 15.061,$$
$$c_5(E_5) \leqslant 14.995, \quad c_6(E_5) \leqslant 15.776, \quad c_7(E_5) \leqslant 15.776.$$

We can now replace all the above values in the formulae of Theorem 7.3 and obtain the bounds in our statement. □

We have an analogous result for the five families of curves $\mathcal{D}_n$ in E_i^2, which we write for simplicity for the subfamilies consisting of all elements for which the index n is a prime.

THEOREM 9.2. *Let $P \in \mathcal{D}_n(\mathbb{Q}) \subseteq E^2$ where E is one of the curves E_i for $i = 1, \ldots, 5$. We write P in terms of the generator g_i as $P = ([a]g_i, [b]g_i)$. Assume that n is a prime number. Then:*

(1) *If $E = E_1$ we have*

$$\hat{h}(P) \leqslant 80239n^2 + 80239n + 20070,$$
$$\max(|a|, |b|) \leqslant \sqrt{212834n^2 + 212834n + 53235}.$$

(2) *If* $E = E_2$ *we have*

$$\hat{h}(P) \leqslant 318556n^2 + 318556n + 79681,$$
$$\max(|a|, |b|) \leqslant \sqrt{6653n^2 + 6653n + 1664}.$$

(3) *If* $E = E_3$ *we have*

$$\hat{h}(P) \leqslant 381137n^2 + 381137n + 95335,$$
$$\max(|a|, |b|) \leqslant \sqrt{21596n^2 + 21596n + 5401}.$$

(4) *If* $E = E_4$ *we have*

$$\hat{h}(P) \leqslant 541943n^2 + 541943n + 135556,$$
$$\max(|a|, |b|) \leqslant \sqrt{8933n^2 + 8933n + 2235}.$$

(5) *If* $E = E_5$ *we have*

$$\hat{h}(P) \leqslant 574207n^2 + 574207n + 143627,$$
$$\max(|a|, |b|) \leqslant \sqrt{4197n^2 + 4197n + 1050}.$$

Proof. These bounds are a direct application of Corollary 8.2. The relevant numerical constants are already listed in the proof of Theorem 9.1. □

With these sharp estimates we are ready to implement the computer search up to the computed bounds for the rational points on our curves, and so to prove Theorem 1.5.

To perform the computer search, we used the PARI/GP [**43**] computer algebra system, an open source program freely available at http://pari.math.u-bordeaux.fr

We first tried to implement a naive algorithm that performs the multiples of the points g_i on the elliptic curve using PARI's implementation of the exact arithmetic of the elliptic curve over the rationals. This has proved far too time-consuming and was only done for $n = 1$.

Then we used a more efficient algorithm pointed out by Joseph H. Silverman. The idea is to identify the elliptic curve E with a quotient $\mathbb{C}/\Lambda$ and see the multiplication by a on E as induced by the multiplication by a in $\mathbb{C}$. This algorithm is quite fast and capable of performing the computations up to about $n = 50$.

The algorithm that we used in our final computation is due to K. Belabas and uses a sieving technique. It is very general and it can be applied to any of the

curves of Theorem 6.3 when $k = \mathbb{Q}$, although we performed the computations only for curves belonging to the families $\mathcal{C}_n$ and $\mathcal{D}_n$.

The idea is that, in order to test which of a finite but very big number of points actually lie on the curve, we test when this happens modulo many big primes.

We are very thankful to K. Belabas for providing us the sieving algorithm presented in the following proof.

Proof of Theorem 1.5. Theorem 1.5 is now a consequence of Theorems 9.1 and 9.2 and an extensive computer search.

For each of the curves E_i and for each n, Theorem 9.1 gives us upper bounds for the integers a, b such that $([a]g_i, [b]g_i) \in \mathcal{C}_n$, therefore we only need to check which of finitely many points lie on the curve $\mathcal{C}_n$ (respectively $\mathcal{D}_n$).

Even though, as remarked in the Introduction, the computations for large n are superseded by the results in Section A.4 of the appendix, we think it is worthwhile, for future applications, to give some details on how they were performed. In particular, we present here the PARI code used to implement Belabas' algorithm in the general case for curves $\mathcal{C}$ as in Theorem 6.3, cut in E^2 by the additional equation $p(x_1) = y_2$, with $p(X)$ a polynomial in $\mathbb{Z}[X]$. The algorithm can possibly be adapted to curves of different shapes.

We fix the polynomial $p(X)$, called `Pol(X)` in the code, of degree n and we start by initializing the following variables

```
A,B,Ba,g,ntest
```

where `A` and `B` are the coefficients of the Weierstrass model of E, `Ba` is the ceiling of the bound on $|a|$ obtained for the chosen polynomial $p(X)$, `g` is the generator of $E(\mathbb{Q})$ and `ntest` is a parameter used to decide when to stop the sieving process.

Then we define the following program, that we indent here for readability

```
0   E = ellinit([A,B]);
1   D=abs(E.disc);
2   Sievea() =
3   {
4     p = nextprime(Ba);
5     L = [1..Ba];
6     cnt = 1;
7     while(1,
8       if(D%p==0,next);
9       if(denominator(g[1])%p==0,next);
10      oldnL = #L;
11      ag = [0];
12      Ep = ellinit(E, p);
13      Lp = List([]);
14      for (a = 1, Ba,
15        ag = elladd(Ep, ag, g);
16        if (#ag == 1, listput(Lp, a); next);
```

```
17        x = ag[1];
18        xp = Mod(x,p);
19        if(polrootsmod('X^3 + A*'X + B - Pol(xp)^2, p), listput(Lp, a)) ;
20      );
21      listsort(Lp);
22      L = setintersect(L, Vec(Lp));
23      if (#L == oldnL, cnt++, cnt = 0);
24      if (#L == 0 || cnt > ntest, break);
25      p = nextprime(p+1);
26    );
27    printf("L=%s\n",L);
28  }
```

The core of the algorithm is the `while` loop in line 7. This loop iterates over the prime `p`, which is initialized in line 4 to a value bigger than `Ba`. At each iteration the algorithm takes the list `L`, which initially contains all positive values of a up to the bound `Ba`, and checks for which of these values there exists a point $([a]g, [b]g)$ on the curve $\mathcal{C}_n$ reduced modulo `p`. This check is done in the `for` loop at line 14. The a that correspond to points modulo `p` are stored in the list `Lp` and the values of a that do not correspond to a point are removed from the list `L` at line 22. The algorithm then changes the prime number `p` to the next one, and the loop starts again. The check at lines 8 and 9 ensures that the primes of bad reduction for the curve `E` and those that divide the denominator of the generator are discarded. The algorithm keeps sieving through the list `L` until either the list becomes empty, which proves that there are no rational points, or `ntest` iterations pass without any value of a being discarded. When this happens the program outputs these values of a, which are candidate solutions and need to be investigated further.

