HAL
open science

Elliptic logarithms, diophantine approximation and the Birch and Swinnerton-Dyer conjecture

Vincent Bosser, Andrea Surroca

To cite this version:

Vincent Bosser, Andrea Surroca. Elliptic logarithms, diophantine approximation and the Birch and Swinnerton-Dyer conjecture. Boletim da Sociedade Brasileira de Matemática / Bulletin of the Brazilian Mathematical Society, 2014, 45 (1), 10.1007/s00574-014-0038-x . hal-02151923

HAL Id: hal-02151923

https://normandie-univ.hal.science/hal-02151923v1

Submitted on 10 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

arXiv:1203.3865v3 [math.NT] 6 Jan 2013

Elliptic logarithms, diophantine approximation and the Birch and Swinnerton-Dyer conjecture

Vincent Bosser (Caen)*
Andrea Surroca (Basle)†

January 8, 2013

Abstract. Most, if not all, unconditional results towards the *abc*-conjecture rely ultimately on classical Baker's method. In this article, we turn our attention to its *elliptic* analogue. Using the elliptic Baker's method, we have recently obtained a new upper bound for the height of the S-integral points on an elliptic curve. This bound depends on some parameters related to the Mordell-Weil group of the curve. We deduce here a bound relying on the conjecture of Birch and Swinnerton-Dyer, involving classical, more manageable quantities. We then study which *abc*-type inequality over number fields could be derived from this elliptic approach.

Keywords: integral points on elliptic curves, quantitative Siegel's theorem, elliptic logarithms, Birch and Swinnerton-Dyer conjecture, *abc*-conjecture.

Mathematical subject classification: Primary: 11G50; Secondary: 11G05, 11J86, 14G05, 11G40.

1 Introduction

The *abc*-conjecture of D. W. Masser and J. Oesterlé (Conjecture 4.1 below) is one of the most important unsolved problems in Diophantine analysis. It is well known that it is connected with several problems in number theory. If true, it would imply strong or quantitative versions of important theorems. Indeed, let us recall the classical Siegel's theorem: for an affine curve of genus ≥ 1 or of genus 0 having at least three points at infinity, the set of integral points is finite. This theorem was later extended to S-integral points by Mahler. For curves of genus ≥ 2, Siegel's theorem is superseded by Faltings' theorem, which asserts that the set of rational points on an algebraic curve of genus greater

*Supported by the contract ANR "HAMOT", BLAN-0115-01.
†Supported by an Ambizione fund PZ00P2_121962 of the Swiss National Science Foundation and the Marie Curie IEF 025499 of the European Community.

than 2 is finite. These results are qualitative statements in general, that is, there is no known proof providing an upper bound for the height of the points, *i.e.* a "quantitative" result, which would allow to find these points. The only known quantitative results on rational points concern integral points and only some particular cases, *e.g.* the case of curves of genus 0, 1, or the case of curves which are Galois coverings of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$. All of them come from classical Baker's method using lower bounds for linear forms in logarithms. We refer the reader to [Győ02], [Bil02] and the references therein for an overview of known results.

As noticed by Elkies [Elk91], the *abc*-conjecture over number fields would imply a quantitative version on Faltings' theorem. As shown by the second author [Sur04], also a quantitative Siegel's theorem would follow, with explicit dependence on the set of places S. Unfortunately only weak results are known towards this conjecture yet, and they are insufficient to yield a quantitative Siegel's theorem for new classes of curves.

On the other hand, it is worth noting that Moret-Bailly [MB90] showed that, conversely, a uniform and effective version of Falting's theorem for the curve $y^2 + y = x^5$ would imply *abc*. As shown in [Sur07], any bound for the height of the more restrictive set of the S-integral points on a fixed curve, explicit in the set S and in the degree and the discriminant of the number field considered, would suffice to imply a result towards the *abc*-conjecture over this number field. Using such a bound given by a quantitative Siegel's theorem due to Bilu [Bil97], the second author obtained in her thesis (see [Sur07]) the first result towards the *abc*-conjecture over an arbitrary number field. Afterwards, K. Gyory and K. Yu ([GY06], [Győ08]) gave completely explicit *abc*-type results using bounds for the height of solutions of S-unit equations. When the number field is $\mathbf{Q}$ better inequalities were known, see [ST86] for the first result obtained and [SY91], [SY01] for later improvements. Roughly speaking, all these results differ from the conjecture from an exponential.[1]

All the quantitative Siegel's theorems and the *abc*-type results mentioned above depend ultimately on lower bounds for linear forms in usual logarithms, complex as well as p-adic. In this paper, we turn our attention to the *elliptic* analogue of Baker's method. In fact, in order to get a quantitative Siegel's theorem in the case of an elliptic curve, it seems to be more natural to take advantage of the group law and thus to use linear forms in *elliptic* logarithms. Following this approach, we have recently obtained in [BS12] a new upper bound for the height of the S-integral points of an elliptic curve E defined over a number field K, using the explicit lower bounds for linear forms in elliptic logarithms of S. David [Dav95] in the archimedean case, and of N. Hirata [Hir12] in the ultrametric one. However, the method leads to a bound which is not quite effective since it depends on several parameters depending on the Mordell-Weil group $E(K)$ of the curve (see Theorem 3.1 below).

This raises the question of knowing under which conditions one can get an explicit, more manageable, upper bound in terms of the set S and the number field K using the elliptic

[1] In another direction, A. Baker [Bak98] and P. Philippon [Phi99] suggested some conjectures on linear forms in logarithms which would imply a weak version of *abc* (where $1 + \epsilon$ is replaced by some other constant). These conjectures involve simultaneously several places (archimedean and non-archimedean) but these kinds of results are now far away from being proved.

Baker's method, and which kind of result towards the *abc*-conjecture can be obtained in this way. This paper gives an answer to these two questions. We will see that, following Manin's conditional algorithm [Man71, Theorem 11.1] based on the assumption of the conjecture of B. J. Birch and H. P. F. Swinnerton-Dyer (Conjecture 3.3, BSD-conjecture for short) and the classical Hasse-Weil conjecture, we can derive from [BS12] a quantitative Siegel's theorem whose bound is explicit in S, the degree and the discriminant of the number field (Theorem 3.4). Thus this paper highlights some connection between Baker's method, the BSD-conjecture and the *abc*-conjecture.

The paper is organized as follows. For convenience to the reader, we have gathered in Section 2 the notation which will be used throughout the text. In Section 3, after recalling the BSD-conjecture, we state and prove a conjectural upper bound for the height of S-integral points (Theorem 3.4). Finally, in Section 4, we prove Theorem 4.2 and discuss the result.

2 Notations

Throughout the text, if x is a non negative real number, we set $\log^+ x = \max\{1, \log x\}$ (with the convention $\log^+ 0 = 1$).

