Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
C. R. Acad. Sci. Paris, Ser. I 337 (2003) 629–634
COMPTES RENDUS MATHEMATIQUE

Théorie des nombres

Approximation diophantienne sur les courbes elliptiques à multiplication complexe

Mohammed Ably [a], Éric Gaudron [b]

[a] *Université des sciences et technologies de Lille, UFR de mathématiques, URA CNRS 751, cité scientifique, 59655 Villeneuve d'Ascq cedex, France*

[b] *Institut Fourier, UMR 5582 du CNRS, BP 74, 38402 Saint-Martin-d'Hères cedex, France*

Reçu le 26 juin 2003 ; accepté après révision le 23 septembre 2003

Présenté par Jean-Pierre Serre

Résumé

Soit $\mathcal{E}$ une courbe elliptique C. M., définie sur $\overline{\mathbf{Q}}$. Considérons une famille de formes linéaires sur l'algèbre de Lie de $\mathcal{E}^n$, à coefficients dans le corps de multiplication complexe de $\mathcal{E}$. Dans ce cadre, nous présentons une mesure d'indépendance linéaire de logarithmes, analogue aux estimations connues actuellement pour les tores (commutatifs) de type $(\log b)(\log a)^n$. Ainsi, à l'instar des récentes avancées dans ce domaine (travaux d'Ably, David, Hirata-Kohno), cette mesure est optimale en la hauteur des formes linéaires considérées ($\log b$) et, en outre, elle est plus précise en la hauteur des points de la courbe elliptique ($\log a$) avec la suppression d'un terme en $\log\log a$. ***Pour citer cet article : M. Ably, É. Gaudron, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Abstract

Diophantine approximation on elliptic curves with complex multiplication. Let $\mathcal{E}$ be an elliptic curve with complex multiplication, defined over $\overline{\mathbf{Q}}$. We consider linear forms on $\mathrm{Lie}(\mathcal{E}^n)$ with coefficients in the CM field of $\mathcal{E}$. Within this framework, we present a new measure of linear independence for elliptic logarithms in $(\log b)(\log a)^n$. Like recent advances in this domain (works by Ably, David, Hirata-Kohno), our result is best possible in terms of the height of the linear forms ($\log b$) while providing a better estimate in the height of algebraic points considered ($\log a$), removing a term in $\log\log a$. ***To cite this article: M. Ably, É. Gaudron, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Abridged English version

Let n be a positive integer and $\mathbf{k}$ be a number field of absolute degree D, assumed to be embedded into $\mathbf{C}$. Let $\mathcal{E}$ be an elliptic curve defined over $\mathbf{k}$ and let

$$y^2 + \alpha_1 xy + \alpha_3 = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6 \tag{1}$$

be a Weierstrass equation for $\mathcal{E}/\mathbf{k}$ with coefficients in the ring of integers of $\mathbf{k}$. This yields a projective embedding $\mathcal{E} \hookrightarrow \mathbf{P}^2_{\mathbf{k}}$ as well as a representation of the exponential map $\exp_{\mathcal{E}}$ of $\mathcal{E}(\mathbf{C})$:

Adresses e-mail : ably@agat.univ-lille1.fr (M. Ably), Eric.Gaudron@ujf-grenoble.fr (É. Gaudron).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2003.09.018

$$\exp_{\mathcal{E}} : z \in \mathbf{C} \mapsto \big(x(z) : y(z) : 1\big),$$

where we identified the tangent space at the origin $t_{\mathcal{E}}(\mathbf{C})$ with $\mathbf{C}$ in a way compatible with its $\mathbf{k}$-structure. Let $u_1, \ldots, u_n$ be complex numbers such that $p_i := \exp_{\mathcal{E}}(u_i) \in \mathbf{P}^2(\mathbf{k})$ (if u_i is a period of $\mathcal{E}(\mathbf{C})$, we have $p_i = (0 : 1 : 0)$). Besides, let us consider V a proper subspace of $t_{\mathcal{E}^n} \simeq \mathbf{k}^n$ defined by independent linear equations

$$b_{i,1}z_1 + \cdots + b_{i,n}z_n = 0, \quad i = 1, \ldots, t,$$

where $b_{i,j}$ is in the field $\mathrm{End}(\mathcal{E}) \otimes_{\mathbf{Z}} \mathbf{Q}$ for $1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant n$. We assume $\mathrm{End}(\mathcal{E}) \otimes_{\mathbf{Z}} \mathbf{Q} \subseteq \mathbf{k}$.

