HAL
open science

Upper bound for the height of S-integral points on elliptic curves

Vincent Bosser, Andrea Surroca

To cite this version:

Vincent Bosser, Andrea Surroca. Upper bound for the height of S-integral points on elliptic curves. Ramanujan Journal, 2013, 32 (1), 10.1007/s11139-012-9440-4 . hal-02151921

HAL Id: hal-02151921

https://normandie-univ.hal.science/hal-02151921v1

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:1208.2693v1 [math.NT] 13 Aug 2012

Upper bound for the height of S-integral points on elliptic curves

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

August 15, 2012

Abstract. We establish new upper bounds for the height of the S-integral points of an elliptic curve. This bound is explicitly given in terms of the set S of places of the number field K involved, but also in terms of the degree of K, as well as the rank, the regulator and the height of a basis of the Mordell-Weil group of the curve. The proof uses the elliptic analogue of Baker's method, based on lower bounds for linear forms in elliptic logarithms.

2010 Mathematics Subject Classification. Primary: 11G50; Secondary: 11G05, 11J86, 14G05.

1 Introduction

A fundamental problem in Diophantine Geometry is to get effective versions of known qualitative results. For example the classical finiteness theorem of Siegel asserts that the set of integral points of an affine algebraic curve of genus greater than one or of genus zero with at least 3 points at infinity is finite. For that curves of genus greater than 2, Siegel's theorem is superseded by Faltings' theorem which asserts that the set of rational points is finite. These are qualitative statements, but not effective. To effectively find these points, say, in a fixed number field, it would suffice to find an effective upper bound for the height of the points. Nowadays, the results of this kind which are known come from Baker's method (based on non trivial lower bounds for linear forms in logarithms). They all concern integral points. The method can be applied for certain classes of curves, in particular, for elliptic curves ([BC70]). Generalizing an idea of Gel'fond, S. Lang [Lan78] has shown that one can also bound the height of integral points of an elliptic curve E using lower bounds for linear forms in *elliptic* logarithms, in a more natural way than using classical logarithms.

Let E be an elliptic curve defined over a number field K_0, let K/K_0 be any finite extension and let S be a finite set of finite places of K. In this paper we obtain new upper

*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.

bounds for the height of the S-integral points of $E(K)$, using lower bounds in linear forms in elliptic logarithms (Theorem 3.1).

This method was first applied successfully by D. Masser [Mas75, Appendix IV] when $K = K_0 = \mathbf{Q}$, the curve E has complex multiplication and $S = \emptyset$. To this end he used his own lower bounds for usual (archimedean) elliptic logarithms. D. Bertrand [Ber78] then established such lower bounds for $\mathfrak{p}$-adic elliptic logarithms, which allowed him to treat the case $K = K_0$ and S arbitrary (again for curves with complex multiplication). Applying 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, we deal here with the general case of an arbitrary elliptic curve defined over K_0 and of an arbitrary field extension K/K_0. Our results improve the previous results of D. Bertrand. Moreover, contrary to the previous works, the bound we obtain for the height of the S-integral points is not only given in terms of the set S, but also in terms of the number field K. More precisely, the "constant" which occurred in the previous works is here explicitly given in terms of the degree $[K : \mathbf{Q}]$, the rank of the Mordell-Weil group $E(K)$, the heights of generators of the free part of $E(K)$, and the regulator of E/K (but we do not make explicit the dependence on E/K_0). As mentioned at the end of Section 4.3, it is possible to derive from our main result a conditional upper bound in terms only of the degree $[K : \mathbf{Q}]$, the discriminant of K and the set of places S.

For convenience to the reader, we have gathered in Section 2 the notations which will be used throughout the text. We state the main theorem in Section 3 and prove it in Section 4.

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 $\sigma : K \hookrightarrow \mathbf{C}$ (we will often 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:

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

Let $E \subset \mathbf{P}^2$ 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 will also denote by O the zero element of $E(K)$.

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

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

If the elliptic curve is defined by a Weiertrass equation $y^2 = x^3 + Ax + B$ with A, B in O_K, then we have the origin $O = (0 : 1 : 0)$. If $Q \neq O$ is a point of E, we then 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 the whole text, we will fix a number field K_0 and an elliptic curve E defined over K_0. Since we do not explicit any dependence on E/K_0, we will call "constant" any quantity depending on E/K_0. This convention about constants will apply in particular to the implicit constant involved in the symbol $\ll$, where $X \ll Y$ means here that $X \leq c(E/K_0)Y$, where $c(E/K_0) \geq 1$ is a number depending at most on E/K_0.

3 Statement of the result

Let K_0 be a fixed number field, and let $E \subset \mathbf{P}^2$ be an elliptic curve defined by a Weierstrass equation

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

with $A, B \in O_{K_0}$. Let K be a finite extension of K_0 and $S \subset M_K^0$ a finite set of places of K.

According to the notations of Section 2, we put $r = \mathrm{rk}(E(K))$, we denote by $(Q_1, \ldots, Q_r)$ any basis of the free part of the Mordell-Weil group $E(K)$, and we write $\mathrm{Reg}(E/K)$ for the regulator of E/K. We further set

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

and we define the real number V by

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

The main result of this article is the following:

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

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

The bounds obtained by classical Baker's method often depend on d, D_K and Σ_S. The bound of Theorem 3.1 depends on d and Σ_S, as well as on the rank $\mathrm{rk}(E(K))$, the heights $\hat{h}(Q_i)$ and the regulator of E/K. Because of the different nature of the parameters involving K, it makes sense to compare our result with the results obtained by classical Baker's method only when the number field is fixed.