In our explicit examples we found that setting `ntest` to 25 was enough, and no candidate solution was ever found other than those arising from rational points on $E_1 \times E_1$. □

The variable `Ba`, and hence the length of the list `L` in line 5, is directly proportional to the square root of the height of the coefficients of the Weierstrass model of E and inversely proportional to the square root of the height of the generator of $E(\mathbb{Q})$, which explains the speed improvement when the generator has a big height compared to the coefficients.

We remark that with a simple modification this algorithm can be made deterministic by stopping the iteration in a suitably chosen way depending on the degree and the coefficients of the curve. However this increases, in general, the running time compared to a good heuristic choice of the parameter `ntest`.

When adapting the algorithm to other examples, if for a certain choice of `ntest` the above algorithm returns a list of possible values, one can either increase `ntest` or directly check the values with the floating point algorithm.

We finally notice that for our method it is not necessary to know *a priori* a generator g of $E(\mathbb{Q})$. Indeed we can argue as follows. Theorem 6.3 gives the bound $\hat{h}(P) \leqslant D$ for any rational point on $\mathcal{C}$. Thus we only need to search for a generator g of $E(\mathbb{Q})$ such that $\hat{h}(g) \leqslant \hat{h}(P)$, otherwise $\mathcal{C}(\mathbb{Q})$ is trivially empty. To this purpose, one can use a suitable search algorithm for generators of height at most D on elliptic curves of rank one, as described in [**41**]. For instance with Silverman's Canonical Height Search Algorithm finding a generator of $E(\mathbb{Q})$ takes about $O(\sqrt{N_E} + D)$, where N_E is the conductor of E. This is also one of the few algorithms that can deal with curves of high conductor.

Acknowledgements

We are indebted to K. Belabas for writing the algorithm to conclude the proof of Theorem 1.5 and for his kind answers on some technical aspects of PARI/GP. We are thankful to M. Stoll for his useful remarks which helped us to improve the paper and for his nice appendix. We warmly thank J. H. Silverman for his useful suggestions and for his interest in our work. We are grateful to P. Philippon for answering some questions on the comparison of several height functions. We also thank Ö. Imamoglu for her comments on an earlier version of this paper. We finally thank the referee for several useful comments and for his/her work. S. Checcoli's work has been funded by the ANR project Gardio 14-CE25-0015. E. Viada thanks the FNS (Fonds National Suisse) Project PP00P2-123262/1 for the financial support.

Appendix A.

M. Stoll[1]

As mentioned in the Introduction, the approach taken in the main paper applies in basically the same setting as Demjanenko's method. The first goal of this appendix is to provide a comparison between the two approaches, first in general terms, and then more concretely for a family of curves of genus 2 to which Demjanenko's approach can be applied quite easily.

In the main paper, the bound obtained is used to find explicitly the set of rational points on certain curves $\mathcal{C}_n(E)$ and $\mathcal{D}_n(E)$ sitting in $E \times E$ for certain elliptic curves E, where the parameter n ranges up to an upper bound depending on E. The second goal of this appendix is to complete the analysis of these examples by determining the set of rational points on the curves $\mathcal{C}_n(E)$ and $\mathcal{D}_n(E)$ (for the five curves E considered there) for *all* n. The additional ingredient we use

[1] Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany. Michael.Stoll@uni-bayreuth.de. WWW: http://www.computeralgebra.uni-bayreuth.de.

is an analysis of the ℓ-adic behaviour of points on the curves close to the origin. This analysis leads to a fast-growing lower bound for the height of a point $(P_1, P_2) \in \mathcal{C}(\mathbb{Q})$ that is not the origin (O, O) and is also not a pair of integral points on E. Since this lower bound grows faster than the upper bound, this implies that all rational points on $\mathcal{C}$ distinct from (O, O) must be pairs of integral points as soon as n is large enough. Since the number of integral points on E is finite, this result shows that $\mathcal{C}_n(E)(\mathbb{Q})$ and $\mathcal{D}_n(E)(\mathbb{Q})$ are contained in a fixed finite set for all sufficiently large n. It is then an easy matter to determine which of these finitely many points are on which of the curves. This approach can be used more generally when the curve $\mathcal{C}$ is given by an equation of the form $F_1(x_1, y_1) = F_2(x_2, y_2)$ with polynomials F_1, F_2 such that the degrees of $F_1(x, y)$ and $F_2(x, y)$, considered as rational functions on E, differ. If the ratio of the degrees is sufficiently large compared to the height and degree of $\mathcal{C}$, then all rational points on $\mathcal{C}$ distinct from (O, O) must be pairs of S-integral points on E (for an explicit finite set S of primes), of which there are only finitely many.

A.1. Comparison with Demjanenko's method. The setting of Demjanenko's method is a curve $\mathcal{C}$, which we take to be defined over $\overline{\mathbb{Q}}$, that allows N independent morphisms $\phi_j : \mathcal{C} \to E$, $j = 1, 2, \ldots, N$, to a fixed elliptic curve E also defined over $\overline{\mathbb{Q}}$. 'Independent' here means that no nontrivial integral linear combination of the ϕ_j is constant. This is equivalent to saying that the image of $\mathcal{C}$ in E^N under the product of the ϕ_j is transverse, and so this setting is essentially the same as considering a transverse curve in E^N as is done in the main paper.

We now paraphrase Demjanenko's method [13] in the case $N = 2$ as applied in [19, 24, 25]. The description below is close to Silverman's in [39]. Consider a curve $\mathcal{C}$ (of genus $\geqslant 2$) over $\overline{\mathbb{Q}}$ with two independent morphisms $\phi_1, \phi_2 : \mathcal{C} \to E$ to an elliptic curve E defined over $\overline{\mathbb{Q}}$. The independence of the morphisms implies that the quadratic form

$$\mathbb{Z}^2 \ni (\alpha_1, \alpha_2) \longmapsto \deg(\alpha_1\phi_1 + \alpha_2\phi_2)$$

is positive definite. Fix a height h on $\mathcal{C}$, which is scaled so that $\hat{h}(\phi_j(P)) = (\deg \phi_j + o(1))h(P)$ for $P \in \mathcal{C}(\overline{\mathbb{Q}})$ as $h(P) \to \infty$. Then there are constants c_j, depending on $\mathcal{C}$, ϕ_1, ϕ_2 and h, but not on P, such that for all $P \in \mathcal{C}(\overline{\mathbb{Q}})$ with $h(P) \geqslant 1$ (see [22, Theorem B.5.9])

$$\begin{aligned}
|(\deg \phi_1)h(P) - \hat{h}(\phi_1(P))| &\leqslant c_1\sqrt{h(P)},\\
|(\deg \phi_2)h(P) - \hat{h}(\phi_2(P))| &\leqslant c_2\sqrt{h(P)},\\
|(\deg(\phi_1 + \phi_2))h(P) - \hat{h}(\phi_1(P) + \phi_2(P))| &\leqslant c_3\sqrt{h(P)}.
\end{aligned}$$