If K is a number field, we will denote by O_K its ring of integers, by D_K the absolute value of its discriminant, and by M_K the set of places of K. The set of the archimedean places will be denoted by M_K^∞ and the set of the ultrametric ones will be denoted by M_K^0. For each v in M_K, we define an absolute value $|\cdot|_v$ on K as follows. If v is archimedean, then v corresponds to an embedding $\sigma : K \hookrightarrow \mathbf{C}$ or its complex conjugate (we identify the place v with the embedding σ), and we set $|x|_v = |x|_\sigma := |\sigma(x)|$, where $|\cdot|$ is the usual absolute value on $\mathbf{C}$. If v is ultrametric, then v corresponds to a non zero prime ideal $\mathfrak{p}$ of O_K (we will identify v and $\mathfrak{p}$), and we take for $|\cdot|_v = |\cdot|_\mathfrak{p}$ the absolute value on K normalized by $|p|_v = p^{-1}$, where p is the prime number such that $\mathfrak{p} \mid p$. We denote by K_v the completion of K at v and use again the notation $|\cdot|_v$ for the unique extension of $|\cdot|_v$ to K_v. If v is an ultrametric place associated to the prime ideal $\mathfrak{p}$, we denote by $e_\mathfrak{p}$ the ramification index of $\mathfrak{p}$ over p, by $f_\mathfrak{p}$ the residue class degree, and by $\mathrm{ord}_\mathfrak{p} : K_\mathfrak{p}^* \to \mathbf{Z}$ the valuation normalized by $\mathrm{ord}_\mathfrak{p}(p) = e_\mathfrak{p}$ (hence $\mathrm{ord}_\mathfrak{p}(x) = -e_\mathfrak{p} \log_p |x|_\mathfrak{p}$ for all x in $K_\mathfrak{p}^*$).

If S is a finite subset of M_K^0, we denote by

$$O_{K,S} = \{x \in K; \forall v \notin S \cup M_K^\infty, |x|_v \leq 1\}$$

the ring of S-integers of K, and we set

$$\Sigma_S = \sum_{\mathfrak{p} \in S} \log N_{K/\mathbf{Q}}(\mathfrak{p}).$$

Note that with our notation, the set S contains only non-archimedean places of K.

Throughout the text, we denote by h the absolute logarithmic Weil height on the projective space $\mathbf{P}^n(\overline{\mathbf{Q}})$, and we denote by $h_K := [K : \mathbf{Q}]h$ the relative height on $\mathbf{P}^n(K)$.

Thus, if $(\alpha_0 : \ldots : \alpha_n) \in \mathbf{P}^n(K)$, we have:

$$h(\alpha_0 : \ldots : \alpha_n) = \frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} [K_v : \mathbf{Q}_v] \log \max\{|\alpha_0|_v, \ldots, |\alpha_n|_v\}. \tag{1}$$

For every $(\alpha_1 : \alpha_2 : \alpha_3) \in \mathbf{P}^2(K)$, we further define

$$\mathrm{rad_K}(\alpha_1 : \alpha_2 : \alpha_3) = \Sigma_S,$$

where $S = \{\mathfrak{p} \in M_K^0; \mathrm{card}\{\mathrm{ord}_\mathfrak{p}(\alpha_1), \mathrm{ord}_\mathfrak{p}(\alpha_2), \mathrm{ord}_\mathfrak{p}(\alpha_3)\} \geq 2\}$.

Let E be an elliptic curve defined over a number field K. The Mordell-Weil group $E(K)$ of K-rational points of E is a finitely generated group:

$$E(K) \simeq E(K)_{tors} \oplus \mathbf{Z}^{\mathrm{rk}(E(K))}.$$

We will often simply write $r = \mathrm{rk}(E(K))$ for its rank, and we will denote by $(Q_1, \ldots, Q_r)$ a basis of its free part.

We further denote by $\hat{h} : E(\overline{K}) \to \mathbf{R}$ the Néron-Tate height on E. The "Néron-Tate pairing" $<,>$ is defined by $< P, Q >= \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$. The regulator $\mathrm{Reg}(E/K)$ of E/K is the determinant of the matrix $\mathcal{H} = (< Q_i, Q_j >)_{1 \leq i,j \leq r}$ of the Néron-Tate pairing with respect to the chosen basis $(Q_1, \ldots, Q_r)$, that is

$$\mathrm{Reg}(E/K) = \det(\mathcal{H}).$$

Suppose now that the elliptic curve E is embedded in $\mathbf{P}^2$ and given by a Weierstrass equation

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

with $A, B \in O_K$. Let us denote by $O = (0 : 1 : 0)$ the zero element of $E(K)$. If $Q \neq O$ is a point of E, we will denote its affine coordinates (in the above Weierstrass model) as usual by $(x(Q), y(Q))$. For Q in $E(\overline{K})$ we define $h_x(Q) := h(1 : x(Q))$ if $Q \neq O$ and $h_x(O) := 0$. Finally, we denote by $E(O_{K,S})$ the set of S-integral points of $E(K)$ with respect to the x-coordinate, that is

$$E(O_{K,S}) = \{Q \in E(K) \setminus \{O\}; x(Q) \in O_{K,S}\} \cup \{O\}.$$

In fact, in all what follows it will be crucial to distinguish the field of definition of the elliptic curve from the field of rationality of the points we will consider. More precisely, we will fix a number field K_0 and an elliptic curve E defined over K_0, and we will consider points in $E(K)$, where K is a finite extension of K_0 (that we will think of as varying). In the estimates that will occur we will neither be interested in the dependence on E/K_0 nor try to explicit it, and we will thus consider as a "constant" any quantity depending on E/K_0. This convention about constants will apply in particular to the various implicit constants involved in the symbols $\ll$ appearing in the text.

3 Conditional upper bound for the height of S-integral points

In this section, we fix a number field K_0 and we consider an elliptic curve E defined over K_0 given by a Weierstrass equation (2), where $A, B \in O_{K_0}$. Let K be a finite extension of K_0 and $S \subset M_K^0$ be a finite set of places of K. We denote by r the rank of the Mordell-Weil group $E(K)$, by $(Q_1, \ldots, Q_r)$ a system of generators of its free part, and we define the real number V by

$$\log V := \max\{\hat{h}(Q_i); 1 \leq i \leq r\}.$$

We further set

$$d := [K : \mathbf{Q}].$$

In [BS12], we have obtained the following result.

Theorem 3.1 *In the above set up, let Q be a point in $E(O_{K,S})$. Then there exist positive effectively computable real numbers γ_0, γ_1 and γ_2 depending only on A and B (that is, on the curve E/K_0), such that, if $r = 0$, then $h_x(Q) \leq \gamma_0$, and, if $r > 0$, then*

$$h_x(Q) \leq C_{E,K} e^{(8r^2+\gamma_1 dr)\Sigma_S}, \tag{3}$$

where

$$C_{E,K} = \gamma_2^{r^2} r^{2r^2} d^{9r+15} (\log^+ d)^{r+6} (\log^+ \log V)^{r+7} (\log^+ \log^+ \log V)^2 \prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\}$$
$$\times \log^+(\mathrm{Reg}(E/K)^{-1})(\log^+\log(\mathrm{Reg}(E/K)^{-1}))^2(\log^+\log^+\log(\mathrm{Reg}(E/K)^{-1})). \tag{4}$$

The aim of this section is to deduce from Theorem 3.1 an upper bound for the height of the S-integral points of $E(K)$, depending only on E/K_0 and on the parameters Σ_S, d and D_K. Such a bound will be obtained assuming the Hasse-Weil conjecture and BSD-conjecture. The approach relies on Manin's algorithm [Man71]. See also Masser's book [Mas75, Appendix IV, p. 140], where the association of Manin's algorithm with linear forms in elliptic logarithms appears for the first time to get an effective version of Siegel's theorem. The precise statement we prove here is given in the next section.