Denote by s the cardinal of S, by $P(S) := \{p \text{ prime} \mid \exists v \in S, v|p\}$ the residue characteristics of S, and by P its maximum. For $K = \mathbf{Q}$, L. Hajdu and T. Herendi [HH98] obtained the following result:

$$\max\{h(x), h(y)\} \leq (\kappa_1 s + \kappa_2)\, 10^{38\, s+86}\, (s+1)^{20\, s+35}\, P^{24}\, (\log^+(P))^{4\, s+2},$$

where κ_1 and κ_2 depend at most on A and B. For any K, the Corollary 6.9 of [Sur07] gives:

$$h_x(Q) \leq k_0 c_d^{s+k_1}\, s^{20\, s+k_2}\, P^{4\, d}\, (\log P)^{8\, s+k_3}\, e^{\gamma(E,K,S)}\, \gamma(E,K,S)^{8d-2},$$

where the numbers k_i depend only on E/K_0, c_d depends only on the degree d and $\gamma(E,K,S) = 4\,(\log D_K + \Sigma_S + k_4 + 4\,\log 4\,d\,\frac{\Sigma_S+k_5}{\log(\Sigma_S+k_5)})$. In order to compare these different bounds we may use the following inequalities (for the last one, one may use the Prime Number Theorem, see, for example [Sur07, Lemma 2.1]):

$$(d \cdot \mathrm{card} P(S))^{-1}\Sigma_S \leq \log P \leq \Sigma_S, \text{and}$$

$$\mathrm{card}(S) \leq d \cdot \mathrm{card} P(S) \leq 4d\frac{\Sigma_S}{\log \Sigma_S}.$$

One can see that, for a fixed K, the bounds of [Sur07, Corollary 6.9] and Theorem 3.1 are of the same order and that for $K = \mathbf{Q}$ the bound of [HH98] is stronger.

4 Proof of Theorem 3.1

To prove Theorem 3.1, we will determine an upper bound for $|x(Q)|_v$ for each $v \in M_K$ and then sum over all the places v using the formula (1). The upper bound for $|x(Q)|_v$ will be obtained using the explicit lower bounds for linear forms in elliptic logarithms of [Hir12] and [Dav95]. In the next section, we first treat the case of an archimedean place v. Then, in Section 4.2, we handle the case where v is ultrametric. We can then prove Theorem 3.1 in Section 4.3.

In the next sections, we denote by $\kappa_1, \kappa_2, \ldots, c_1, c_2, \ldots$ positive real numbers (which we will call "constants") depending at most on A and B, *i.e.* on the curve E/K_0. We use the greek letters for the constants appearing in the statements and the latin letters for the proofs. In each proof we start counting by c_1.

4.1 The archimedean case

In this section we fix an archimedean place v of K, and we assume that the rank r of the group $E(K)$ is non zero. We denote by $\sigma : K \hookrightarrow \mathbf{C}$ the embedding corresponding to v, and by E_σ the elliptic curve defined by

$$y^2 = x^3 + \sigma(A)x + \sigma(B).$$

The homomorphism σ obviously induces a group isomorphism $\sigma : E(K) \simeq E_\sigma(\sigma(K))$.

Put $g_{2,\sigma} = -4\sigma(A)$ and $g_{3,\sigma} = -4\sigma(B)$. Then E_σ is isomorphic to the elliptic curve defined by

$$Y^2 = 4X^3 - g_{2,\sigma}X - g_{3,\sigma} \tag{5}$$

under the substitution $X = x$, $Y = 2y$. Let Λ_σ be the lattice of $\mathbf{C}$ with invariants $g_{2,\sigma}$, $g_{3,\sigma}$. We will consider the exponential map of E_σ, which is given by

$$\begin{array}{rccl} \exp_\sigma : & \mathbf{C} & \to & E_\sigma(\mathbf{C}) \\ & z & \mapsto & \left\{ \begin{array}{l} (\wp_\sigma(z) : \wp'_\sigma(z)/2 : 1) \text{ if } z \notin \Lambda_\sigma \\ (0:1:0) \text{ if } z \in \Lambda_\sigma, \end{array} \right. \end{array} \tag{6}$$

where $\wp_\sigma$ is the Weierstrass function associated to the lattice Λ_σ. It induces a group isomorphism $\mathbf{C}/\Lambda_\sigma \simeq E_\sigma(\mathbf{C})$. Let $(\omega_{1,\sigma}, \omega_{2,\sigma})$ be a basis of the lattice Λ_σ, and denote by Π_σ the associated fundamental parallelogram centered at zero. Then $\exp_\sigma|_{\Pi_\sigma} : \Pi_\sigma \to E_\sigma(\mathbf{C})$ is bijective and we will denote by $\psi_\sigma : E_\sigma(\mathbf{C}) \to \Pi_\sigma$ its inverse map (the elliptic logarithm).

Proposition 4.1 *Let Q be a non-torsion point of $E(K)$. Write $Q = m_1Q_1 + \cdots + m_rQ_r + Q_{r+1}$, where $Q_{r+1} \in E(K)$ is a torsion point and $m_i \in \mathbf{Z}$, $1 \le i \le r$, and define $M := \max\{|m_1|, \ldots, |m_r|\}$. Recall that $\log V := \max\{\hat{h}(Q_i); 1 \le i \le r\}$. Then we have*

$$\log|x(Q)|_\sigma \le \kappa_1^{r^2} r^{2r^2} d^{2r+8} (\log^+ d)^{r+5} (\log^+ M)(\log^+ \log M) \times (\log^+ \log V)^{r+5} \prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\}.$$

To prove this we will use the following result, which is a consequence of Theorem 2.1 of [Dav95] (in which we have chosen $E = e$).

Theorem 4.2 (S. David) *Let $m_1, \ldots, m_{r+1}, n_1, n_2$ be rational integers, and let $\gamma_1, \ldots, \gamma_{r+1}$ be elements of $E_\sigma(\sigma(K))$. Define $u_i = \psi_\sigma(\gamma_i)$, $1 \le i \le r+1$, and put*

$$\mathcal{L} = m_1u_1 + \cdots + m_{r+1}u_{r+1} + n_1\omega_{1,\sigma} + n_2\omega_{2,\sigma}.$$

Set further $B = \max\{|m_1|, \ldots, |m_{r+1}|, |n_1|, |n_2|\}$ and $\log W = \max\{\hat{h}(\gamma_i), 1 \le i \le r+1\}$. If $\mathcal{L} \ne 0$, then

$$\log|\mathcal{L}| \ge -\kappa_2^{r^2} r^{2r^2} d^{2r+8} (\log^+ d)^{r+5} (\log^+ B)(\log^+ \log B) \times (\log^+ \log W)^{r+5} \prod_{i=1}^{r+1} \max\{1, \hat{h}(\gamma_i)\}.$$

Proof of Proposition 4.1. Let Q, Q_{r+1}, $m_1, \ldots, m_r$ and M be as in the Proposition. We set $\gamma_i = \sigma(Q_i) \in E_\sigma(\mathbf{C})$ and $u_i = \psi_\sigma(\gamma_i)$, $1 \le i \le r+1$. We have $\sigma(Q) = m_1\gamma_1 + \cdots + m_r\gamma_r + \gamma_{r+1}$ and thus, by definition of ψ_σ there exist $n_1, n_2 \in \mathbf{Z}$ such that

$$\psi_\sigma(\sigma(Q)) = m_1u_1 + \cdots + m_ru_r + u_{r+1} + n_1\omega_{1,\sigma} + n_2\omega_{2,\sigma}. \tag{7}$$