We write $\langle P_1, P_2\rangle = \frac{1}{2}(\hat{h}(P_1+P_2) - \hat{h}(P_1) - \hat{h}(P_2))$ for the height pairing and similarly $\langle \phi_1, \phi_2\rangle = \frac{1}{2}(\deg(\phi_1+\phi_2) - \deg\phi_1 - \deg\phi_2)$. Then we deduce that

$$|\langle \phi_1, \phi_2\rangle h(P) - \langle \phi_1(P), \phi_2(P)\rangle| \leqslant c_4\sqrt{h(P)}$$

with $c_4 = \frac{1}{2}(c_1+c_2+c_3)$. This gives that

$$\deg(\alpha_1\phi_2+\alpha_2\phi_2)h(P) - \hat{h}(\alpha_1\phi_1(P)+\alpha_2\phi_2(P)) \leqslant (\alpha_1^2 c_1 + 2|\alpha_1\alpha_2|c_4 + \alpha_2^2 c_2)\sqrt{h(P)}$$

and so (still for $h(P) \geqslant 1$)

$$h(P) \leqslant \frac{\hat{h}(\alpha_1\phi_1(P)+\alpha_2\phi_2(P))}{\deg(\alpha_1\phi_2+\alpha_2\phi_2)} + \gamma(\alpha_1,\alpha_2)\sqrt{h(P)}, \tag{A.1}$$

where

$$\gamma(\alpha_1,\alpha_2) = \frac{\alpha_1^2 c_1 + 2|\alpha_1\alpha_2|c_4 + \alpha_2^2 c_2}{\alpha_1^2(\deg\phi_1) + 2\alpha_1\alpha_2\langle\phi_1,\phi_2\rangle + \alpha_2^2(\deg\phi_2)}.$$

Since the denominator is positive definite, there is a uniform upper bound, for example

$$\gamma(\alpha_1,\alpha_2) \leqslant \gamma := \frac{2\max\{c_1,c_2\} + c_3/2}{\lambda},$$

where λ is the smaller eigenvalue of the matrix $(\langle\phi_i,\phi_j\rangle)_{1\leqslant i,j\leqslant 2}$.

Now let $P \in \mathcal{C}(\overline{\mathbb{Q}})$ be such that $\phi_1(P)$ and $\phi_2(P)$ generate a subgroup of rank 1 in E. Then there are $\alpha_1, \alpha_2 \in \mathbb{Z}$, not both zero, such that $\alpha_1\phi_1(P)+\alpha_2\phi_2(P) = O$. Then from (A.1) we obtain the bound $h(P) \leqslant \max\{1, \gamma^2\}$. In particular, if $\mathcal{C}$, E and the morphisms are defined over some number field K and $E(K)$ has rank 1, then $h(P) \leqslant \max\{1,\gamma^2\}$ for all K-rational points P on $\mathcal{C}$. (For this application it is sufficient to use bounds c_j that are only valid for K-rational points.)

We get a better bound when (writing $\phi_3 = \phi_1+\phi_2$) suitable positive multiples of the pulled-back divisors $\phi_j^*(O)$ are linearly equivalent, for $j = 1,2,3$. We can then take the height h so that

$$(\deg\phi_j)h(P) = 3h_{\phi_j^*(O)}(P) + O(1) = 3h_O(\phi_j(P)) + O(1) = \hat{h}(\phi_j(P)) + O(1),$$

where h_D denotes a height associated to the divisor D, compare [22, Theorem B.3.2]. Then everything we did above is valid when replacing $\sqrt{h(P)}$ by 1 throughout; in particular, the final bound is then just $h(P) \leqslant \max\{1,\gamma\}$.

One situation where this applies is when $\mathcal{C}$ is hyperelliptic. In this case, after translation by a constant point in E, any morphism $\phi\colon \mathcal{C} \to E$ descends to a

morphism $\tilde{\phi}\colon \mathbb{P}^1 \to \mathbb{P}^1$ on x-coordinates, so that we have a commutative diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\phi} & E \\ {\scriptstyle \pi_{\mathcal{C}}}\downarrow & & \downarrow{\scriptstyle \pi_E} \\ \mathbb{P}^1 & \xrightarrow{\tilde{\phi}} & \mathbb{P}^1 \end{array}$$

where $\pi_{\mathcal{C}}$ and π_E are the x-coordinate morphisms. Then

$$2\phi^*(O) = \phi^*(2O) = \phi^*\pi_E^*(\infty) = \pi_{\mathcal{C}}^*\tilde{\phi}^*(\infty) \sim (\deg\phi)\pi_{\mathcal{C}}^*(\infty)$$

and so $2\phi^*(O)$ is linearly equivalent to a multiple of $\pi_{\mathcal{C}}^*(\infty)$ for every ϕ.

We can expect c_j to be of the order of $(\deg\phi_j)h(\mathcal{C})$ (with $\phi_3 = \phi_1 + \phi_2$) with some notion of height for $\mathcal{C}$. The resulting height bound will then have order of magnitude $h(\mathcal{C})$ in the special case just discussed (the contribution of the degrees will cancel, since the degrees also occur in the denominator of $\gamma(\alpha_1, \alpha_2)$). This will usually be better than the bound obtained in the main paper; see for example the comparison in Section A.2. In the general case, we obtain a bound that has order of magnitude $h(\mathcal{C})^2$; this is to be compared with $\deg(\mathcal{C})(h(\mathcal{C}) + \deg(\mathcal{C}))$ for the bound obtained in the main paper (which likely has a larger constant in front).

If one starts with a concrete curve $\mathcal{C}$ with two morphisms to E, then it will usually not be very hard to find the constants needed to get a bound as derived in this section, in particular when $\mathcal{C}$ is hyperelliptic. On the other hand, starting from a curve $\mathcal{C}$ given as a subvariety of $E \times E$ by some equation, one first has to fix a suitable height on $\mathcal{C}$. It appears natural to take the height used previously, namely $\hat{h}(P_1) + \hat{h}(P_2)$, suitably scaled, which means that we divide by the sum of the degrees of the two morphisms to E. We then have to bound

$$\begin{aligned} &(\deg\phi_2)\hat{h}(P_1) - (\deg\phi_1)\hat{h}(P_2) \\ &\quad \text{and (say)} \quad (\deg(\phi_1+\phi_2))\hat{h}(P_1) - (\deg\phi_1)\hat{h}(P_1+P_2) \end{aligned}$$

to obtain the necessary constants. This may be not so easy in general. So in this situation, the method of Checcoli, Veneziano and Viada produces a bound that is easy to compute, but is likely to be larger than what we would obtain from Demjanenko's method. One possible source for the comparative weakness of the bound is that the Arithmetic Bézout Theorem bounds the *sum* of the heights of *all* points in the fibre of $\alpha_1\phi_1 + \alpha_2\phi_2\colon \mathcal{C} \to E$ that contains P, and this sum (with potentially many terms) is used to bound a single summand.

A.2. An application to curves of genus 2. We illustrate the comparison between the two approaches by considering a family of curves of genus 2 whose

members have two independent morphisms to the same elliptic curve. This is a setting where Demjanenko's method can be applied fairly easily (this has been done in [25]) and with constant height difference bounds, which gives Demjanenko's approach a considerable advantage.