3.1 Statement of the result

In order to state the conjectural quantitative Siegel's theorem we obtain, we need to introduce the two conjectures we will use. Denote by $L(E/K, s)$ the L-series (or ζ-function) of E/K at s, which is an analytic function for all s satisfying $\Re(s) > \frac{3}{2}$. Let $\mathcal{F}_{E/K}$ denote the conductor of E over K. Following [Mil72], define the normalized L-function as

$$\Lambda(E/K, s) = N_{K/\mathbf{Q}}(\mathcal{F}_{E/K})^{s/2} \cdot D_K^s \cdot ((2\pi)^{-s} \cdot \Gamma(s))^{[K:\mathbf{Q}]} \cdot L(E/K, s).$$

We then have the classical conjecture.

Conjecture 3.2 (Hasse-Weil) *Let E/K be an elliptic curve defined over a number field. The L-series of E/K has an analytic continuation of finite order to the entire complex plane and satisfies the functional equation*

$$\Lambda(E/K, 2-s) = \varepsilon\Lambda(E/K, s), \text{ for some } \varepsilon = \pm 1.$$

This conjecture is true for abelian varieties with complex multiplication ([ST61]), for elliptic curves over $\mathbf{Q}$ ([Wil95]) and in some special cases, this conjecture is also true for modular abelian varieties ([Shi94]).

Denote $Ш(E/K) = \ker(H^1(\mathrm{Gal}(\overline{K}/K), E_K) \to \prod_v H^1(\mathrm{Gal}(\overline{K}_v/K_v), E_{K_v}))$ the Tate-Shafarevich group, which is conjectured to be a finite group. (See [Rub87] and [Kol88] for the first examples of elliptic curves for which it was proved that the Tate-Shafarevich group is finite.) Let $F(x, y) = 0$ be a Weierstrass equation for E. Denote F_y the partial derivative of F with respect to y. Then the invariant differential of the Weierstrass equation, $\omega = \frac{dx}{F_y}$, is holomorphic and non vanishing. Let $\mathcal{E}$ denote the Néron model of E over O_K and let $\Omega^1_{\mathcal{E}/O_K}$ be the invertible sheaf of the differential 1-forms on $\mathcal{E}$. The module $H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/O_K})$ of global invariant differentials on $\mathcal{E}$ is a projective O_K-module of rank 1 and can be written as

$$H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/O_K}) = \omega\mathfrak{a},$$

where $\mathfrak{a}$ is a fractional ideal of K (depending on ω).

To every place v of K, we will associate a local number c_v. For v a finite place of K, let $E^0(K_v)$ be the subgroup of K_v-rational points which reduces to the identity component of the Néron model $\mathcal{E}$. Let μ_v be an additive Haar measure on K_v such that $\mu_v(O_{K_v}) = 1$ if v is finite, μ_v is the Lebesgue measure if v is a real archimedean place and twice the Lebesgue measure if v is complex. Define, for an *archimedean* place v, the *local period*

$$c_v = \int_{E(K_v)} |\omega|\mu_v.$$

Define, for a *finite* place v of K, $c_v = \mathrm{card}(E(K_v)/E^0(K_v))$ and

$$c_\infty(E/K) = \prod_{v \in M_K^\infty} c_v \cdot N_{K/\mathbf{Q}}(\mathfrak{a}),$$

which is independent of the choice of the differential ω.

The Birch and Swinnerton-Dyer conjecture can be stated as follows [BSD65] (see also [Gro82]).

Conjecture 3.3 (Birch and Swinnerton-Dyer) *Let E/K be an elliptic curve defined over a number field.*

1. *The L-series $L(E/K, s)$ has an analytic continuation to the entire complex plane.*
2. $\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rk}(E(K))$.

3. *The leading coefficient* $L^\star(E/K,1) = \lim_{s\to 1} \frac{L(E/K,s)}{(s-1)^{\mathrm{rk}(E(K))}}$ *in the Taylor expansion of* $L(E/K,s)$ *at* $s=1$ *satisfies*

$$L^\star(E/K,1) = |Ш(E/K)| \cdot \mathrm{Reg}(E/K) \cdot |E(K)_{tors}|^{-2} \cdot c_\infty(E/K) \cdot \prod_{v\in M_K^0} c_v \cdot D_K^{-1/2}. \quad (5)$$

We can now state the conjectural quantitative Siegel's theorem that we obtain.

Theorem 3.4 *Let* K_0 *be a number field, and let* E *be an elliptic curve given by a Weierstrass equation* $y^2 = x^3 + Ax + B$ *with* $A, B \in O_{K_0}$. *Let* K/K_0 *be a finite extension,* S *a finite set of finite places of* K, *and denote by* d *the degree* $[K:\mathbf{Q}]$.

Suppose that the L-series of E/K *satisfies a functional equation (Conjecture 3.2) and that the Birch and Swinnerton-Dyer Conjecture (Conjecture 3.3) holds for* E/K.

Then, there exist positive numbers α_1 *and* α_2 *(depending on* E/K_0 *only) such that, for every point* Q *in* $E(O_{K,S})$, *we have*

$$h_x(Q) \le \exp\{\alpha_1^d + \alpha_2\, d^6 (\log^+ D_K)^2\, [\Sigma_S + \log(d \log^+ D_K)]\}.$$

The rest of Section 3 is devoted to the proof of this theorem. To deduce Theorem 3.4 from Theorem 3.1, we need to bound from above in terms of d, D_K and Σ_S the following parameters : the rank r, the product $\prod_{i=1}^r \max\{1, \hat{h}(Q_i)\}$, the greatest height $\log V$ and the inverse of the regulator $\mathrm{Reg}(E/K)^{-1}$. In Section 3.2, we first bound from above the rank r. Then, in Section 3.3, we bound from above the three remaining quantities. The bounds for $\prod_{i=1}^r \max\{1, \hat{h}(Q_i)\}$ and $\log V$ will rely on the BSD-conjecture. Finally, we prove Theorem 3.4 in Section 3.4.

3.2 An upper bound for the rank of the Mordell-Weil group

Explicit computations for the Weak Mordell-Weil theorem give a bound for the rank of the Mordell-Weil group in terms of the discriminant of the number field.[2] The following is Theorem 1 of [OT89], slightly corrected by G. Rémond ([Rém10, Proposition 5.1]), for the special case where the abelian variety is an elliptic curve. We denote by $\mathcal{F}^0_{E/K}$ the radical of the conductor of E over K, that is, the product of the prime ideals of O_K where E has bad reduction.

Lemma 3.5 (Ooe-Top, Rémond) *There exist real numbers* κ_1, κ_2 *and* κ_3 *depending only on the degree* $d = [K:\mathbf{Q}]$ *such that*

$$\mathrm{rk} E(K) \le \kappa_1 \log N_{K/\mathbf{Q}} \mathcal{F}^0_{E/K} + \kappa_2 \log D_K + \kappa_3,$$

and one may take $\kappa_2 = \frac{2^7}{\log 2} d$, $\kappa_1 = 4d\kappa_2$ *and* $\kappa_3 = \kappa_2(\log 16 \cdot d^2 - 1)$.

[2] Remark that, contrary to our situation, most often the interest in bounding the rank lies in the dependence on the conductor of the elliptic curve, and the dependence on the number field is not considered. For example, under Conjectures 3.2 and 3.3 and the generalized Riemann hypothesis for $L(E/\mathbf{Q})$, one would obtain $\mathrm{rk}(E(K)) \ll \frac{\log \mathcal{F}_{E/K}}{\log\log \mathcal{F}_{E/K}}$, where the implied constant in $\ll$ depends on K. (See [Mes86].)