Since the function $\wp_\sigma$ has a pole of order 2 at zero, there exists a constant $c_{1,\sigma} = c_1(\sigma(A), \sigma(B)) > 0$ such that $|z^2\wp_\sigma(z)| \le c_{1,\sigma}$ for all z in Π_σ. Applying this to $z = \psi_\sigma(\sigma(Q))$ and putting $c_1 := \max_\sigma\{c_{1,\sigma}\}$ (which depends only on the restriction of σ to K_0 hence on E/K_0 only), we find that

$$|x(Q)|_\sigma \le c_1 \cdot |\psi_\sigma(\sigma(Q))|^{-2}$$

i.e.

$$\log|x(Q)|_\sigma \le \log c_1 - 2\log|\psi_\sigma(\sigma(Q))|. \tag{8}$$

In order to use Theorem 4.2, observe that since all the norms on $\mathbf{R}^2$ are equivalent, there exists a constant $c_{2,\sigma} = c_2(\sigma(A), \sigma(B)) > 0$ such that $|x\omega_{1,\sigma} + y\omega_{2,\sigma}| \ge c_{2,\sigma}\max\{|x|, |y|\}$

for all real numbers $x, y \in \mathbf{R}$. Therefore we have, using (7) and since obviously $|u| \leq (|\omega_{1,\sigma}| + |\omega_{2,\sigma}|)/2$ for every u belonging to the fundamental parallelogram Π_σ,

$$c_{2,\sigma} \max\{|n_1|, |n_2|\} \leq |\psi_\sigma(\sigma(Q))| + M(|u_1| + \cdots + |u_{r+1}|) \leq c_{3,\sigma}(1 + (r+1)M) \leq c_{4,\sigma} r M.$$

Hence

$$\max\{|n_1|, |n_2|\} \leq c_2 r M$$

with $c_2 = \max_\sigma\{c_{4,\sigma}/c_{2,\sigma}\}$ (which depends only on E/K_0 for the same reason as above), and so

$$B := \max\{1, |m_1|, \ldots, |m_r|, |n_1|, |n_2|\} \leq c_3 r M. \tag{9}$$

Applying now Theorem 4.2 to the linear form (7) (which is not zero since Q is not torsion) and taking into account (9), we deduce

$$\log|\psi_\sigma(\sigma(Q))| \geq -c_4^{r^2} r^{2r^2} d^{2r+8} (\log^+ d)^{r+5} (\log^+ M)(\log^+ \log M) \\ \times (\log^+ \log V)^{r+5} \prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\}.$$

This estimate, together with (8), yields the proposition. □

4.2 The ultrametric case

We fix here an ultrametric place v of K associated to a prime ideal $\mathfrak{p}$ lying above the prime number p, and we assume again that the rank r of the group $E(K)$ is non zero. We will prove :

Proposition 4.3 *Let Q be a non-torsion point of $E(K)$. Write $Q = m_1 Q_1 + \cdots + m_r Q_r + Q_{r+1}$, where $Q_{r+1} \in E(K)$ is a torsion point and $m_i \in \mathbf{Z}$, $1 \leq i \leq r$, and define $M := \max\{|m_1|, \ldots, |m_r|\}$. Recall that $\log V := \max\{\hat{h}(Q_i); 1 \leq i \leq r\}$. Then we have*

$$\log|x(Q)|_\mathfrak{p} \leq \kappa_3^{r^2} r^{2r^2} p^{8r^2 + \kappa_4 dr} d^{9r+14} (\log^+ d)^{r+3} (\log^+ M) \\ \times (\log^+ \log V)^{r+3} \prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\}.$$

To prove this Proposition we will use the v-adic exponential map of E, whose definition and properties we now recall for reader's convenience. By [Wei36] (see also [Lut37]), there exists a unique function $\psi(z)$ analytic in a neighbourhood of 0 in $K_\mathfrak{p}$ which satisfies

$$\psi'(z) = (1 + Az^4 + Bz^6)^{-\frac{1}{2}}; \;\; \psi(0) = 0$$

(where we define of course $(1+t)^{-1/2} = 1 - t/2 + \cdots$ for t in $K_\mathfrak{p}$ with $|t|_\mathfrak{p}$ small). It is not difficult to see that this function ψ is analytic in the open disk

$$\mathcal{C}_\mathfrak{p} = \{z \in K_\mathfrak{p}; |z|_\mathfrak{p} < p^{-\lambda_p}\},$$

where $\lambda_p = (p-1)^{-1}$ if $p \neq 2$ and $\lambda_p = 1/2$ if $p = 2$. Moreover, one can show that for $z \in \mathcal{C}_\mathfrak{p}$, $z \neq 0$, we have

$$\psi(z) = z + \sum_{n \geq 2} \psi_n z^n$$

with $|\psi_n z^n|_\mathfrak{p} < |z|_\mathfrak{p}$ for all $n \geq 2$. It follows from results of non-archimedean analysis (see *e.g.* [Gün66, Satz 2]) that ψ induces a bijection $\psi : \mathcal{C}_\mathfrak{p} \to \mathcal{C}_\mathfrak{p}$, whose inverse map is also analytic. Let $\varphi = \psi^{-1} : \mathcal{C}_\mathfrak{p} \to \mathcal{C}_\mathfrak{p}$ be this inverse map. Then φ is the unique solution on $\mathcal{C}_\mathfrak{p}$ of the differential equation

$$y' = (1 + Ay^4 + By^6)^{\frac{1}{2}}; \;\; y(0) = 0.$$

Moreover, $|\varphi(z)|_\mathfrak{p} = |z|_\mathfrak{p}$ and $\varphi(-z) = -\varphi(z)$ for all $z \in \mathcal{C}_\mathfrak{p}$ (note that the similar results proved in [Lut37, p. 246] give a smaller disk than our $\mathcal{C}_\mathfrak{p}$ when $p = 2$).