A curve of genus 2 over $\mathbb{Q}$ is given by an affine equation

$$\mathcal{C}\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0$$

with $f_0, \ldots, f_6 \in \mathbb{Z}$ and such that the right hand side has degree at least 5 and has no multiple roots. Assume that $\mathcal{C}$ has two morphisms ϕ_1, ϕ_2 to the same elliptic curve E. The simplest case is when both ϕ_1 and ϕ_2 have degree 2. If $\mathcal{C}$ is a double cover of E, then $\mathcal{C}$ has an 'extra involution' σ, which is an automorphism of order 2 that is not the hyperelliptic involution ι. One can check that in this situation σ has two fixed points with the same x-coordinate, and the same is true for $\sigma\iota$. (The other possibility would be that σ and $\sigma\iota$ have the same two Weierstrass points as fixed points, but this would force σ to be of order 4.) These two x-coordinates are then rational (we assume that $\mathcal{C} \to E$ and hence σ is defined over $\mathbb{Q}$), and so we can assume that they are 0 and ∞; then σ is given by $(x, y) \mapsto (-x, y)$ and $\sigma\iota$ is $(x, y) \mapsto (-x, -y)$. The equation of $\mathcal{C}$ then has the form

$$y^2 = ax^6 + bx^4 + cx^2 + d$$

and the quotient elliptic curve $\mathcal{C}/\langle\sigma\rangle$ is $E_1\colon y^2 = x^3 + bx^2 + acx + a^2d$, whereas the quotient $\mathcal{C}/\langle\sigma\iota\rangle$ is $E_2\colon y^2 = x^3 + cx^2 + dbx + d^2a$. In the simplest situation, $E_2 = E_1$, so $b = c$ and $a = d$. (In general, E_2 can be isomorphic to E_1 without being equal to it.) So we now consider the curve

$$\mathcal{C}\colon y^2 = ax^6 + bx^4 + bx^2 + a,$$

where $a, b \in \mathbb{Z}$. We assume that $a \neq 0, -b, b/3$ to ensure that $\mathcal{C}$ has genus 2. A Weierstrass equation for $E = E_1 = E_2$ is

$$y^2 = x^3 + bx^2 + abx + a^3.$$

To apply the results of the main paper, we transform this into the short Weierstrass equation

$$E\colon y^2 = x^3 + 27b(3a - b)x + 27(27a^3 - 9ab^2 + 2b^3).$$

(We remark that this increases the height of the equation defining E, which leads to a final bound that is worse than what could be obtained by working with the 'long' equation directly.) We can then embed $\mathcal{C} \hookrightarrow E \times E$ via

$$(x, y) \longmapsto ((9ax^2 + 3b, 27ay), (9ax^{-2} + 3b, 27ax^{-3}y)).$$

Its image is the projective closure of the affine curve given inside $E \times E$ by

$$(x_1 - 3b)(x_2 - 3b) = 81a^2.$$

The image $\mathcal{C}'$ of $\mathcal{C}$ under the composition of morphisms

$$\mathcal{C} \hookrightarrow E \times E \subseteq \mathbb{P}^2 \times \mathbb{P}^2 \xrightarrow{\text{Segre}} \mathbb{P}^8$$

has degree 12.

We need a bound on the height $h_2(\mathcal{C}')$. Setting $\xi_j = (x_j - 3b)/(9a)$, we have $\xi_1\xi_2 = 1$. Taking $\xi_1 = \zeta$ and $\xi_2 = \zeta^{-1}$, where ζ is a root of unity, we get $x_1 = 9a\zeta + 3b$, $x_2 = 9a\zeta^{-1} + 3b$, and y_1, y_2 are square roots of $(27a)^2(a\zeta^{\pm 3} + b\zeta^{\pm 2} + b\zeta^{\pm 1} + a)$. Using that a and b are rational integers, which implies that the contributions to the height coming from non-Archimedean places vanish, and the triangle inequality to bound the contributions from the Archimedean places shows that there are infinitely many points $P = (P_1, P_2)$ defined over $\overline{\mathbb{Q}}$ on the image of $\mathcal{C}$ in $E \times E$ such that

$$h_2(P) = h_2(P_1) + h_2(P_2) \leqslant \log(1456a^2(|a| + |b|) + (9|a| + 3|b|)^2 + 1).$$

So by Zhang's inequality, we find that

$$h_2(\mathcal{C}') \leqslant 24\log(1456a^2(|a|+|b|)+(9|a|+3|b|)^2+1) \leqslant 24\log 3057 + 72\log m, \tag{A.2}$$

where $m = \max\{|a|, |b|\}$.

COROLLARY A.1. *Let $\mathcal{C}\colon y^2 = ax^6 + bx^4 + bx^2 + a$ with $a, b \in \mathbb{Z}$, $a \neq 0, -b, b/3$, and let E be as above. Assume that $E(\mathbb{Q})$ has rank 1, and let $P_0 \in E(\mathbb{Q})$ generate the free part of $E(\mathbb{Q})$. For a point $P \in \mathcal{C}(\mathbb{Q})$, write $\phi_1(P) = n_1P_0 + T_1$, $\phi_2(P) = n_2P_0 + T_2$ with $n_1, n_2 \in \mathbb{Z}$ and $T_1, T_2 \in E(\mathbb{Q})_{\text{tors}}$. Then*

$$\begin{aligned}\min\{|n_1|, |n_2|\} &\leqslant \sqrt{\frac{433.506h_2(\mathcal{C}') + 31311.3 + 20808.3c_1(E) + 2c_2(E)}{\hat{h}(P_0)}} \\ &\leqslant \sqrt{\frac{358956.08 + 93638.80\log m}{\hat{h}(P_0)}},\end{aligned}$$

where $m = \max\{|a|, |b|\}$.

Proof. From Theorem 4.2 and $\deg(\mathcal{C}') = 12$, we obtain the bound

$$\hat{h}(P) = \hat{h}(\phi_1(P)) + \hat{h}(\phi_2(P)) \leqslant 72.251(12h_2(\mathcal{C}') + 144(6.019 + 4c_1(E))) + 4c_2(E)$$

for points $P \in \mathcal{C}(\mathbb{Q})$, where $c_1(E)$, $c_2(E)$ are as in Table 1. Since $h_{\mathcal{W}}(E) \leqslant \frac{1}{2}\log 108 + \log m$, we have

$$c_1(E) \leqslant 11.733 + 3\log m \quad \text{and} \quad c_2(E) \leqslant 5.939 + \tfrac{3}{2}\log m,$$

which using (A.2) gives

$$\hat{h}(P) \leqslant 717912.16 + 187277.60 \log m.$$

Also, $\hat{h}(P) = (n_1^2 + n_2^2)\hat{h}(P_0)$, so $\min\{|n_1|, |n_2|\} \leqslant \sqrt{\hat{h}(P)/(2\hat{h}(P_0))}$, which together with the bound for $\hat{h}(P)$ gives the statement. □

The bound in the theorem was chosen to be in a simple form. In concrete cases, one will use the more precise bound in terms of a and b in (A.2) and also better bounds on $c_1(E)$ and $c_2(E)$.