In this Note, we present a measure of simultaneous approximation for elliptic logarithms

$$\Lambda_i := b_{i,1}u_1 + \cdots + b_{i,n}u_n,$$

i.e., a lower bound for $\max_{1\leqslant i\leqslant t}\{|\Lambda_i|\}$, when $\mathcal{E}$ has *complex multiplication*. The parameters to take into account are the following:

(i) the degree D of $\mathbf{k}$;
(ii) the (absolute logarithmic) Weil height $h(V)$ of V;
(iii) the absolute value of u_i and the Néron–Tate height $\hat{h}(p_i)$ of p_i (for all $1 \leqslant i \leqslant n$).

We consider some positive real numbers $b,\ a_1, \ldots, a_n,\ E$ such that $E \geqslant e := 2,718\ldots$ and

$$\log b \geqslant \max\big\{1,\ h(V)\big\} \quad \text{and} \quad \forall j \in \{1, \ldots, n\}, \quad \log a_j \geqslant \max\left\{\hat{h}(p_j),\ \frac{(E|u_j|)^2}{D},\ \frac{\log E}{D}\right\}. \tag{2}$$

For convenience, we shall suppose $a_1 \geqslant \cdots \geqslant a_n$ (that is not a restrictive condition).

We are now in position to state our result.

Theorem 0.1. *Let us assume that $\mathcal{E}$ has complex multiplication. There exists a constant $c > 0$, depending only on n, $\mathcal{E}$ and on its Weierstrass model* (1)*, having the following property.*

- *If, for all $i \in \{1, \ldots, t\}$, $\Lambda_i = 0$ then there exists an abelian subvariety $\mathcal{A}$ of $\mathcal{E}^n$, of dimension g, such that* (a) $(u_1, \ldots, u_n) \in t_{\mathcal{A}}(\mathbf{C})$; (b) $t_{\mathcal{A}} + V \neq t_{\mathcal{E}^n}$ *and whose geometric degree* $\deg \mathcal{A}$*, relative to the embedding $\mathcal{E}^n \hookrightarrow (\mathbf{P}^2_{\mathbf{k}})^n$, satisfies inequality* (5).
- *In the other case, when there exists $i \in \{1, \ldots, t\}$ such that $\Lambda_i \neq 0$, we have the lower bound for* $\log \max_{1\leqslant i\leqslant t}\{|\Lambda_i|\}$ *given by inequality* (6).

While being best possible in terms of the height of V, the conclusions of this theorem are also sharper in the parameters a_i's than the previous estimates [1,3,4,6] because there is no longer a supernumerary (polynomial) term in $\log^+ \log(a_1 \cdots a_n)$.

The demonstration rests on Baker's method as developped by Philippon and Waldschmidt in [9]. To achieve these estimates, three steps of the proof have been modified (see French version). As is usual nowadays in this kind of problems, we work with the algebraic group $\mathbb{G}_{\mathrm{a}} \times \mathcal{E}^n$ instead of $\mathcal{E}^n$ only. To construct the auxiliary polynomial, we use a new idea by David and Hirata-Kohno (see [4]) based on an absolute Siegel lemma (Lemma 4.7 of [5], see also §2.1 of the French version). That allows us to get rid of the height of a $\mathbf{Q}$-basis of $\mathbf{k}$ (or, equivalently, the absolute discriminant of $\mathbf{k}$) from (6). We include into this step the Lagrange polynomial on the affine part $\mathbb{G}_{\mathrm{a}}$ to slow down the growth of the auxiliary function (see [1,2] and also formula (7)). Besides, from the "rationality" assumption on V, we can give very sharp ultrametric estimates for some Taylor coefficients arising from the auxiliary polynomial. Lastly, we make use of an analytic extrapolation on points

$$(s,\ sp_1, \ldots, sp_n) \in \big(\mathbb{G}_{\mathrm{a}} \times \mathcal{E}^n\big)(\mathbf{k}) \quad \text{with } s \in \mathrm{End}(\mathcal{E}), \quad \|s\| \leqslant S.$$