Set now $\wp = 1/\varphi^2$. One has on $\mathcal{C}_\mathfrak{p} \setminus \{0\}$

$$\frac{1}{4}\wp'^2 = \wp^3 + A\wp + B.$$

The v-adic exponential map of E is then defined by

$$\begin{array}{rccl} \exp_\mathfrak{p} : & \mathcal{C}_\mathfrak{p} & \to & E(K_\mathfrak{p}) \\ & z & \mapsto & \begin{cases} (\wp(z) : \wp'(z)/2 : 1) \text{ if } z \neq 0 \\ O \text{ if } z = 0 \end{cases} \end{array}$$

or equivalently by

$$\exp_\mathfrak{p}(z) = (\varphi(z) : -\varphi'(z) : \varphi^3(z)) \tag{10}$$

for all $z \in \mathcal{C}_\mathfrak{p}$. This is an injective group homomorphism which is not surjective. Let $\mathcal{U}_\mathfrak{p} = \exp_\mathfrak{p}(\mathcal{C}_\mathfrak{p})$ be the image of the exponential map. It is known that the group $E(K_\mathfrak{p})/\mathcal{U}_\mathfrak{p}$ is finite. We will need an explicit upper bound for the exponent of this group.

Lemma 4.4 *The exponent $\nu_\mathfrak{p}$ of the group $E(K_\mathfrak{p})/\mathcal{U}_\mathfrak{p}$ satisfies*

$$\nu_\mathfrak{p} \leq p^{\kappa_5 d}.$$

Proof. In what follows we will denote by $\mathfrak{O}_\mathfrak{p} = \{z \in K_\mathfrak{p}; |z|_\mathfrak{p} \leq 1\}$ the valuation ring of $K_\mathfrak{p}$, by $\mathfrak{M}_\mathfrak{p} = \{z \in K_\mathfrak{p}; |z|_\mathfrak{p} < 1\}$ the maximal ideal of $\mathfrak{O}_\mathfrak{p}$, by π a uniformizer (*i.e.* $\mathfrak{M}_\mathfrak{p} = \pi\mathfrak{O}_\mathfrak{p}$), and by $k(\mathfrak{p}) = \mathfrak{O}_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$ the residue field of $\mathfrak{O}_\mathfrak{p}$.

Let $E_\mathfrak{p} \subset \mathbf{P}_2$ be a minimal Weierstrass model of E at $\mathfrak{p}$. We know that there is an admissible change of coordinates

$$f : K_\mathfrak{p}^2 \to K_\mathfrak{p}^2, \quad (x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \tag{11}$$

with $u, r, s, t \in \mathfrak{O}_\mathfrak{p}$, such that f induces a group isomorphism $f : E_\mathfrak{p}(K_\mathfrak{p}) \simeq E(K_\mathfrak{p})$. Thus, it suffices to estimate the exponent of the group $E_\mathfrak{p}(K_\mathfrak{p})/\mathfrak{U}_\mathfrak{p}$, where $\mathfrak{U}_\mathfrak{p} := f^{-1}(\mathcal{U}_\mathfrak{p})$.

We now claim that the group $\mathcal{U}_\mathfrak{p}$ is explicitly given by

$$\mathcal{U}_\mathfrak{p} = \{(x:y:1) \in E(K_\mathfrak{p});\ |x|_\mathfrak{p} > p^{2\lambda_p}\} \cup \{O\}. \tag{12}$$

Indeed, $\mathcal{U}_\mathfrak{p}$ is clearly contained in the right-hand side of (12) since $|\varphi(z)|_\mathfrak{p} = |z|_\mathfrak{p}$ for all $z \in \mathcal{C}_\mathfrak{p}$. Conversely, if $(x:y:1) \in E(K_\mathfrak{p})$ satisfies $|x|_\mathfrak{p} > p^{2\lambda_p}$, then we can write

$$y^2/x^2 = x(1 + \frac{A}{x^2} + \frac{B}{x^3}) = x(1+t)$$

with

$$|t|_\mathfrak{p} = |\frac{A}{x^2} + \frac{B}{x^3}|_\mathfrak{p} < p^{-4\lambda_p}.$$

It follows that $(1+t)$ is a square in $K_\mathfrak{p}$ since then the series $(1+t)^{1/2} = 1 + t/2 - t^2/8 + \cdots$ converges in $K_\mathfrak{p}$ (for $p=2$ it converges as soon as $|t|_\mathfrak{p} < |2|_\mathfrak{p}^2$), and thus x is also a square in $K_\mathfrak{p}$, say $x = \alpha^2$. We then have α^{-1} in $\mathcal{C}_\mathfrak{p}$, and it follows that there exists z in $\mathcal{C}_\mathfrak{p}$ such that $\alpha^{-1} = \varphi(z)$, *i.e.* $x = \varphi(z)^{-2}$. We have moreover $y^2 = x^3 + Ax + B = \varphi'^2(z)/\varphi^6(z)$. Hence, taking $-z$ instead of z if necessary, we may choose z so that $y = -\varphi'(z)/\varphi^3(z)$. Therefore, we have found z in $\mathcal{C}_\mathfrak{p}$ such that $\exp_\mathfrak{p}(z) = (x:y:1)$. This proves (12).

Using the formulas (11) and the ultrametric inequality, we deduce from this

$$\begin{aligned}\mathfrak{U}_\mathfrak{p} &= \{(x:y:1) \in E_\mathfrak{p}(K_\mathfrak{p});\ |x|_\mathfrak{p} > |u|_\mathfrak{p}^{-2} p^{2\lambda_p}\} \cup \{0\} \\ &= \{(x:y:1) \in E_\mathfrak{p}(K_\mathfrak{p});\ \mathrm{ord}_\mathfrak{p}(x)/2 < -(e_\mathfrak{p}\lambda_p + \mathrm{ord}_\mathfrak{p}(u))\} \cup \{0\}.\end{aligned}$$

In other words, if we denote the canonical $\mathfrak{p}$-adic filtration of $E_\mathfrak{p}$ as in [Hus04], Chapter 14, by

$$E_\mathfrak{p}(K_\mathfrak{p}) \supset E_\mathfrak{p}^{(0)}(K_\mathfrak{p}) \supset \cdots \supset E_\mathfrak{p}^{(n)}(K_\mathfrak{p}) \supset \cdots,$$

we see that $\mathfrak{U}_\mathfrak{p} = E_\mathfrak{p}^{(n)}(K_\mathfrak{p})$ with $n = [e_\mathfrak{p}\lambda_p] + \mathrm{ord}_\mathfrak{p}(u) + 1$.