We compare this with the bound obtained in [**25**]. There curves with $a = 1$ are studied, where b (denoted t in [**25**]) can be rational. Then (if $E(\mathbb{Q})$ has rank 1) they show that for all $P \in \mathcal{C}(\mathbb{Q})$

$$h_W(x(P)) \leqslant \tfrac{7}{2}h(b) + \tfrac{1}{2}\log 81468 \leqslant \tfrac{7}{2}h(b) + 5.654.$$

Since the x-coordinates of the images of P on E are given by $9x(P)^{\pm 2} + 3b$, this translates into

$$\min\{|n_1|, |n_2|\} \leqslant \sqrt{\frac{12h(b) + 22.946 + 3c_3(E)}{\hat{h}(P_0)}}. \tag{A.3}$$

This is considerably smaller than the bound given in Corollary A.1.

EXAMPLE A.2. For a concrete example, consider the curve with $a = b = 1$:

$$\mathcal{C}\colon y^2 = x^6 + x^4 + x^2 + 1.$$

Then E is the curve 128a1 in the Cremona database [**11**] (and [**1**, 128.a2]), and $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. We have $\hat{h}(P_0) > 0.6485$. The bound in the theorem above (using the bound for $h_2(\mathcal{C}')$ in (A.2) and the bounds for $c_1(E)$ and $c_2(E)$ from Table 1) gives

$$\min\{|n_1|, |n_2|\} \leqslant 728.$$

For comparison, the bound in (A.3) gives

$$\min\{|n_1|, |n_2|\} \leqslant 7.$$

From this, it is easy to find the set of rational points on $\mathcal{C}$:

$$\mathcal{C}(\mathbb{Q}) = \{\infty_+, \infty_-, (-1, \pm 2), (0, \pm 1), (1, \pm 2)\}.$$

For an example with a larger b, consider $b = 1003$ (this is the smallest $b \geqslant 1000$ such that $E(\mathbb{Q})$ has rank 1). Corollary A.1 gives a bound of 354 for the minimum of $|n_1|$ and $|n_2|$, whereas (A.3) gives a bound of 4.

The fairly large discrepancy (roughly a factor 100 for the bound on n_1 and n_2 and a factor 10^4 for the bound on the height) between the bounds obtained by the method of the main paper and by Demjanenko's method suggests that it might be possible to obtain better bounds from the approach taken by Checcoli, Veneziano and Viada than given in Theorem 4.2. In any case, the comparison in this specific case is perhaps a bit unfair, since the setting is rather advantageous for an application of Demjanenko's method.

A.3. A lower bound for nonintegral points. Let E be an elliptic curve over $\mathbb{Q}$ of rank 1 given by a Weierstrass equation with integral coefficients. In this section, we consider a curve $\mathcal{C} \subseteq E \times E$ that is given by an affine equation of the form

$$F_1(x_1, y_1) = F_2(x_2, y_2)$$

(where (x_1, y_1) are the affine coordinates on the first and (x_2, y_2) on the second factor E) with polynomials $F_1, F_2 \in \mathbb{Z}[x, y]$. Using the equation of E, we can assume that $F_j(x, y) = f_j(x) + g_j(x)y$ with univariate polynomials $f_j, g_j \in \mathbb{Z}[x]$. Note that F_j is a rational function on E whose only pole is at the origin O and that $d_j := \deg F_j = \max\{2 \deg f_j, 3 + 2 \deg g_j\}$. The *leading coefficient* of F_j is the coefficient of the term of largest degree present in F_j. We also require in the following that d_1 is strictly greater than d_2. Our goal in this section is to obtain a *lower* bound on the height of a point $P \in \mathcal{C}(\mathbb{Q})$.

Let ℓ be a prime number. For our purposes the *kernel of reduction* $K_\ell(E)$ of E at ℓ is the subgroup of $E(\mathbb{Q}_\ell)$ consisting of points reducing mod ℓ to the origin on the model of E defined by the given equation. (This may differ from the more usual notion, which refers to a minimal model of E, when E has bad reduction at ℓ.) We write v_ℓ for the (additive) ℓ-adic valuation on $\mathbb{Q}_\ell$, normalized so that $v_\ell(\ell) = 1$.

We let $t := x/y$ be the standard uniformizer of E at O. Then if a point $P \in E(\mathbb{Q}_\ell)$ is in the kernel of reduction, we have $v_\ell(t(P)) > 0$, and standard properties of formal groups imply when ℓ is odd or when $\ell = 2$ and E is given by an integral Weierstrass equation without 'mixed terms' y or xy that

$$v_\ell(t(nP)) = v_\ell(t(P)) + v_\ell(n). \tag{A.4}$$

Let S be a finite set of primes containing the primes dividing the leading coefficients of F_1 and F_2 and also the prime 2 if the equation defining E contains mixed terms. Then for a prime $\ell \notin S$ and a point $P \in E(\mathbb{Q}_\ell)$, we have that

$$P \in K_\ell(E) \iff v_\ell(F_j(P)) < 0, \tag{A.5}$$

and in this case we have the relation

$$v_\ell(F_j(P)) = -d_j v_\ell(t(P)). \tag{A.6}$$

We denote the ring of S-integers by $\mathbb{Z}_S$.

THEOREM A.3. *Consider E, $\mathcal{C}$ and S as above (with $d_1 > d_2$). Set*

$$\lambda = \hat{h}(P_0) \min\{a_\ell^2 \ell^{2\lceil d_1/d_2 \rceil - 2} : \ell \notin S\},$$

where P_0 is a generator of the free part of $E(\mathbb{Q})$ and a_ℓ is the smallest positive integer such that $a_\ell P_0 \in K_\ell(E) + E(\mathbb{Q})_{\text{tors}}$. Then

$$\mathcal{C}(\mathbb{Q}) \subseteq \{(O, O)\} \cup (E(\mathbb{Z}_S) \times E(\mathbb{Z}_S)) \cup \{P \in E(\mathbb{Q}) \times E(\mathbb{Q}) : \hat{h}(P) \geqslant \lambda\}.$$

Proof. Assume $P = (P_1, P_2) \in \mathcal{C}(\mathbb{Q})$, but $P \neq (O, O)$ and $P \notin E(\mathbb{Z}_S) \times E(\mathbb{Z}_S)$. Since O is the only pole of F_1 and F_2, we have $P_1 = O \iff P_2 = O$, but this case is excluded. By assumption, one of P_1 and P_2 is not S-integral. If P_1 is not S-integral, then there is a prime $\ell \notin S$ such that $P_1 \in K_\ell(E)$. By (A.5), this implies that $P_2 \in K_\ell(E)$ as well. If P_2 is not S-integral, the same argument applies. So P_1 and P_2 are both nontrivial points in $K_\ell(E) \cap E(\mathbb{Q})$. Then by (A.6) we must have

$$d_1 v_\ell(t(P_1)) = -v_\ell(F_1(P_1)) = -v_\ell(F_2(P_2)) = d_2 v_\ell(t(P_2)).$$