The hypothesis of complex multiplication is used here and it yields a Schwarz exponent in TS^2 ($T =$ order of derivation) instead of TS (refer to [1,8] to see how this trick can be used).

1. Énoncé du résultat

Soient n un entier naturel non nul et $\mathbf{k}$ un corps de nombres, de degré $D = [\mathbf{k} : \mathbf{Q}]$ sur $\mathbf{Q}$, que l'on considère plongé dans $\mathbf{C}$ par σ_0. Soit $\mathcal{E}$ une courbe elliptique, définie sur $\mathbf{k}$, munie d'un modèle de Weierstrass

$$y^2 + \alpha_1 xy + \alpha_3 = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6, \tag{3}$$

à coefficients α_i *entiers* algébriques. Nous disposons ainsi d'un plongement projectif $\mathcal{E} \hookrightarrow \mathbf{P}^2_{\mathbf{k}}$ et d'une représentation de l'exponentielle $\exp_{\mathcal{E}}$ de $\mathcal{E}(\mathbf{C})$:

$$\exp_{\mathcal{E}} : z \in \mathbf{C} \mapsto \big(x(z) : y(z) : 1\big),$$

où nous avons identifié l'espace tangent à l'origine $t_{\mathcal{E}}(\mathbf{C})$ avec $\mathbf{C}$ d'une façon compatible avec sa $\mathbf{k}$-structure.

Soient $u_1, \ldots, u_n$ des nombres complexes tels que $p_i := \exp_{\mathcal{E}}(u_i) \in \mathbf{P}^2(\mathbf{k})$ (avec les précautions d'usage : si u_i est une période de $\mathcal{E}(\mathbf{C})$ alors $\exp_{\mathcal{E}}(u_i) = (0 : 1 : 0)$). Nous désignerons par $\hat{h}(p_i)$ la hauteur de Néron–Tate de p_i. Considérons $a_1, \ldots, a_n$, E des nombres réels tels que

$$E \geqslant e \text{ et } \forall j \in \{1, \ldots, n\}, \quad \log a_j \geqslant \max\left\{\hat{h}(p_j), \frac{(E|u_j|)^2}{D}, \frac{\log E}{D}\right\}. \tag{4}$$

Par *commodité* de présentation du théorème, nous supposerons que $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n$ (ce qui est toujours possible après permutations des indices).

Soient $1 \leqslant t \leqslant n$ un entier naturel et $(b_{i,j})_{1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant n}$ une matrice $t \times n$ à coefficients dans le corps des endomorphismes $\mathrm{End}(\mathcal{E}) \otimes \mathbf{Q}$ de $\mathcal{E}$ et de rang (*maximal*) t. Quitte à étendre $\mathbf{k}$, on peut supposer qu'il contient $\mathrm{End}(\mathcal{E}) \otimes \mathbf{Q}$. Soit V le sous-espace de $t_{\mathcal{E}^n} \simeq \mathbf{k}^n$, de codimension t, défini par les équations

$$b_{i,1} z_1 + \cdots + b_{i,n} z_n = 0, \quad i = 1, \ldots, t.$$

L'hypothèse sur les coefficients $b_{i,j}$ signifie que V est l'algèbre de Lie d'une sous-variété abélienne de $\mathcal{E}^n$, autrement dit que V est *rationnel*. Nous désignerons par $h(V)$ la hauteur (logarithmique absolue) de Weil de V et par $\log b$ un majorant de $\max\{1, h(V)\}$. Nous posons $\Lambda_i := b_{i,1} u_1 + \cdots + b_{i,n} u_n$.