Estimating the exponent of the group $E_\mathfrak{p}(K_\mathfrak{p})/\mathfrak{U}_\mathfrak{p} = E_\mathfrak{p}(K_\mathfrak{p})/E_\mathfrak{p}^{(n)}(K_\mathfrak{p})$ now easily follows from well-known properties of the $\mathfrak{p}$-adic filtration. Indeed, let $\Delta_\mathfrak{p} \in K_\mathfrak{p}$ be the minimal discriminant of the elliptic curve E at $\mathfrak{p}$. By the addendum to Theorem 3 of [Tat74] we first have

$$[E_\mathfrak{p}(K_\mathfrak{p}) : E_\mathfrak{p}^{(0)}(K_\mathfrak{p})] \leq \max\{4, \mathrm{ord}_\mathfrak{p}(\Delta_\mathfrak{p})\}, \tag{13}$$

and by [Sil94, Proposition VII.2.1] we have

$$[E_\mathfrak{p}^{(0)}(K_\mathfrak{p}) : E_\mathfrak{p}^{(1)}(K_\mathfrak{p})] \leq 2\mathrm{card}(k(\mathfrak{p})) + 1 = 2p^{f_\mathfrak{p}} + 1 \leq \frac{5}{2}p^{f_\mathfrak{p}}. \tag{14}$$

On the other hand, if we define $\widehat{\mathfrak{M}_\mathfrak{p}^m}$ for every $m \geq 1$ as the set $\mathfrak{M}_\mathfrak{p}^m$ endowed with the group structure given by the formal group law associated to $E_\mathfrak{p}$, we know that the map $t : E_\mathfrak{p}^{(m)}(K_\mathfrak{p}) \to \widehat{\mathfrak{M}_\mathfrak{p}^m}$ defined by $t(O) = 0$ and $t(Q) = -x(Q)/y(Q)$ if $Q \neq O$ is a group isomorphism (see *e.g.* the proof of Theorem 14.1.2 of [Hus04]). It follows, by [Sil94, Proposition IV.3.2(a)], that we have for every $m \geq 1$ group isomorphisms

$$E_\mathfrak{p}^{(m)}(K_\mathfrak{p})/E_\mathfrak{p}^{(m+1)}(K_\mathfrak{p}) \simeq \widehat{\mathfrak{M}_\mathfrak{p}^m}/\widehat{\mathfrak{M}_\mathfrak{p}^{m+1}} \simeq \mathfrak{M}_\mathfrak{p}^m/\mathfrak{M}_\mathfrak{p}^{m+1} \simeq k(\mathfrak{p}).$$

Since the characteristic of the field $k(\mathfrak{p})$ is equal to p, we thus get that the exponent of the group $E_{\mathfrak{p}}^{(m)}(K_{\mathfrak{p}})/E_{\mathfrak{p}}^{(m+1)}(K_{\mathfrak{p}})$ is equal to p for all $m \geq 1$. Hence we deduce, using (13) and (14), that the exponent of the group $E_{\mathfrak{p}}(K_{\mathfrak{p}})/E_{\mathfrak{p}}^{(n)}(K_{\mathfrak{p}})$ is at most

$$\frac{5}{2}\max\{4, \mathrm{ord}_{\mathfrak{p}}(\Delta_{\mathfrak{p}})\}p^{f_{\mathfrak{p}}+n-1}.$$

Let $\Delta = -16(4A^3 + 27B^2)$ be the discriminant of the equation (2). Write now $\Delta = u^{12}\Delta_{\mathfrak{p}}$. We have

$$n - 1 = [e_{\mathfrak{p}}\lambda_p] + (\mathrm{ord}_{\mathfrak{p}}(\Delta) - \mathrm{ord}_{\mathfrak{p}}(\Delta_{\mathfrak{p}}))/12 \leq [e_{\mathfrak{p}}\lambda_p] + \mathrm{ord}_{\mathfrak{p}}(\Delta)/12,$$

hence

$$\nu_{\mathfrak{p}} \leq \frac{5}{2}\max\{4, \mathrm{ord}_{\mathfrak{p}}(\Delta_{\mathfrak{p}})\}p^{f_{\mathfrak{p}}+[e_{\mathfrak{p}}\lambda_p]+\mathrm{ord}_{\mathfrak{p}}(\Delta)/12}.$$

Noticing now that $\mathrm{ord}_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) \leq \mathrm{ord}_{\mathfrak{p}}(\Delta) \leq c_1 e_{\mathfrak{p}}$ (with $c_1 = \max\limits_{v \in M^0_{\mathbf{Q}(A,B)}} \{\mathrm{ord}_v(\Delta)\}$) and since $\lambda_p \leq 1/2$, we find

$$\nu_{\mathfrak{p}} \leq c_2 e_{\mathfrak{p}} p^{f_{\mathfrak{p}}+e_{\mathfrak{p}}/2+c_1 e_{\mathfrak{p}}/12} \leq c_2 d p^{c_3 d}.$$

□

We will also need the following lemma (where we set $x(O) = \infty$):

Lemma 4.5 *Let Q be a point of $E(K_{\mathfrak{p}})$ such that $|x(Q)|_{\mathfrak{p}} > 1$. Then, for any positive integer m, we have $|x(mQ)|_{\mathfrak{p}} \geq |x(Q)|_{\mathfrak{p}}$.*

Proof. Let

$$E(K_{\mathfrak{p}}) \supset E^{(0)}(K_{\mathfrak{p}}) \supset \cdots \supset E^{(n)}(K_{\mathfrak{p}}) \supset \cdots$$

denote the canonical $\mathfrak{p}$-adic filtration of E (see for instance [Hus04], Section 14.1). We recall that for $n \geq 1$ we have

$$E^{(n)}(K_{\mathfrak{p}}) = \{Q \in E(K_{\mathfrak{p}}); \mathrm{ord}_{\mathfrak{p}}(x(Q)) \leq -2n\}. \tag{15}$$

Let $Q \neq O$ be a point of $E(K_{\mathfrak{p}})$ as in the lemma. We know that $\mathrm{ord}_{\mathfrak{p}}(x(Q))$ is even and thus Q belongs to $E^{(n)}(K_{\mathfrak{p}})$ with $n := -\mathrm{ord}_{\mathfrak{p}}(x(Q))/2 \geq 1$. Since mQ also belongs to $E^{(n)}(K_{\mathfrak{p}})$ ($E^{(n)}(K_{\mathfrak{p}})$ is a group), it follows at once from (15) that $\mathrm{ord}_{\mathfrak{p}}(x(mQ)) \leq -2n = \mathrm{ord}_{\mathfrak{p}}(x(Q))$. □

The following Theorem was kindly communicated to us by N. Hirata (see [Hir12]) :