Now let $P' \in E(\mathbb{Q})$ be a generator of the intersection $E(\mathbb{Q}) \cap K_\ell(E)$ (this group is isomorphic to $\mathbb{Z}$ when $E(\mathbb{Q})$ has rank 1; recall that the kernel of reduction does not contain nontrivial elements of finite order when ℓ is odd; $\ell = 2$ is taken care of by our choice of S). We can then write $P_1 = n_1 P'$, $P_2 = n_2 P'$ with $n_1, n_2 \in \mathbb{Z}$, and we have by (A.4) that

$$v_\ell(t(P')) + v_\ell(n_1) = v_\ell(t(P_1)) \quad \text{and} \quad v_\ell(t(P')) + v_\ell(n_2) = v_\ell(t(P_2)).$$

Combining this with the relation between $v_\ell(t(P_1))$ and $v_\ell(t(P_2))$, we obtain

$$v_\ell(n_2) = v_\ell(t(P_2)) - v_\ell(t(P')) = \frac{d_1 - d_2}{d_2} v_\ell(t(P')) + \frac{d_1}{d_2} v_\ell(n_1) \geqslant \frac{d_1 - d_2}{d_2},$$

since $v_\ell(n_1) \geqslant 0$ and $v_\ell(t(P')) \geqslant 1$. It follows that $n_2 \geqslant \ell^{\lceil d_1/d_2 \rceil - 1}$. We have that $P' = \pm a_\ell P_0 + T_\ell$ with $T_\ell \in E(\mathbb{Q})_{\text{tors}}$, and so

$$\hat{h}(P) = \hat{h}(P_1) + \hat{h}(P_2) = a_\ell^2(n_1^2 + n_2^2)\hat{h}(P_0) \geqslant a_\ell^2 \ell^{2\lceil d_1/d_2 \rceil - 2}\hat{h}(P_0) \geqslant \lambda,$$

which was to be shown. □

We can combine these results with the upper bound from Theorem 4.2. If this upper bound is smaller than λ, then it follows that

$$\mathcal{C}(\mathbb{Q}) \subseteq \{(O, O)\} \cup (E(\mathbb{Z}_S) \times E(\mathbb{Z}_S)).$$

Note that $E(\mathbb{Z}_S)$ is a finite set that can easily be determined in practice once a generator P_0 of the free part of $E(\mathbb{Q})$ is known.

In the following, $\ell_{\min}$ denotes the smallest prime not in S.

One way of applying Theorem A.3 is to consider families of curves in $E \times E$ such that $\ell_{\min}^{d_1/d_2}$ tends to infinity sufficiently fast compared to the height and the degree of the curves. Once the parameter is sufficiently large, it follows that the rational points of all the curves must be contained in some explicit finite set, so that one can determine the set of rational points on all the curves in the family. We will do this in the next section for the examples $\mathcal{C}_n$ and $\mathcal{D}_n$ given in Theorem 1.5.

Given a concrete curve, one can also increase the set S until λ exceeds the upper bound. This is always possible, since $\lambda \geqslant \ell_{\min}^2 \hat{h}(P_0)$. The conclusion is again that all rational points on the curve other than (O, O) must be S-integral, which may lead to a simpler way of determining this set.

We also state the following special case.

THEOREM A.4. *Assume that, in the situation of Theorem A.3, $E(\mathbb{Q})_{\text{tors}} = 0$ and $P_0 \notin E(\mathbb{Z}_\ell)$ for some $\ell \notin S$. Then*

$$\mathcal{C}(\mathbb{Q}) \subseteq \{(O, O)\} \cup \{P \in E(\mathbb{Q}) \times E(\mathbb{Q}) : \hat{h}(P) \geqslant \ell^{2\lceil d_1/d_2 \rceil - 2}\hat{h}(P_0)\}.$$

Proof. In this case, all points $P = (P_1, P_2) \in \mathcal{C}(\mathbb{Q})$ have $P_1, P_2 \in K_\ell(E)$. The argument in the proof of Theorem A.3 then applies to all these points with this fixed ℓ (here $a_\ell = 1$, since $P_0 \in K_\ell(E)$). □

If the lower bound $\ell^{2\lceil d_1/d_2 \rceil - 2}$ exceeds the upper bound given by Theorem 4.2, then it immediately follows that the only rational point on $\mathcal{C}$ is (O, O).

A.4. The curves $\mathcal{C}_n$ and $\mathcal{D}_n$. We recall the examples given in Theorem 1.5. The first family of examples consists of the curves $\mathcal{C}_n(E)$ defined as the closure of the subset of $(E \setminus \{O\})^2$ given by the equation $x_1^n = y_2$, for $n \geqslant 1$ and the

five elliptic curves $E = E_1, \dots, E_5$ as defined in the Introduction. The second family consists of the curves $\mathcal{D}_n(E_i)$ given by $\Phi_n(x_1) = y_2$, where Φ_n is the nth cyclotomic polynomial, for the same set of elliptic curves E_i.

In Theorem 1.5 the sets of rational points $\mathcal{C}_n(E_i)(\mathbb{Q})$ and $\mathcal{D}_n(E_i)(\mathbb{Q})$ are determined for varying ranges of n. We will use our results to find $\mathcal{C}_n(E_i)(\mathbb{Q})$ and $\mathcal{D}_n(E_i)(\mathbb{Q})$ for *all* n. We recall the upper bounds on $\hat{h}(P)$ for $P \in \mathcal{C}_n(E_i)(\mathbb{Q})$ from Theorem 9.1:

$$\begin{aligned}
E_1 &: \hat{h}(P) \leqslant b_1(n) = 73027n^2 + 219081n + 164320\\
E_2 &: \hat{h}(P) \leqslant b_2(n) = 311345n^2 + 934033n + 700566\\
E_3 &: \hat{h}(P) \leqslant b_3(n) = 373925n^2 + 1121775n + 841382\\
E_4 &: \hat{h}(P) \leqslant b_4(n) = 534732n^2 + 1604195n + 1203216\\
E_5 &: \hat{h}(P) \leqslant b_5(n) = 566995n^2 + 1700984n + 1275813.
\end{aligned}$$

From Corollary 8.2 we obtain the following bounds for $P \in \mathcal{D}_n(E_i)(\mathbb{Q})$:

$$\begin{aligned}
E_1 &: \hat{h}(P) \leqslant b_1'(n) = (901.5 \cdot 2^{\omega_2(n)} + 18257)(2\varphi(n) + 3)^2 + 9.7\\
E_2 &: \hat{h}(P) \leqslant b_2'(n) = (901.5 \cdot 2^{\omega_2(n)} + 77837)(2\varphi(n) + 3)^2 + 41.4\\
E_3 &: \hat{h}(P) \leqslant b_3'(n) = (901.5 \cdot 2^{\omega_2(n)} + 93482)(2\varphi(n) + 3)^2 + 50\\
E_4 &: \hat{h}(P) \leqslant b_4'(n) = (901.5 \cdot 2^{\omega_2(n)} + 133683)(2\varphi(n) + 3)^2 + 70\\
E_5 &: \hat{h}(P) \leqslant b_5'(n) = (901.5 \cdot 2^{\omega_2(n)} + 141749)(2\varphi(n) + 3)^2 + 75.
\end{aligned}$$

In all cases, we can take $S = \varnothing$ in Theorem A.3, since the leading coefficients of $F_1(x, y) = x^n$ or $\Phi_n(x)$ and $F_2(x, y) = y$ are both 1 and the curves are given by short integral Weierstrass equations. We have $d_1 = 2n$ (respectively, $d_1 = 2\varphi(n)$) and $d_2 = 3$, so for $n \geqslant 2$ (respectively, $n \geqslant 3$), the assumption $d_1 > d_2$ is satisfied.