Notre résultat est le suivant :

Théorème 1.1. *Supposons que la courbe elliptique $\mathcal{E}$ admette une* multiplication complexe. *Alors il existe une constante $c > 0$, dépendant seulement de n, $\mathcal{E}$ et du modèle de Weierstrass* (3) *choisi, ayant la propriété suivante.*

– *Si, pour tout $i \in \{1, \ldots, t\}$, on a $\Lambda_i = 0$ alors il existe une sous-variété abélienne $\mathcal{A}$ de $\mathcal{E}^n$, de dimension g, telle que* (a) $(u_1, \ldots, u_n) \in t_{\mathcal{A}}(\mathbf{C})$; (b) $t_{\mathcal{A}} + V \neq t_{\mathcal{E}^n}$ *et dont le degré relatif au plongement $\mathcal{E}^n \hookrightarrow (\mathbf{P}^2_{\mathbf{k}})^n$ est majoré* :

$$\deg \mathcal{A} \leqslant c\left(\frac{D}{\log E}\right)^g \left(1 + \frac{D}{\log E} \log\left(1 + \frac{D}{\log E}\right)\right) \times \prod_{j=1}^{g} \log a_j. \tag{5}$$

– *Dans le cas contraire, s'il existe $i \in \{1, \ldots, t\}$ tel que $\Lambda_i \neq 0$, on dispose de la minoration* (*de formes linéaires simultanées de logarithmes*) *suivante* :

$$\log \max_{1 \leqslant i \leqslant t} \{|\Lambda_i|\} \geqslant -c\left\{\left(\frac{D}{\log E}\right)^n \left(1 + \frac{D}{\log E} \log\left(1 + \frac{D}{\log E}\right)\right) \times \prod_{j=1}^{n} \log a_j\right\}^{1/t} \times \left\{D \log b + \log\Big(E + \max_{1 \leqslant i \leqslant n} \{|u_i|\}\Big) + \log \max_{1 \leqslant i \leqslant n} \left\{1, \frac{1}{|u_i|}\right\}\right\}. \tag{6}$$

À la manière de [6], on peut paraphraser cet énoncé en des termes plus géométriques : soient u un logarithme d'un point $\mathbf{k}$-rationnel de $\mathcal{E}^n$ (de composantes $u_1, \ldots, u_n$) et V l'algèbre de Lie d'une sous-variété abélienne de $\mathcal{E}^n$ (de codimension t). Si $u \in V(\mathbf{C})$, la conclusion est la même que le premier point du théorème (et en particulier le majorant du degré de $\mathcal{A}$ ne dépend pas de V), et le second point donne une minoration de la distance entre u et $V(\mathbf{C})$.

2. Ingrédients de la démonstration

Le schéma de la preuve du théorème s'inscrit dans le cadre de la *méthode de Baker*, telle qu'elle a été élaborée dans ce contexte par Philippon et Waldschmidt [9]. Généralement, il comporte six étapes :

(1) Un « conditionnement » des données de départ.
(2) Un choix préliminaire des paramètres pour tenir compte, dans la preuve même, du sous-groupe « obstructeur » $\mathcal{A}$ (celui de la première partie de l'énoncé), sous-groupe qui apparaît dans les inégalités du type de celle du lemme de zéros [7].
(3) La construction d'un polynôme auxiliaire P (à coefficients algébriques et de petite hauteur) dont la restriction au groupe s'annule en certains multiples de p le long du sous-espace V à certains ordres.
(4) Une majoration aux places finies d'un élément α de $\mathbf{k}$, construit comme coefficient de Taylor à partir de P composé avec l'exponentielle du groupe.
(5) Des majorations de même type, mais aux places infinies, de α avec une borne très précise à la place σ_0, obtenue à l'aide d'un « lemme de Schwarz approché ». C'est à cet endroit de la preuve que la *méthode de Baker* est particulièrement décisive.
(6) Avec les étapes précédentes, si la distance de u à V est « trop petite », on démontre que α est nul (formule du produit) puis on déduit une contradiction en utilisant à nouveau le lemme de zéros [7].