Theorem 4.6 (N. Hirata) *Let $\beta_1, \ldots, \beta_n$ be elements of K, and let $\gamma_1, \ldots, \gamma_n$ be n elements of $E(K) \cap \mathcal{U}_{\mathfrak{p}}$. Define $u_i = \exp_{\mathfrak{p}}^{-1}(\gamma_i)$, $1 \leq i \leq n$, and let*

$$\mathcal{L} = \beta_1 u_1 + \cdots + \beta_n u_n.$$

Define the following parameters :

$$\log B = \max\{1, h(\beta_1), \ldots, h(\beta_n)\}$$

$$h_E = \max\{1, h(1:A:B)\}$$

$$\mathcal{E} = \frac{p^{-\lambda_p}}{\max\limits_{1\le i\le n}\{|u_i|_{\mathfrak{p}}\}}$$

$$\delta = \max\{1, \frac{d}{\log \mathcal{E}}\}$$

$$g = \max_{1\le i\le n}\{1, \log\delta, h_E, \log\hat{h}(\gamma_i)\}$$

If $\mathcal{L}\neq 0$, then

$$\log|\mathcal{L}|_{\mathfrak{p}} \ge -\kappa_6^{n^2}(n+1)^{2n(n+8)}p^{8n(n+1)}\delta^{2n+2}(\log\mathcal{E})^{-2n-1}(\log B + g + \log(\delta\mathcal{E}))$$
$$\times (g+\log(\delta\mathcal{E}))^{n+1}\prod_{i=1}^{n}(h_E + \max\{1, \hat{h}(\gamma_i)\}), \quad (16)$$

where $\kappa_6 > 0$ is an absolute constant.

Corollary 4.7 *Let $m_1,\dots,m_{r+1}$ be rational integers, and let $\gamma_1,\dots,\gamma_{r+1}$ be $r+1$ elements of $E(K)\cap\mathcal{U}_{\mathfrak{p}}$. Define $u_i = \exp_{\mathfrak{p}}^{-1}(\gamma_i)$, $1\le i\le r+1$, and put*

$$\mathcal{L} = m_1u_1 + \cdots + m_{r+1}u_{r+1}.$$

Set further $M = \max\{|m_1|,\dots,|m_{r+1}|\}$ and $\log W = \max\{\hat{h}(\gamma_i), 1\le i\le r+1\}$. If $\mathcal{L}\neq 0$, then

$$\log|\mathcal{L}|_{\mathfrak{p}} \ge -\kappa_7^{r^2}r^{2r^2}p^{8r^2+28r+23}(\log p)^{-3r-4}\,d^{6r+11}\,(\log^+ d)^{r+3}$$
$$\times (\log^+ M)\,(\log^+\log W)^{r+3}\prod_{i=1}^{r+1}\max\{1, \hat{h}(\gamma_i)\}. \quad (17)$$

Proof. In the following proof, we use the notation of Theorem 4.6. Let us begin by bounding from below the parameter $\mathcal{E}$. Let n_i be the integer such that $|u_i|_{\mathfrak{p}} = p^{-n_i/e_{\mathfrak{p}}}$. Since $u_i\in\mathcal{C}_{\mathfrak{p}}$ we have $|u_i|_{\mathfrak{p}} < p^{-\lambda_{\mathfrak{p}}}$, hence $n_i/e_{\mathfrak{p}} - \lambda_{\mathfrak{p}} > 0$. If $p\neq 2$ (hence $\lambda_{\mathfrak{p}} = 1/(p-1)$), we have

$$\frac{n_i}{e_{\mathfrak{p}}} - \lambda_{\mathfrak{p}} \ge \frac{1}{(p-1)e_{\mathfrak{p}}} \ge \frac{1}{pe_{\mathfrak{p}}},$$

and if $p=2$ one easily checks that the same bound holds. It follows from this and the definition of $\mathcal{E}$ that we have

$$\log\mathcal{E} \ge \frac{\log p}{pe_{\mathfrak{p}}} \ge \frac{\log p}{pd}. \quad (18)$$

Suppose first that $d\ge\log\mathcal{E}$. Then $\delta = d/\log\mathcal{E}$, and a rough estimate gives (noticing that $\log(\delta\mathcal{E})\ge 1$ and since h_E is a constant)

$$g + \log(\delta\mathcal{E}) \ll (\log^+\log W)\,\log(\delta\mathcal{E}). \quad (19)$$

Now, using (18) we get :

$$\begin{aligned}\log(\delta\mathcal{E}) &= \log d + \log\mathcal{E} - \log\log\mathcal{E}\\ &\leq 2\log d + \log p - \log\log p + \log\mathcal{E}\\ &\ll (\log p)\ (\log^+ d)\ (\log^+\mathcal{E}).\end{aligned}$$

Replacing this estimate in (19), we obtain :

$$g + \log(\delta\mathcal{E}) \ll (\log p)\,(\log^+ d)\,(\log^+\log W)\,(\log^+\mathcal{E}).$$

Using now Hirata's bound (16), we find :

$$\begin{aligned}\log|\mathcal{L}|_{\mathfrak{p}} \geq -c_1^{r^2} r^{2r^2} p^{8(r+1)(r+2)}\,(\log p)^{r+3}\,d^{2r+4}\,(\log^+ d)^{r+3}\,(\log^+ M)\\ \times(\log^+\log W)^{r+3}\,(\log^+\mathcal{E})^{r+3}\,(\log\mathcal{E})^{-4r-7}\prod_{i=1}^{r+1}\max\{1,\hat{h}(\gamma_i)\}.\end{aligned}$$

Writing finally

$$(\log^+\mathcal{E})^{r+3}\,(\log\mathcal{E})^{-4r-7} = \max\{1,(\log\mathcal{E})^{-1}\}^{r+3}\,(\log\mathcal{E})^{-3r-4}$$

and using the lower bound (18) to estimate from above this latter quantity, we obtain (17) as required.