We first consider E_1. Let $P_0 = (1, 1)$; this is a generator of $E_1(\mathbb{Q})$. Since P_0, $2P_0$ and $3P_0$ are all integral, we have $a_\ell \geqslant 4$ for all ℓ (and indeed $a_2 = 4$). So we have

$$\lambda(n) = 16 \cdot 2^{2\lceil 2n/3 \rceil - 2} \hat{h}(P_0) \geqslant 2^{4n/3+2} \hat{h}(P_0).$$

This is larger than $b_1(n)$ as soon as $n \geqslant 19$. For $\mathcal{D}_n(E_1)$, we have to compare $\lambda(\varphi(n))$ with $b_1'(n)$. We use the crude bound $2^{\omega_2(n)} \leqslant \varphi(n)$; we then have that $\lambda(\varphi(n)) \geqslant b_1'(n)$ for $\varphi(n) \geqslant 19$, which covers all $n \geqslant 61$. So for $n \geqslant 19$, we get from Theorem A.3 that

$$\mathcal{C}_n(E_1)(\mathbb{Q}) \subseteq \{(O, O)\} \cup (E_1(\mathbb{Z}) \times E_1(\mathbb{Z}))$$

and for $n \geqslant 61$, we get that

$$\mathcal{D}_n(E_1)(\mathbb{Q}) \subseteq \{(O, O)\} \cup (E_1(\mathbb{Z}) \times E_1(\mathbb{Z})).$$

We have that

$$E_1(\mathbb{Z}) = \{(1, \pm 1), (2, \pm 3)\ (13, \pm 47)\} = \{\pm P_0, \pm 2P_0, \pm 3P_0\}$$

(as obtained by a quick computation in Magma [4], for example).

To deal with $\mathcal{C}_n(E_1)$, we now only have to check which pairs of such points can satisfy the relation $x_1^n = y_2$. The only possibilities are $y_2 = 1$, so $P_2 = (1, 1)$ and $x_1 = 1$, so $P_1 = (1, \pm 1)$. Since the cases $n < 19$ are covered by Theorem 1.5, we obtain the following result.

COROLLARY A.5. *For all $n \geqslant 1$, we have*

$$\mathcal{C}_n(E_1)(\mathbb{Q}) = \{(O, O), ((1, 1), (1, 1)), ((1, -1), (1, 1))\}.$$

We now consider $\mathcal{D}_n(E_1)$. We have to solve the equation $\Phi_n(x_1) = y_2$, with $x_1 \in \{1, 2, 13\}$ and $y_2 \in \{\pm 1, \pm 3, \pm 47\}$. The easy estimate $|\Phi_n(2)| > 5^{\varphi(n)/4}$ and the even easier estimate $|\Phi_n(13)| \geqslant 12^{\varphi(n)}$ show that $x_1 = 1$ is the only possibility (when $n \geqslant 61$). We have the well-known fact that $\Phi_n(1) = 1$ unless $n = 1$ or n is a prime power, and $\Phi_{p^m}(1) = p$. This proves the following statement for $n \geqslant 61$; the remaining cases with $n \geqslant 7$ are covered by Theorem 1.5, which also shows that for $n \leqslant 6$, it is still true that all rational points other than (O, O) on $\mathcal{D}_n(E_1)$ are pairs of integral points on E_1, but there are some deviations from the pattern in the statement below (coming from small values of $\Phi_n(2)$: $\Phi_1(2) = 1$, $\Phi_2(2) = \Phi_6(2) = 3$).

COROLLARY A.6. *For all $n \geqslant 7$,*

$$\begin{aligned}
&\mathcal{D}_n(E_1)(\mathbb{Q}) = \{(O, O), ((1, 1), (1, 1)), ((1, -1), (1, 1))\} \\
&\qquad\qquad \text{if } n \text{ is not a prime power,} \\
&\mathcal{D}_n(E_1)(\mathbb{Q}) = \{(O, O)\} \quad \text{if } n = p^m \text{ with } p \neq 3, 47, \\
&\mathcal{D}_n(E_1)(\mathbb{Q}) = \{(O, O), ((1, 1), (2, 3)), ((1, -1), (2, 3))\} \quad \text{if } n = 3^m, \\
&\mathcal{D}_n(E_1)(\mathbb{Q}) = \{(O, O), ((1, 1), (13, 47)), ((1, -1), (13, 47))\} \quad \text{if } n = 47^m.
\end{aligned}$$

Now we consider the remaining curves E_i, $i = 2, 3, 4, 5$. In each case $E_i(\mathbb{Q}) \cong \mathbb{Z}$, and the generator is not ℓ-adically integral for $\ell = 491$, 11, 1418579, and 3956941, when $i = 2$, 3, 4 and 5, respectively. So we can apply Theorem A.4 with this ℓ. The lower bound exceeds the upper bound $b_i(n)$ (respectively, $b_i'(n)$) when $n \geqslant 3$ (respectively, $n \geqslant 7$) for $i = 2$, when $n \geqslant 6$ (respectively, $n \geqslant 19$) for $i = 3$ and when $n \geqslant 3$ (respectively, $n \geqslant 7$) for $i = 4$ and $i = 5$. So for these ranges, we obtain immediately that $\mathcal{C}_n(E_i)(\mathbb{Q}) = \mathcal{D}_n(E_i)(\mathbb{Q}) = \{(O, O)\}$. The

remaining cases are taken care of by Theorem 1.5; therefore we have now proved the following.

COROLLARY A.7. *For all $n \geqslant 1$ and $i = 2, 3, 4, 5$, we have*

$$\mathcal{C}_n(E_i)(\mathbb{Q}) = \mathcal{D}_n(E_i)(\mathbb{Q}) = \{(O, O)\}.$$

References

[1] LMFDB - The L-functions and Modular Forms Database, http://www.lmfdb.org/.

[2] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, 4 (Cambridge University Press, Cambridge, 2006).

[3] E. Bombieri, D. Masser and U. Zannier, 'Anomalous subvarieties—structure theorems and applications', *Int. Math. Res. Not. IMRN* **19** (2007), Art. ID rnm057, 33.