Lemma 3.6 *The conductors of the elliptic curve over K and over K_0 satisfy*

$$\log N_{K/\mathbf{Q}}\mathcal{F}_{E/K} \leq 8[K:\mathbf{Q}] \log N_{K_0/\mathbf{Q}}\mathcal{F}_{E/K_0}.$$

Proof. We will use the upper bounds for the exponents of the conductor $\mathcal{F}_{E/K}$ given in [LRS93, Theorem 0.1] and [BK94, Theorem 6.2]. According to these results, if we write the conductor $\mathcal{F}_{E/K}$ of E/K as

$$\mathcal{F}_{E/K} = \prod_{\mathfrak{q}} \mathfrak{q}^{\delta_{\mathfrak{q}}(E)},$$

then, for each prime ideal $\mathfrak{q}$ lying above the prime number p, we have $\delta_{\mathfrak{q}}(E) \leq 2$ if $p \geq 5$, $\delta_{\mathfrak{q}}(E) \leq 2 + 3e_{\mathfrak{q}}$ if $p = 3$, and $\delta_{\mathfrak{q}}(E) \leq 2 + 6e_{\mathfrak{q}}$ if $p = 2$. In all cases we thus have the bound $\delta_{\mathfrak{q}}(E) \leq 8e_{\mathfrak{q}}$. Moreover, it is well known that if $\delta_{\mathfrak{q}}(E) \neq 0$, then $\mathfrak{q}$ must lie above a prime ideal $\mathfrak{p}$ of O_{K_0} at which E has bad reduction. Since the prime ideals $\mathfrak{p}$ of bad reduction are those dividing $\mathcal{F}_{E/K_0}$, we obtain

$$\begin{aligned} N_{K/\mathbf{Q}}(\mathcal{F}_{E/K}) &= \prod_{\mathfrak{p}|\mathcal{F}_{E/K_0}} \prod_{\mathfrak{q}|\mathfrak{p}} N_{K/\mathbf{Q}}(\mathfrak{q})^{\delta_{\mathfrak{q}}(E)} \leq \prod_{\mathfrak{p}|\mathcal{F}_{E/K_0}} \prod_{\mathfrak{q}|\mathfrak{p}} N_{K_0/\mathbf{Q}}(\mathfrak{p})^{8e_{\mathfrak{q}}f_{\mathfrak{q}/\mathfrak{p}}} \\ &\leq \prod_{\mathfrak{p}|\mathcal{F}_{E/K_0}} N_{K_0/\mathbf{Q}}(\mathfrak{p})^{8[K:\mathbf{Q}]} \leq N_{K_0/\mathbf{Q}}(\mathcal{F}_{E/K_0})^{8[K:\mathbf{Q}]}. \end{aligned}$$

□

Lemmas 3.5 and 3.6, together with the fact that $N_{K/\mathbf{Q}}\mathcal{F}^0_{E/K} \leq N_{K/\mathbf{Q}}\mathcal{F}_{E/K}$, lead to the following bound for the rank.

Lemma 3.7 *The rank r of the Mordell-Weil group $E(K)$ satisfies*

$$r \ll d^3(\log^+ D_K),$$

where the implicit constant depends at most on E/K_0.

3.3 On the generators of the Mordell-Weil group

We give here upper bounds for $\log V$, $\prod_{i=1}^r \max\{1, \hat{h}(Q_i)\}$ and $\mathrm{Reg}(E/K)^{-1}$. For this purpose, we follow the approach of Yu. Manin [Man71]. We argue in two steps. In Section 3.3.1, we obtain first unconditional upper bounds, but involving the regulator $\mathrm{Reg}(E/K)$. The main ingredients used are a result on the geometry of numbers as well as a lower bound for the Néron-Tate height of non-torsion points due to Masser. Then, in Section 3.3.2, we bound from above the regulator $\mathrm{Reg}(E/K)$ using the BSD-conjecture.

3.3.1 An upper bound for $\log V$, $\prod_{i=1}^r \max\{1, \hat{h}(Q_i)\}$ and $\mathrm{Reg}(E/K)^{-1}$

Geometry of numbers. Recall that the Néron-Tate height on E extends to a positive definite quadratic form on $E(K) \otimes_{\mathbf{Z}} \mathbf{R}$. The Néron-Tate pairing gives $E(K) \otimes_{\mathbf{Z}} \mathbf{R} \simeq \mathbf{R}^r$ the structure of an Euclidean space. The free part of the Mordell-Weil group, $\Lambda := E(K)/E(K)_{tors}$, sits as a lattice in this vector space. The regulator of E/K is the square of the volume of a fundamental domain for the lattice. Thus we have

$$\mathrm{Reg}(E/K) = (\det(\Lambda))^2 = \det(\mathcal{H}),$$

where $\mathcal{H} = (< Q_i, Q_j >)_{1 \leq i,j \leq r}$ is the matrix of the Néron-Tate pairing with respect to the chosen basis $(Q_1, \ldots, Q_r)$. We begin by choosing a good basis.

Lemma 3.8 (Minkowski) *We can choose a basis $(Q_1, \ldots, Q_r)$ for the free part of the Mordell-Weil group satisfying $\hat{h}(Q_1) \leq \ldots \leq \hat{h}(Q_r)$, and*

$$\prod_{i=1}^{r} \hat{h}(Q_i) \leq (r!)^4 \mathrm{Reg}(E/K). \tag{6}$$

Proof. Put together Minkowski's theorem on the successive minima [Cas97, Theorem V, Chapter VIII, section 4.3] with Lemma 8 page 135 of [Cas97] as [Rém05, Lemma 5.1]. □

From now on, we assume that we have chosen a basis $(Q_1, \ldots, Q_r)$ as in Lemma 3.8. Thus, in order to bound the regulator from below, it suffices to use a lower bound for the $\hat{h}(Q_i)$'s. In order to bound from above $\prod_{i=1}^r \max\{1, \hat{h}(Q_i)\}$ (resp. $\log V = \hat{h}(Q_r)$), we will use inequality (6) together with a lower bound for the $\hat{h}(Q_i)$'s satisfying $\hat{h}(Q_i) < 1$ (resp. for $\hat{h}(Q_1), \ldots, \hat{h}(Q_{r-1})$). So we now bring our attention to the problem of giving lower bounds for the height of non-torsion points of the Mordell-Weil group.

Lower bound for the height of non-torsion points. It is known that for non-torsion points, the Néron-Tate height is non-zero and we can then ask for a lower bound. Since the elliptic curve E/K_0 is fixed, but not the degree $[K : \mathbf{Q}]$ of the field of rationality of the point Q, we are interested in Lehmer's type results. The following corollary of a theorem of D. Masser [Mas89] is enough for our purpose. [3]

Proposition 3.9 (Masser) *There exists a positive real number $\kappa_4 < 1$, depending on the curve E/K_0, such that, for any field extension K/K_0 of degree $d = [K : \mathbf{Q}] \geq 2$ and for all points Q in $E(K) \setminus E_{tors}$ one has*

$$\hat{h}(Q) \geq \frac{\kappa_4}{d^3 (\log d)^2}. \tag{7}$$

We then obtain the following bounds.