Suppose now that $d < \log\mathcal{E}$. Then $\delta = 1$ and we get in this case

$$g + \log(\delta\mathcal{E}) \ll (\log^+\log W)\,(\log^+\mathcal{E}).$$

Using (16) and (18) as before, we find now

$$\begin{aligned}\log|\mathcal{L}|_{\mathfrak{p}} \geq -c_2^{r^2} r^{2r^2}\, p^{8r^2+26r+19}(\log p)^{-2r-3}\,d^{2r+3}\,(\log^+ M)\\ \times(\log^+\log W)^{r+3}\prod_{i=1}^{r+1}\max\{1,\hat{h}(\gamma_i)\},\end{aligned}$$

which again implies the bound (17). □

Proof of Proposition 4.3. Let Q, Q_{r+1}, $m_1,\ldots,m_r$ and M be as in the Proposition. We note that since Q is a non-torsion point we have $M \geq 1$. Denote by $\nu_{\mathfrak{p}}$ the exponent of the group $E(K_{\mathfrak{p}})/\mathcal{U}_{\mathfrak{p}}$. Then $\nu_{\mathfrak{p}}Q, \nu_{\mathfrak{p}}Q_1,\ldots,\nu_{\mathfrak{p}}Q_{r+1}$ belong to $\mathcal{U}_{\mathfrak{p}}$, and the following linear form in $\mathfrak{p}$-adic elliptic logarithms is well-defined (and non zero since $\nu_{\mathfrak{p}}Q \neq O$):

$$\mathcal{L} := \exp_{\mathfrak{p}}^{-1}(\nu_{\mathfrak{p}}Q) = m_1\exp_{\mathfrak{p}}^{-1}(\nu_{\mathfrak{p}}Q_1) + \cdots + m_r\exp_{\mathfrak{p}}^{-1}(\nu_{\mathfrak{p}}Q_r) + \exp_{\mathfrak{p}}^{-1}(\nu_{\mathfrak{p}}Q_{r+1}).$$

Since $\varphi : \mathcal{C}_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ is an isometry, the formula (10) gives

$$|\mathcal{L}|_{\mathfrak{p}}^{-2} = |\varphi(\mathcal{L})|_{\mathfrak{p}}^{-2} = |x(\exp_{\mathfrak{p}}(\mathcal{L}))|_{\mathfrak{p}} = |x(\nu_{\mathfrak{p}}Q)|_{\mathfrak{p}}. \tag{20}$$

Observe that $|x(Q)|_{\mathfrak{p}} \leq |x(\nu_{\mathfrak{p}}Q)|_{\mathfrak{p}}$. Indeed, this is clearly true if $|x(Q)|_{\mathfrak{p}} \leq 1$ since $|x(\nu_{\mathfrak{p}}Q)|_{\mathfrak{p}} > 1$ by (12), and this is also true if $|x(Q)|_{\mathfrak{p}} > 1$ by Lemma 4.5. This remark together with (20) yields $\log |x(Q)|_{\mathfrak{p}} \leq -2 \log |\mathcal{L}|_{\mathfrak{p}}$. Applying Corollary 4.7, we get an upper bound for $\log |x(Q)|_{\mathfrak{p}}$ involving $\hat{h}(\nu_{\mathfrak{p}}Q_i)$ $(1 \leq i \leq r+1)$. Noticing that $\hat{h}(\nu_{\mathfrak{p}}Q_i) = \nu_{\mathfrak{p}}^2 \hat{h}(Q_i)$ and that $\hat{h}(Q_{r+1}) = 0$, we get

$$\log |x(Q)|_{\mathfrak{p}} \leq 2\kappa_7^{r^2} r^{2r^2} p^{8r^2+28r+23} \nu_{\mathfrak{p}}^{2r} (\log p)^{-3r-4} d^{6r+11} (\log^+ d)^{r+3} \\ \times (\log^+ M)\,(2\log \nu_{\mathfrak{p}} + \log^+ \log V)^{r+3} \prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\}.$$

But by Lemma 4.4, we have

$$\nu_{\mathfrak{p}} \leq p^{\kappa_5 d} \quad \text{hence} \quad \log \nu_{\mathfrak{p}} \ll d \log p.$$

Proposition 4.3 follows from these estimates. □

4.3 Proof of Theorem 3.1

We prove here Theorem 3.1. According to the notation of Section 2, we write $\mathcal{H} = (< Q_i, Q_j >)_{1 \leq i,j \leq r}$ for the matrix of the Néron-Tate pairing with respect to the chosen basis $(Q_1, \ldots, Q_r)$.

Lemma 4.8 *Suppose that $r \geq 1$. Let us denote by $\lambda_{\min}$ the smallest eigenvalue of the matrix $\mathcal{H}$, and by $\lambda_{\max}$ its largest eigenvalue. Let Q be a point of $E(K)$ of the form $Q = m_1Q_1 + \cdots + m_rQ_r + Q_{r+1}$, where $m_1, \ldots, m_r \in \mathbf{Z}$ and Q_{r+1} is a torsion point of $E(K)$. Define further $M = \max\{|m_1|, \ldots, |m_r|\}$. Then we have*

$$\lambda_{\min} M^2 \leq \hat{h}(Q) \leq r\lambda_{\max} M^2.$$

Proof. It follows for example from [ST94, § 3, inequality 1] and from its proof. □

Lemma 4.9 *For all Q in $E(K)$ we have*

$$\left| \hat{h}(Q) - \frac{1}{2} h_x(Q) \right| \leq \kappa_8.$$

Proof. See [Sil90, Theorem 1.1]. One can take for instance $\kappa_8 = h(\Delta)/12 + h(j(E))/8 + 1.07$, where $\Delta = -16(4A^3 + 27B^2)$ is the discriminant of the equation (2) and $j(E) = -1728(4A)^3/\Delta$ is the j-invariant of E. □

Proof of Theorem 3.1. Let Q be an S-integral point of $E(K)$. If $\hat{h}(Q) = 0$ then the bound (3) of Theorem 3.1 is clearly true, since then $h_x(Q) \leq 2\kappa_8$ by Lemma 4.9. So we will assume in the following that $\hat{h}(Q) > 0$. Thus Q is non-torsion and we have $r \geq 1$. Write $Q = m_1Q_1 + \cdots + m_rQ_r + Q_{r+1}$, where $m_1, \ldots, m_r$ are integers and Q_{r+1} is a torsion point of $E(K)$. Define $M := \max\{|m_1|, \ldots, |m_r|\}$. Applying Proposition 4.3 to all ultrametric

places $\mathfrak{p} \in S$ and Proposition 4.1 to all archimedean places σ, and adding all the inequalities obtained, we get (recall that Q is S-integral, so the places $v \notin S \cup M_K^\infty$ do not contribute to the height)

$$\begin{aligned} h_x(Q) &= \frac{1}{[K:\mathbf{Q}]} \sum_{v \in S} [K_v : \mathbf{Q}_v] \log \max\{1, |x(Q)|_v\} \\ &\leq c_1^{r^2}\, C(E,K)\, (\log^+ M)(\log^+ \log M) \times \frac{1}{[K:\mathbf{Q}]} \big(\sum_{v \in S} [K_v : \mathbf{Q}_v] p^{8r^2 + \kappa_4 dr} \big), \end{aligned}$$

where

$$C(E,K) = r^{2r^2} d^{9r+14} (\log^+ d)^{r+5} (\log^+ \log V)^{r+5} \prod_{i=1}^{r} \max\{1, \hat{h}(Q_i)\}. \tag{21}$$