[4] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265. See also the Magma home page at http://magma.maths.usyd.edu.au/magma/.

[5] J.-B. Bost, H. Gillet and C. Soulé, 'Heights of projective varieties and positive Green forms', *J. Amer. Math. Soc.* **7**(4) (1994), 903–1027.

[6] P. Bruin, 'Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur les courbes elliptiques sur $\mathbb{Q}$', *Acta Arith.* **160**(4) (2013), 385–397.

[7] N. Bruin and M. Stoll, 'The Mordell–Weil sieve: proving non-existence of rational points on curves', *LMS J. Comput. Math.* **13** (2010), 272–306.

[8] C. Chabauty, 'Sur les points rationnels des courbes algébriques de genre supérieur à l'unité', *C. R. Math. Acad. Sci. Paris* **212** (1941), 882–885.

[9] S. Checcoli, F. Veneziano and E. Viada, 'On the explicit Torsion Anomalous Conjecture', *Trans. Amer. Math. Soc.* **369** (2017), 6465–6491.

[10] R. F. Coleman, 'Effective Chabauty', *Duke Math. J.* **52**(3) (1985), 765–770.

[11] J. E. Cremona, Elliptic Curve Data, https://johncremona.github.io/ecdata/.

[12] J. E. Cremona, M. Prickett and S. Siksek, 'Height difference bounds for elliptic curves over number fields', *J. Number Theory* **116** (2006), 42–68.

[13] V. A. Demjanenko, 'Rational points of a class of algebraic curves', *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 1373–1396.

[14] G. Faltings, 'Endlichkeitssätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.* **73**(3) (1983), 349–366.

[15] G. Faltings, 'Diophantine approximation on abelian varieties', *Ann. of Math. (2)* **133**(3) (1991), 549–576.

[16] G. Faltings, 'The general case of S. Lang's conjecture', in *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, (eds. V. Christante and W. Messing) Perspectives in Math. 15 (Academic Press, San Diego, CA, 1994), 175–182.

[17] E. V. Flynn, 'A flexible method for applying Chabauty's theorem', *Compos. Math.* **105**(1) (1997), 79–94.

[18] W. Fulton, *Intersection Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 2 (Springer, Berlin, 1984).

[19] M. Girard and L. Kulesz, 'Computation of sets of rational points of genus-3 curves via the Dem'janenko-Manin method', *LMS J. Comput. Math.* **8** (2005), 267–300.

[20] P. Habegger, 'Intersecting subvarieties of $\mathbb{G}_m^n$ with algebraic subgroups', *Math. Ann.* **342**(2) (2008), 449–466.
[21] M. Hindry, 'Autour d'une conjecture de Serge Lang', *Invent. Math.* **94**(3) (1988), 575–603.
[22] M. Hindry and J. H. Silverman, *Diophantine Geometry*, Graduate Texts in Mathematics, 201 (Springer, New York, 2000), An introduction.
[23] L.-C. Kappe and B. Warren, 'An elementary test for the Galois group of a quartic polynomial', *Amer. Math. Monthly* **96**(2) (1989), 133–137.
[24] L. Kulesz, 'Application de la méthode de Dem'janenko-Manin à certaines familles de courbes de genre 2 et 3', *J. Number Theory* **76**(1) (1999), 130–146.
[25] L. Kulesz, G. Matera and E. Schost, 'Uniform bounds on the number of rational points of a family of curves of genus 2', *J. Number Theory* **108**(2) (2004), 241–267.
[26] Ju. I. Manin, 'The p-torsion of elliptic curves is uniformly bounded', *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 459–465.
[27] D. W. Masser and G. Wüstholz, 'Estimating isogenies on elliptic curves', *Invent. Math.* **100**(1) (1990), 1–24.
[28] B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* **47** (1978), 33–186. 1977.
[29] W. McCallum and B. Poonen, 'The Method of Chabauty and Coleman', *Explicit methods in number theory; rational points and diophantine equations*, Panoramas et Synthèses 36 (Société Math. de France, 2012), 99–117.
[30] L. J. Mordell, 'On the rational solutions of the indeterminate equation of the third and fourth degrees', *Math. Proc. Cambridge Philos. Soc.* **21** (1922), 179–192.
[31] P. Parent, 'Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres', *J. Reine Angew. Math.* **506** (1999), 85–116.
[32] P. Philippon, 'Sur des hauteurs alternatives. I', *Math. Ann.* **289**(2) (1991), 255–283.
[33] P. Philippon, 'Sur des hauteurs alternatives. III.', *J. Math. Pures Appl. (9)* **74**(4) (1995), 345–365.
[34] P. Philippon, 'Sur une question d'orthogonalité dans les puissances de courbes elliptiques'. Preprint, 2012, arXiv:hal--00801376.
[35] G. Rémond, 'Décompte dans une conjecture de Lang', *Invent. Math.* **142**(3) (2000), 513–545.
[36] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, Aspects of Mathematics, E15 (Friedr. Vieweg & Sohn, Braunschweig, 1989), Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.
[37] S. Siksek, 'Explicit Chabauty over number fields', *Algebra Number Theory* **7**(4) (2013), 765–793.
[38] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 1986).
[39] J. H. Silverman, 'Rational points on certain families of curves of genus at least 2', *Proc. Lond. Math. Soc. (3)* **55**(3) (1987), 465–481.
[40] J. H. Silverman, 'The difference between the Weil height and the canonical height on elliptic curves', *Math. Comp.* **55**(192) (1990), 723–743.
[41] J. H. Silverman, 'Computing rational points on rank 1 elliptic curves via L-series and canonical heights', *Math. Comp.* **68**(226) (1999), 835–858.
[42] M. Stoll, 'Rational points on curves', *J. Théor. Nombres Bordeaux* **23**(1) (2011), 257–277.
[43] The PARI Group. *PARI/GP version* `2.8.0`. 2015. http://pari.math.u-bordeaux.fr/.
[44] E. Viada, 'An explicit Manin–Dem'janenko theorem in elliptic curves', *Canad. J. Math.* **70**(5) (2018), 1173–1200.
[45] 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**(1) (2003), 47–75.

[46] E. Viada, 'Explicit height bounds and the effective Mordell–Lang conjecture', *Riv. Mat. Uni. Parma (8)* **7**(1) (2016), 101–131. Proceedings of the 'Third Italian Number Theory Meeting' Pisa (Italy), September 21–24, 2015.

[47] P. Vojta, 'Siegel's theorem in the compact case', *Ann. of Math. (2)* **133**(3) (1991), 509–548.

[48] U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematics Studies, 181 (Princeton University Press, Princeton, NJ, 2012), With appendixes by David Masser.

[49] S. Zhang, 'Positive line bundles on arithmetic varieties', *J. Amer. Math. Soc.* **8**(1) (1995), 187–221.

[50] H. G. Zimmer, 'On the difference of the Weil height and the Néron-Tate height', *Math. Z.* **147**(1) (1976), 35–51.