[3] Note that, as pointed out by Manin [Man71], for a given elliptic curve and a given number field K, it is not difficult to compute an effective lower bound for $\hat{h}(Q)$.

Lemma 3.10 *The following inequalities hold :*

$$\log^+(\mathrm{Reg}(E/K)^{-1}) \ll d^3\,(\log^+ d)\,(\log^+ D_K)\,(\log^+ \log D_K). \tag{8}$$

$$\log V \leq \left(\frac{d^3(\log^+ d)^2}{\kappa_4}\right)^{r-1} \cdot (r!)^4 \cdot \mathrm{Reg}(E/K). \tag{9}$$

$$\prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\} \leq \left(\frac{d^3(\log^+ d)^2}{\kappa_4}\right)^{r} \cdot (r!)^4 \cdot \mathrm{Reg}(E/K), \tag{10}$$

where the implicit constant in the symbol $\ll$ depends at most on E/K_0.

Proof. It follows from Lemma 3.8 and from Proposition 3.9 that we have

$$\left(\frac{\kappa_4}{d^3(\log^+ d)^2}\right)^{r} \leq (r!)^4 \mathrm{Reg}(E/K).$$

Hence we get, using Lemma 3.7 :

$$\begin{aligned} \log^+(\mathrm{Reg}(E/K)^{-1}) &\leq 4r\log r + r\log\left(\frac{d^3(\log^+ d)^2}{\kappa_4}\right) \\ &\ll d^3(\log^+ d)\,(\log^+ D_K)\,(\log^+ \log D_K). \end{aligned}$$

This proves (8). To prove (9), we simply apply Masser's lower bound (7) to the $r-1$ smallest points of the basis and replace it in Minkowski's inequality (6). Finally, to prove (10), write $\prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\} = \prod_{i=1}^{r} \hat{h}(Q_i) \times \left(\prod_{\hat{h}(Q_i)<1} \hat{h}(Q_i)\right)^{-1}$, where the second product runs over the i's for which $\hat{h}(Q_i) < 1$. Applying the inequality (6) for the first factor and Masser's lower bound (7) to the second one, we get the result. □

3.3.2 A conditional upper bound for the regulator

On the BSD-conjecture. The upper bounds (9) and (10) obtained in Lemma 3.10 for the height of the generators involve the regulator $\mathrm{Reg}(E/K)$. In order to bound it from above, the BSD-conjecture suggests to bound each of the terms of the formula (5). We denote $h_{Falt}(E/K)$ the Faltings' height of E/K. The next proposition is Proposition 3.12 of [Sur12].

Proposition 3.11 *Suppose that Conjecture 3.2 and 3.3 hold for the elliptic curve E/K. Then*

$$\mathrm{Reg}(E/K) \leq C_d \cdot D_K^{3/2} \cdot \sqrt{N_{K/\mathbf{Q}}(\mathcal{F}_{E/K})} \cdot (\exp\{h_{Falt}(E/K)\} \cdot h_{Falt}(E/K))^d, \tag{11}$$

where $d = [K : \mathbf{Q}]$ and we may take $C_d = \left(\frac{9}{2\pi}\right)^d \cdot (3d^2)^d \cdot (129.(5^d-1)(3d)^6)^{\frac{(1+3^{d/2})^8}{\log(1+3^{d/2})}}$.

Using this proposition and Lemma 3.6 for the conductor, we get a conditional bound for the regulator as we want and we can also bound the other quantities involving the generators of the Mordell-Weil group.

Lemma 3.12 *Suppose that Conjecture 3.2 and 3.3 hold for the elliptic curve E/K. Then there exist positive numbers κ_5, κ_6, κ_7 (depending at most on E/K_0) such that*

1. $\mathrm{Reg}(E/K) \ll e^{\kappa_5^d} D_K^{3/2}$.
2. $\log^+ \log V \ll \kappa_6^d \, (\log^+ D_K) \, (\log^+ \log D_K)$.
3. $\displaystyle\prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\} \ll \left(d \cdot \log^+ D_K\right)^{\kappa_7 d^3 \log^+ D_K} e^{\kappa_5^d} \cdot D_K^{3/2}$,

where the implicit constants in the symbol $\ll$ depend at most on E/K_0.

Proof.

1. By [CS86, Remark 5.1.1, Chapter IX], we have $h_{Falt}(E/K) \leq h_{Falt}(E/K_0)$. Using now Lemma 3.6, the result is an immediate consequence of Proposition 3.11.
2. Use the bound (9) of Lemma 3.10, item 1 and Lemma 3.7.
3. The result follows from the bound (10) of Lemma 3.10, Lemma 3.7 and item 1.

□

3.4 Proof of Theorem 3.4

We want to apply Theorem 3.1, so we need to estimate first $C_{E,K}$. By Lemma 3.7, Lemma 3.12 and Inequality (8) of Lemma 3.10, we have :

$$\log C_{E,K} \quad \leq \quad c_1 d^6 \, (\log^+ D_K)^2 \, (\log(d \log^+ D_K)) + \kappa_5^d,$$

for some $c_1 = c_1(E/K_0)$. On the other hand, by Lemma 3.7 again, we have :

$$8r^2 + \gamma_1 dr \leq c_2 d^6 \, (\log^+ D_K)^2,$$

for some $c_2 = c_2(E/K_0)$. Theorem 3.4 follows at once from these estimates and from Theorem 3.1. □

4 What about *abc*?

As already mentioned in the introduction, the second author has shown in [Sur07] that one can deduce an *abc*-type inequality over number fields from a bound for the height of the S-integral points on a fixed curve, explicit in the set S, the degree $[K : \mathbf{Q}]$ and the discriminant D_K of the number field. The aim of this section is to prove such an inequality using the conditional bound obtained for the integral points in Theorem 3.4, following the method of [Sur07].

With the notations of Section 2, the *abc*-conjecture of D. Masser [Mas02] and J. Oesterlé [Oes88] over number fields can be stated as follows (see [Elk91]).

Conjecture 4.1 (Masser-Oesterlé) *(abc)*
Let F be a number field. For every $\varepsilon > 0$, there exists a real number $c_{\varepsilon,F} > 0$ such that, for a, b, c non zero elements of F satisfying $a + b = c$, we have

$$h_F(a : b : c) < (1 + \varepsilon)\mathrm{rad_F}(a : b : c) + c_{\varepsilon,F}.$$

The result that we will prove in this section is the following.

Theorem 4.2 *Let a, b, c be non zero elements in the number field F satisfying $a + b = c$. Let E be any elliptic curve defined over some number field $K_0 \subset F$. Suppose that for any finite extension K of F, the L-series of E/K satisfies a functional equation (Conjecture 3.2) and that the Birch and Swinnerton-Dyer Conjecture (Conjecture 3.3) holds for the elliptic curve E/K.*

Then, there exist real positive numbers β_1 and β_2 depending at most on the curve E/K_0, the degree $[F : \mathbf{Q}]$ and the absolute value D_F of the discriminant of F, such that

$$h_F(a : b : c) < \exp\{\beta_1 \mathrm{rad_F}(a : b : c)^3 + \beta_2\}.$$

In Theorem 4.2 one may take $\beta_1 = c_1(E/K_0) \cdot [F : \mathbf{Q}]^6 \cdot (\log^+[F : \mathbf{Q}]) \cdot (\log^+ D_F)^2$ and $\beta_2 = c_2(E/K_0)^{[F:\mathbf{Q}]}$, where $c_1(E/K_0)$ and $c_2(E/K_0)$ depend at most on E/K_0.