Le théorème comprend trois hypothèses – le groupe algébrique est une puissance d'une courbe elliptique, cette courbe est avec multiplication complexe et le sous-espace est rationnel – qui permettent d'apporter une réponse spécifique aux estimations des étapes (3), (4) et (5), à condition de modifier légèrement les données de départ (étape (1)) de la manière suivante.

Soit $\mathbf{G}$ le groupe algébrique $\mathbb{G}_{\mathrm{a}} \times \mathcal{E}^n$, plongé dans $\mathbf{P}^1_{\mathbf{k}} \times (\mathbf{P}^2_{\mathbf{k}})^n$. Posons $u := (1, u_1, \ldots, u_n) \in \mathbf{C}^{n+1}$ et considérons $W := t_{\mathbb{G}_{\mathrm{a}}} \oplus V$. La distance de u à W est aussi la distance de $(u_1, \ldots, u_n)$ à V et il suffit d'établir le théorème avec ces données.

2.1. Construction du polynôme auxiliaire

Cette construction consiste d'une part à choisir sur $\mathbb{G}_{\mathrm{a}}$ une famille ($\mathbf{C}$-libre) de polynômes de type Lagrange

$$\Delta_R(X)^\ell := \prod_{\substack{x \in \mathcal{O} \setminus \{0\} \\ \|x\| \leqslant R}} \left(\frac{X+x}{x}\right)^\ell, \quad R > 0,\ \ell \in \mathbf{N}, \tag{7}$$

où $\mathcal{O}$ est l'anneau des entiers de $\mathrm{End}(\mathcal{E}) \otimes \mathbf{Q}$ que l'on identifie à un réseau de $\mathbf{R}^2$ (muni de sa norme euclidienne $\|\cdot\|$) comme cela a déjà été mis en œuvre par le premier auteur [1]. Ces polynômes ont l'avantage de croître plus « lentement » que les monômes usuels tout en restant « raisonnable » du point de vue de leur croissance arithmétique ; le Théorème 2.1 de [2] précise les guillemets de cette affirmation. D'autre part, pour la construction proprement dite du polynôme auxiliaire, nous utilisons le lemme de Siegel « absolu » suivant, dû à David et Philippon.

Lemme [5]. *Soient N un entier naturel et $F \subseteq \overline{\mathbf{Q}}^{N+1}$ un sous-espace vectoriel non nul, de hauteur (logarithmique absolue) de Schmidt $h(F)$. Alors il existe un élément $y \in F \setminus \{0\}$ de hauteur $\leqslant (h(F)/\dim F) + \log \dim F$.*

Cette technique a été introduite très récemment dans ce contexte par David et Hirata [4]. Elle permet de se débarrasser de la hauteur d'une **Q**-base du corps de nombres **k**, qui apparaît par exemple dans les mesures de [6] lorsqu'on utilise le lemme de « petites valeurs », dit de Thue–Siegel. Il faut noter que l'estimation de la hauteur *finie* (i.e. la somme restreinte aux places ultramétriques) du sous-espace F que nous considérerons nécessite le lemme arithmétique du paragraphe suivant.

2.2. Amélioration arithmétique

Cette partie n'utilise que l'hypothèse de rationalité du sous-espace V (ou W), à travers l'hypothèse sur les coefficients de la matrice M ci-dessous. En notant $\overline{\mathbf{Z}}$ l'anneau des entiers algébriques et $(z_1, \ldots, z_n)$ l'idéal maximal de $\mathbf{C}[[z_1, \ldots, z_n]]$ engendré par les z_i, le lemme-clef peut s'énoncer de la manière suivante.