Now, introducing the set $P(S) := \{p \text{ prime} \mid \exists v \in S, v|p\}$, we have :

$$\begin{aligned} \frac{1}{[K:\mathbf{Q}]} \big(\sum_{v \in S} [K_v : \mathbf{Q}_v] p^{8r^2 + \kappa_4 dr} \big) &\leq \frac{1}{[K:\mathbf{Q}]} \sum_{p \in P(S)} \big(\sum_{v|p} [K_v : \mathbf{Q}_v] \big) p^{8r^2 + \kappa_4 dr} \\ &= \sum_{p \in P(S)} p^{8r^2 + \kappa_4 dr} \leq \prod_{p \in P(S)} p^{8r^2 + \kappa_4 dr} \\ &= \exp\{(8r^2 + \kappa_4 dr) \sum_{p \in P(S)} \log p\} \leq e^{(8r^2 + \kappa_4 dr)\Sigma_S}. \end{aligned}$$

Hence we deduce

$$h_x(Q) \leq c_1^{r^2}\, C(E,K)\, (\log^+ M)\, (\log^+ \log M)\, e^{(8r^2 + \kappa_4 dr)\Sigma_S}. \tag{22}$$

Lemma 4.9 yields

$$\log^+ \hat{h}(Q) \ll \log^+ h_x(Q) \quad \text{and} \quad \log^+ \log \hat{h}(Q) \ll \log^+ \log h_x(Q),$$

and so, by Lemma 4.8 :

$$\log^+ M \leq \frac{1}{2} \big(\log^+ \hat{h}(Q) + \log^+ \lambda_{\min}^{-1}) \big) \ll (\log^+ h_x(Q)).(\log^+ \lambda_{\min}^{-1})$$

and

$$\log^+ \log M \ll (\log^+ \log h_x(Q)).(\log^+ \log \lambda_{\min}^{-1}).$$

Substituting these estimates in (22), we get

$$\frac{h_x(Q)}{(\log^+ h_x(Q))(\log^+ \log h_x(Q))} \leq U \tag{23}$$

with

$$U = c_2^{r^2}\, C(E,K)\, (\log^+ \lambda_{\min}^{-1})\, (\log^+ \log \lambda_{\min}^{-1})\, e^{(8r^2 + \kappa_4 dr)\Sigma_S}. \tag{24}$$

We now have

$$\lambda_{\max} \leq \operatorname{trace}(\mathcal{H}) = \sum_{i=1}^{r} \hat{h}(Q_i) \leq r \log V,$$

hence

$$\operatorname{Reg}(E/K) = \det(\mathcal{H}) \leq \lambda_{\min}\lambda_{\max}^{r-1} \leq \lambda_{\min} r^{r-1} (\log V)^{r-1},$$

from which we obtain

$$\lambda_{\min}^{-1} \leq \frac{r^{r-1}(\log V)^{r-1}}{\operatorname{Reg}(E/K)}.$$

It follows

$$\log^+ \lambda_{\min}^{-1} \ll r(\log^+ r)\,(\log^+ \log V)\,(\log^+ \operatorname{Reg}(E/K)^{-1})$$

and

$$\log^+ \log \lambda_{\min}^{-1} \ll (\log^+ r)\,(\log^+ \log^+ \log V)\,(\log^+ \log \operatorname{Reg}(E/K)^{-1}).$$

Substituting these inequalities in (24) and noticing that (23) implies

$$h_x(Q) \ll U(\log U)(\log \log U),$$

we get the upper bound (3). □

Remark : One would like to bound explicitly the height of the S-integral points of $E(K)$ in terms of more manageable objects, as the set of places S, the degree and the discriminant of the number field K. In a forthcoming paper, we show that it is possible to deduce from Theorem 3.1 a conditional bound of this kind, relying on the conjecture of B. J. Birch and H. P. F. Swinnerton-Dyer [BSD65]. We quote here the result that we obtain.

Proposition 4.10 *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 $[K : \mathbf{Q}]$ and D_K the absolute value of the discriminant of K.*

Suppose that the L-series of E satisfies a Hasse-Weil functional equation and that the Birch and Swinnerton-Dyer Conjecture holds for E/K.

Then, there exist positive numbers κ_{10} and κ_{11} (depending on E/K_0 only) such that, for every point Q in $E(O_{K,S})$, we have

$$h_x(Q) \leq \exp\{\kappa_{10}^d + \kappa_{11}\, d^6 (\log^+ D_K)^2 \,\big(\Sigma_S + \log(d \log^+ D_K)\big)\}.$$

Following [Sur07], we deduce from this bound a (weak exponential) inequality of the type of the *abc*-conjecture of D. Masser and J. Oesterlé.

References

[BC70] A. Baker and J. Coates. Integer points on curves of genus 1. *Proc. Cambridge Philos. Soc.*, 67:595–602, 1970.

[Ber78] D. Bertrand. Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe. *Compositio Math.*, 37(1):21–50, 1978.

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

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

[Gün66] U. Güntzer. Zur Funktionentheorie einer Veränderlichen über einem vollständigen nichtarchimedischen Grundkörper. *Arch. Math. (Basel)*, 17:415–431, 1966.

[HH98] L. Hajdu and T. Herendi. Explicit bounds for the solutions of elliptic equations with rational coefficients. *J. Symbolic Comput.*, 25(3):361–366, 1998.

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

[Hus04] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[Lan78] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

[Lut37] E. Lutz. Sur l'équation $y^2 = x^3 - ax - b$ dans les corps $\mathfrak{p}$-adiques. *J. Reine Angew. Math.*, 177:238–247, 1937.

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

[Sil90] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[ST94] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.

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

[Tat74] J. T. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.

[Wei36] A. Weil. Sur les fonctions elliptiques $\mathfrak{p}$-adiques. *C. R. Acad. Sci., Paris*, 203:22–24, 1936.

Vincent Bosser
Laboratoire Nicolas Oresme
Université de Caen
F-14032 Caen cedex
France

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