Roughly speaking, the known results on *abc* over number fields ([Sur07], [GY06], [Győ08]) give an inequality

$$h(a : b : c) \leq \exp\{\beta_1 \mathrm{rad_F}(a : b : c) + \beta_2\}.$$

In [Győ08], one may take $\beta_1 = 1 + \epsilon$. Thus the bound obtained in Theorem 4.2 is less good as the known results. However, our result is obtained by a totally different method, which shows a connection between two conjectures of a very different nature, namely the BSD-conjecture and the *abc*-conjecture. Moreover, improvements in the lower bounds used for linear forms in elliptic logarithms could yield a better inequality, see the discussion in the remarks 4.6 and 4.7 below.

Observe that the validity of the hypothesis (the functional equation and the BSD-conjecture) is only needed for a single elliptic curve E (which we may choose as we wish), but for infinitely many field extensions K/F. In fact, it turns out (see Section 4.1) that we need the hypothesis only for every extension K/F of relative degree $[K : F] \leq \deg(f)$,

where f is any fixed Belyĭ function associated to E. For instance, we may choose the CM curve given by the affine equation $y^2 = x^3 - x$ and for which $(x, y) \mapsto -\frac{1}{4}\frac{(1-x)^2}{x}$ is a Belyĭ map of degree 4. Note also that if the elliptic curve has complex multiplication or is defined over $\mathbf{Q}$, then the conjecture concerning the functional equation is true (see [ST61] and [Wil95]). On the other hand, there is some evidence for the truth of the BSD-conjecture (see [CW77], [GZ86], [Rub87] and [Kol88]).

It is worth noting that with different methods, D. Goldfeld and L. Szpiro [GS95, Theorem 2] proved that there is a relation between the BSD-conjecture and Szpiro's conjecture. The latter one relates the discriminant of the curve with its conductor, namely $D = O(N^{6+\epsilon})$. It is known to imply a weak version of the *abc*-conjecture over $\mathbf{Q}$ (where in conjecture 4.1, $1 + \epsilon$ is replaced by an absolute constant). They proved that if the order of the Tate-Shafarevich group satisfies $|Ш| = O(N^{1/2+\epsilon})$, for every $\epsilon > 0$, for *all* elliptic curves defined over $\mathbf{Q}$, then the relation $D = O(N^{18+\epsilon})$ holds for every elliptic curve over $\mathbf{Q}$. Their proof uses the BSD-conjecture for all elliptic curves over $\mathbf{Q}$ in the case of rank zero, which is a theorem in this case.

4.1 Proof of Theorem 4.2.

Let a, b, c be non zero elements of the number field F such that $a + b = c$. Let S_1 be the set of the prime ideals $\mathfrak{p}$ of F such that $\mathrm{card}\{\mathrm{ord}_{\mathfrak{p}}(a), \mathrm{ord}_{\mathfrak{p}}(b), \mathrm{ord}_{\mathfrak{p}}(c)\} \geq 2$. We then have

$$\mathrm{rad}_{\mathrm{F}}(a : b : c) = \sum_{\mathfrak{p} \in S_1} \log N_{F/\mathbf{Q}}\mathfrak{p} := \Sigma_{S_1}.$$

To our point $(a : b : c)$ will correspond an integral point on an elliptic curve. Choose E any elliptic curve defined over a subfield $K_0 \subset F$. Let

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

be a Weierstrass equation of E, with $A, B \in O_{K_0}$. This curve being fixed once for all and chosen independently of a, b, c, all the parameters depending only on K_0 and E/K_0 will be considered as "constants".

Using a uniformization theorem of G. V. Belyĭ, we can lift the point $(a : b : c)$ to an integral point of the elliptic curve. Indeed, by [Bel79, Theorem 4], there exists a finite surjective morphism $f : E \to \mathbf{P}^1$ defined over K_0, unramified outside 0, 1 and ∞, and sending the origin $O = (0 : 1 : 0)$ of E to $\{0, 1, \infty\}$. Let Q be a point of $E(\overline{F})$ such that

$$f(Q) = (a : c) \in \mathbf{P}^1 \setminus \{0, 1, \infty\}.$$

Since $b = c - a$, the point $(a : c)$ is an S_1-integral point of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the point Q contains all the information about our triple $(a : b : c)$. Moreover, we can use the properties of the elliptic curve.

The Chevalley-Weil theorem (see [Ser97, § 4.2] or [Sur07, Lemma 2.4 and Lemma 2.5] for an affine version), gives us information about the lift.

Lemma 4.3 (Chevalley-Weil) *The field of definition $K = F(Q)$ of the point Q is a finite extension of F of relative degree*

$$[K : F] \leq \deg(f) \tag{12}$$

and which is unramified outside $S = S_1 \cup S_0$, for some finite set of places S_0 of F depending only on the curve E/K_0 and the function f. Moreover, the point Q is S'-integral, where S' is the set of places of K lying above S. [4]

We apply now Theorem 3.4 which gives us a conditional upper bound for the height of the lift of $(a : c)$ depending on the field extension K and the set of places S':

$$h_x(Q) \leq \exp\{\alpha_1^d + \alpha_2\, d^6 (\log^+ D_K)^2\, [\Sigma_{S'} + \log(d \log^+ D_K)], \tag{13}$$

where $d = [K : \mathbf{Q}]$ and α_1 and α_2 depend at most on E/K_0.

To end the proof of Theorem 4.2, it remains to relate $h_x(Q)$ to $h(a : b : c)$ on the one hand, and the parameters d, $\Sigma_{S'}$ and D_K to the radical $\mathrm{rad_F}(a : b : c)$ on the other hand. This is achieved by the following lemma.

Lemma 4.4 *The following inequalities hold :*

1. $h(a : b : c) \ll h_x(Q)$.
2. $d = [K : \mathbf{Q}] \ll [F : \mathbf{Q}]$.
3. $\Sigma_{S'} \ll \mathrm{rad_F}(a : b : c)$
4. $\log D_K \ll \mathrm{rad_F}(a : b : c) + \log D_F$.

where the implicit constants in the symbol $\ll$ depend at most on K_0 and E/K_0.

Proof. Using the basic properties of the heights and because the Belyĭ map f and the x-coordinate are both functions on E, we have

$$h_x(Q) \gg h_f(Q) = \frac{1}{\deg(f)} h(f(Q)) = \frac{1}{\deg(f)} h(a : c) \geq \frac{1}{\deg(f)} (h(a : b : c) - \log 2).$$

Hence the first point is proved. The second point follows from (12) and from the fact that the Belyĭ map depends only on E/K_0. To prove the third item, we first note that

$$\Sigma_S \ll \mathrm{rad_F}(a : b : c) \tag{14}$$

since

$$\Sigma_S = \Sigma_{S_0 \cup S_1} \leq \Sigma_{S_0} + \Sigma_{S_1} = \Sigma_{S_0} + \mathrm{rad_F}(a : b : c)$$

[4] See [BSS11] for a quantitative version with control on the height of the set S_0.

and since S_0 depends only on E/K_0 (and on the choice of f). Now we have, by definition of $\Sigma_{S'}$:

$$\Sigma_{S'} = \sum_{\mathfrak{p}\in S}\sum_{\mathfrak{q}|\mathfrak{p}} \log N(\mathfrak{q}) \leq \sum_{\mathfrak{p}\in S}\sum_{\mathfrak{q}|\mathfrak{p}} \frac{f_{\mathfrak{q}}}{f_{\mathfrak{p}}} \log N(\mathfrak{p}) \leq [K:F]\,\Sigma_S,$$

from which the third item follows, by (12) and (14). Finally, let us prove the last inequality. From Lemma 4.3, the set of places of F on which the extension K/F ramifies is contained in S. We can then apply the following form of the Dedekind-Hensel inequality which is Lemma 3.17 of [BSS11]:

$$\log D_K \leq \Sigma_S + [K:F]\,(\log D_F + 1.26)\,. \tag{15}$$

We conclude with (12) and (14) as before. □

The proof of Theorem 4.2 is now straightforward : It suffices to insert the inequalities of Lemma 4.4 in (13). □

4.2 Some remarks

Remark 4.5 Observe why the bound of Theorem 4.2 has growth order $\exp\{\mathrm{rad_F}(a:b:c)^3\}$. The first remark is that, in the bound for the height of the integral points of the curve obtained in Theorem 3.1, the radical of $(a:b:c)$ appears in several ways.

First, the radical appears, as expected, in the set of places S (see (14)) :

$$\Sigma_S \ll \mathrm{rad_F}(a:b:c).$$

Next, in the bound of Theorem 3.1, the radical appears in the rank, in the height of a system of generators and in the regulator. More precisely, by the Weak Mordell-Weil theorem, $\mathrm{rk}(E/K)$ can be bounded linearly by $\log D_K$ (see Lemma 3.7) which is in turn bounded linearly by the radical of $(a:b:c)$ (it comes from the method, that is, Belyĭ's theorem, the Chevalley-Weil theorem and the Dedekind-Hensel inequality; see Lemma 4.4, Item 4). Thus we have

$$\mathrm{rk}(E/K) \ll \log D_K \ll \mathrm{rad_F}(a:b:c).$$

Using Minkowski's theorem on the successive minima and a lower bound for the height of non-torsion points, $\log(\mathrm{Reg}(E/K))^{-1}$ is bounded by $(\log D_K \,.\, \log\log D_K)$ (Lemma 3.10), hence

$$\log(\mathrm{Reg}(E/K))^{-1} \ll \mathrm{rad_F}(a:b:c)\ .\log(\mathrm{rad_F}(a:b:c)).$$

The factors concerning the heights of the generators are bounded under the BSD-conjecture by Lemma 3.12:

$$(\log^+\log V)^r \leq \exp\{c_1\mathrm{rad_F}(a:b:c)\cdot\log\mathrm{rad_F}(a:b:c)\}$$

and

$$\prod \max\{1,\hat{h}(Q_i)\} \leq \exp\{c_2\mathrm{rad_F}(a:b:c)\cdot\log\mathrm{rad_F}(a:b:c)\},$$

where c_1, c_2 are constants.

In the bound of Theorem 3.1 appears also a factor concerning the rank:

$$r^{2r^2} \leq \exp\{c_3 \mathrm{rad}_{\mathrm{F}}(a:b:c)^2 \log \mathrm{rad}_{\mathrm{F}}(a:b:c)\}.$$

Finally, we have the factors

$$\exp(\gamma_1 dr\Sigma_S) \leq \exp\{c_4 \mathrm{rad}_{\mathrm{F}}(a:b:c)^2\} \tag{16}$$

and

$$\exp(8r^2\Sigma_S) \leq \exp\{c_5 \mathrm{rad}_{\mathrm{F}}(a:b:c)^3\}, \tag{17}$$

the latter one being the biggest contribution to the radical. It comes from the factor $p^{8n(n+1)}$ of the bound of N. Hirata (see Theorem 4.6 in [BS12]) for the linear form in elliptic logarithms in the ultrametric case, where n is the number of logarithms (essentially $n = r$) and p is the prime number lying below the ultrametric place.

Remark 4.6 According to N. Hirata, it seems possible that in the lower bound of linear forms of elliptic logarithms in the ultrametric case, a refinement on p of the order p^n could be obtained (instead of $p^{8n(n+1)}$), giving a contribution of the form $\exp\{c_6 \mathrm{rad}_{\mathrm{F}}(a:b:c)^2\}$, instead of (17). This would lead to a final bound in Theorem 4.2

$$h_F(a:b:c) < \exp\{\beta_1 \mathrm{rad}_{\mathrm{F}}(a:b:c)^2 \log \mathrm{rad}_{\mathrm{F}}(a:b:c) + \beta_2\}.$$

The worse contribution in this case would be the factor r^{2r^2} which appears both in the ultrametric and the archimedean lower bounds for linear forms in elliptic logarithms (theorems 4.2 and 4.6 in [BS12]). It seems reasonable to conjecture that the lower bounds for linear forms in logarithms are still valid with the smaller factor r^r instead of r^{2r^2}. In that case, the worse contributions would be the factors p^n and $\exp(\gamma_1 dr\Sigma_S)$, both yielding a factor of the shape $\exp\{c_7 \mathrm{rad}_{\mathrm{F}}(a:b:c)^2\}$. The presence of the factor $\exp(\gamma_1 dr\Sigma_S)$ shows that even a drastic improvement in the dependence on p and on the number of logarithms would not be sufficient to get a final inequality better than $\exp\{c_7 \mathrm{rad}_{\mathrm{F}}(a:b:c)^2\}$.

Remark 4.7 S. David and N. Hirata ([DHK09]) suggested an elliptic analog of the classical Lang-Waldschmidt conjecture. We quote here the following particular case.

Conjecture 4.8 (Elliptic Lang-Waldschmidt) *Let n be a rational integer ≥ 1. There exists a strictly positive real number $C(n)$ such that the following property holds. Let K be a number field of degree d over $\mathbf{Q}$. Let E/K be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$. Denote $h_E = \max\{1, h(1:A:B)\}$. Let $b_0, b_1, \ldots, b_n$ be rational integers and $B = \max_{1\leq i\leq n}\{|b_i|\}$. Let γ_i be points in $E(K) \subset \mathbf{P}^2(K)$ and u_i be an elliptic logarithm of γ_i. Put $\mathcal{L} = b_0 + b_1u_1 + \cdots + b_nu_n$. If $\mathcal{L} \neq 0$, then*

$$\log|\mathcal{L}| \geq -C(n)d^2(\log B + h_E)(\sum_{i=1}^{n} \max\{1, \hat{h}(\gamma_i)\}).$$

Following the results in the classical (non elliptic) case, we can expect that $C(n) = c_1^n$, where c_1 is some absolute constant. For the ultrametric analogue, by considering Theorem 1' of [Yu94], we can conjecture a constant of the form $C(p, n, d) = c_1^n \cdot p^{c_2 d}$, where c_1 and c_2 are absolute. Using Conjecture 4.8 with $C(n) = c_1^n$, instead of David's theorem (Theorem 4.2 of [BS12]), together with an ultrametric analogue of Conjecture 4.8 with $C(p, n, d) = c_1^n \cdot p^{c_2 d}$, instead of Hirata's theorem (Theorem 4.6 of [BS12]), our method would give the following *abc*-type inequality

$$h_F(a : b : c) < \exp\{\beta_1 \mathrm{rad}_{\mathrm{F}}(a : b : c) \cdot \log \mathrm{rad}_{\mathrm{F}}(a : b : c) + \beta_2\}.$$

Indeed, with the notation of [BS12], the factor $\exp(\gamma_1 dr\Sigma_S)$ comes from the factor $\nu_{\mathfrak{p}}^{2r}$, where $\nu_{\mathfrak{p}}$ is the exponent of a certain group satisfying $\nu_{\mathfrak{p}} \leq p^{c_8 d}$. If we repeat the arguments given in [BS12] for the proof of Theorem 3.1 using Conjecture 4.8, we see that we now get $r\nu_{\mathfrak{p}}^2$ instead of $\nu_{\mathfrak{p}}^{2r}$, and thus the factor $\exp(\gamma_1 dr\Sigma_S)$ is replaced by $r\exp(\gamma_1 d\Sigma_S)$, giving a contribution $\exp(c_9 \mathrm{rad}_{\mathrm{F}}(a : b : c))$ instead of (16). Hence the worse contribution here would come from $\sum_{1\leq i\leq r} \max\{1, \hat{h}(Q_i)\}$ which we bound, under the BSD-conjecture, by

$$r \cdot \max_{1\leq i\leq r}\{1, \hat{h}(Q_i)\} \ll r(r!)^4 (\frac{\kappa_4}{d^3(\log d)^2})^{1-r} \cdot D_K^{3/2} \leq \exp\{c_{10}\mathrm{rad}_{\mathrm{F}}(a : b : c) \cdot \log \mathrm{rad}_{\mathrm{F}}(a : b : c)\}.$$

References

[Bak98] A. Baker. Logarithmic forms and the *abc*-conjecture. In *Number theory (Eger, 1996)*, pages 37–44. de Gruyter, Berlin, 1998.

[Bel79] G. V. Belyĭ. Galois extensions of a maximal cyclotomic field. *(Russian) Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 1979. Translation in *Math. USSR-Izv.* 14(2):247–256, 1980.

[Bil97] Y. Bilu. Quantitative Siegel's theorem for Galois coverings. *Compositio Math.*, 106(2):125–158, 1997.

[Bil02] Y. Bilu. Baker's method and modular curves. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 73–88. Cambridge Univ. Press, Cambridge, 2002.

[BK94] A. Brumer and K. Kramer. The conductor of an abelian variety. *Compositio Math.*, 92(2):227–248, 1994.

[BS12] V. Bosser and A. Surroca. Upper bound for the height of S-integral points on elliptic curves. *arXiv:1208.2693*, to appear in Ramanujan Journal, 17 pages, 2012.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[BSS11] Y. Bilu, M. Strambi, and A. Surroca. A quantitative Chevalley-Weil theorem for curves. *arXiv:0908.1233*, 2011.

[Cas97] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[CS86] G. Cornell and J. H. Silverman, editors. *Arithmetic geometry*. Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.

[CW77] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[Dav95] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[DHK09] S. David and N. Hirata-Kohno. Linear forms in elliptic logarithms. *J. Reine Angew. Math.*, 628:37–89, 2009.

[Elk91] N. D. Elkies. *ABC* implies Mordell. *Internat. Math. Res. Notices*, (7):99–109, 1991.

[Gro82] B. H. Gross. On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. In *Number theory related to Fermat's last theorem (Cambridge, Mass., 1981)*, volume 26 of *Progr. Math.*, pages 219–236. Birkhäuser Boston, Mass., 1982.

[GS95] D. Goldfeld and L. Szpiro. Bounds for the order of the Tate-Shafarevich group. *Compositio Math.*, 97(1-2):71–87, 1995. Special issue in honour of Frans Oort.

[GY06] K. Győry and K. Yu. Bounds for the solutions of S-unit equations and decomposable form equations. *Acta Arith.*, 123(1):9–41, 2006.

[Győ02] K. Győry. Solving Diophantine equations by Baker's theory. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 38–72. Cambridge Univ. Press, Cambridge, 2002.

[Győ08] K. Győry. On the *abc* conjecture in algebraic number fields. *Acta Arith.*, 133(3):281–295, 2008.

[GZ86] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Hir12] N. Hirata. Minorations de formes linéaires de logarithmes elliptiques p-adiques. *Work in progress*, 2012.

[Kol88] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[LRS93] P. Lockhart, M. Rosen, and J. H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993.

[Man71] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.

[Mas75] D. W. Masser. *Elliptic functions and transcendence*. Springer-Verlag, Berlin, 1975. Lecture Notes in Mathematics, Vol. 437.

[Mas89] D. W. Masser. Counting points of small height on elliptic curves. *Bull. Soc. Math. France*, 117(2):247–265, 1989.

[Mas02] D. W. Masser. On *abc* and discriminants. *Proc. Amer. Math. Soc.*, 130(11):3141–3150 (electronic), 2002.

[MB90] Laurent Moret-Bailly. Hauteurs et classes de Chern sur les surfaces arithmétiques. *Astérisque*, (183):37–58, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[Mes86] J.-F. Mestre. Formules explicites et minorations de conducteurs de variétés algébriques. *Compositio Math.*, 58(2):209–232, 1986.

[Mil72] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[Oes88] J. Oesterlé. Nouvelles approches du "théorème" de Fermat. *Astérisque*, (161-162):Exp. No. 694, 4, 165–186 (1989), 1988. Séminaire Bourbaki, Vol. 1987/88.

[OT89] T. Ooe and J. Top. On the Mordell-Weil rank of an abelian variety over a number field. *J. Pure Appl. Algebra*, 58(3):261–265, 1989.

[Phi99] P. Philippon. Quelques remarques sur des questions d'approximation diophantienne. *Bull. Austral. Math. Soc.*, 59(2):323–334, 1999.

[Rém05] G. Rémond. Intersection de sous-groupes et de sous-variétés. I. *Math. Ann.*, 333(3):525–548, 2005.

[Rém10] G. Rémond. Nombre de points rationnels des courbes. *Proc. Lond. Math. Soc. (3)*, 101:759–794, 2010.

[Rub87] K. Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 89(3):527–559, 1987.

[Ser97] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kano Memorial Lectures, 1.

[ST61] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[ST86] C. L. Stewart and R. Tijdeman. On the Oesterlé-Masser conjecture. *Monatsh. Math.*, 102(3):251–257, 1986.

[Sur04] A. Surroca. Siegel's theorem and the *abc* conjecture. *Riv. Mat. Univ. Parma (7)*, 3*:323–332, 2004.

[Sur07] A. Surroca. Sur l'effectivité du théorème de Siegel et la conjecture *abc*. *J. Number Theory*, 124:267–290, 2007.

[Sur12] A. Surroca. On the Mordell-Weil group and the Tate-Shafarevich group of an abelian variety. *arXiv:0801.1054*, 22 pages, 2012.

[SY91] C. L. Stewart and K. Yu. On the *abc* conjecture. *Math. Ann.*, 291(2):225–230, 1991.

[SY01] C. L. Stewart and K. Yu. On the *abc* conjecture. II. *Duke Math. J.*, 108(1):169–181, 2001.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[Yu94] K. Yu. Linear forms in p-adic logarithms. III. *Compositio Math.*, 91(3):241–276, 1994.

Vincent Bosser
Laboratoire Nicolas Oresme
Université de Caen
F14032 Caen cedex
France

Andrea Surroca
Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel
Switzerland