Lemme 2.1. *Soit $P \in \overline{\mathbf{Z}}[X_1, Y_1, \ldots, X_n, Y_n]$ et posons*

$$F(\mathbf{z}) = \frac{P(x(z_1), y(z_1), \ldots, x(z_n), y(z_n))}{y(z_1)^{D_1} \cdots y(z_n)^{D_n}},$$

où $\mathbf{z} = (z_1, \ldots, z_n)$, $(x(z), y(z))$ sont les coordonnées sur la courbe elliptique définies par (3) *et, pour tout $i \in \{1, \ldots, n\}$, D_i est le degré partiel de P relatif au couple de variables (X_i, Y_i). Soit M une matrice $n \times n$ à coefficients dans* $\mathrm{End}(\mathcal{E})$. *Supposons que $F(M\mathbf{z}) \in (z_1, \ldots, z_n)^T$ pour un certain entier $T \geqslant 0$. Alors le polynôme de Taylor d'ordre T de $F(M\mathbf{z})$ appartient à $\overline{\mathbf{Z}}[\mathbf{z}]$.*

La preuve de ce lemme repose sur le même type d'argument que [4], lié aux techniques de calculs « formels » sur le complété formel (le long de la section nulle) de la courbe elliptique $\mathcal{E}$ (voir Chapitre 4 de [10]). Elle est fondée sur le changement de variable $\mathfrak{t} = -\frac{x}{y}$, $\mathfrak{s} = -\frac{1}{y}$ et la loi d'addition formelle associée au modèle de Weierstrass de la courbe elliptique, dont les coefficients appartiennent à $\overline{\mathbf{Z}}$ (par choix des α_i).

2.3. Raffinement analytique

Dans ce paragraphe, nous n'utilisons que l'hypothèse de multiplication complexe. Elle intervient à travers le *nombre* de points de l'ensemble $\{(s, sp_1, \ldots, sp_n);\ s \in \mathrm{End}(\mathcal{E}),\ \|s\| \leqslant S\}$ avec lequel nous effectuons l'extrapolation, qui est de l'ordre[1] de S^2. Cela permet d'avoir un exposant de Schwarz de l'ordre de TS^2 (ici T est l'ordre de dérivation) dans la formule d'interpolation pour des réseaux (cf. Lemme 3.3 de [1]). Des détails supplémentaires sont fournis dans [1,8].

Remerciements

Nous remercions S. David pour ses explications concernant l'utilisation du lemme de Siegel absolu dans ce contexte des formes linéaires de logarithmes ainsi que G. Diaz et G. Rémond pour leurs remarques sur une première version de cette Note.

[1] On notera que l'ajout du facteur $\mathbb{G}_a$ se justifie ici – au moins techniquement – en éliminant la possibilité pour cet ensemble d'être « trop petit », comme cela eût été le cas par exemple si les p_i étaient nuls (i.e. égaux à $(0:1:0)$ dans $\mathbf{P}^2$) !

Références

[1] M. Ably, Formes linéaires de logarithmes de points algébriques sur une courbe elliptique de type CM, Ann. Inst. Fourier (Grenoble) 50 (2000) 1–33.
[2] M. Ably, M. M'Zari, Polynômes de Lagrange sur les entiers d'un corps quadratique imaginaire, J. Th. des Nombres de Bordeaux 10 (1998) 85–105.
[3] S. David, Minorations de formes linéaires de logarithmes elliptiques, Mém. Soc. Math. France 62 (1995).
[4] S. David, N. Hirata, Linear forms in elliptic logarithms (2003), en préparation.
[5] S. David, P. Philippon, Minorations des hauteurs normalisées des sous-variétés des tores, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) XXVIII (1999) 489–543.
[6] É. Gaudron, Mesure d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif, Thèse de Doctorat, Université Jean Monnet de Saint-Étienne, 2001.
[7] P. Philippon, Lemme de zéros dans les groupes algébriques commutatifs, Bull. Soc. Math. France 114 (1986) 355–383 ; Errata et Addenda, Bull. Soc. Math. France 115 (1987).
[8] P. Philippon, M. Waldschmidt, Formes linéaires de logarithmes simultanées sur les groupes algébriques commutatifs, Séminaire de Th. des Nombres, Paris (1986/1987) 313–347.
[9] P. Philippon, M. Waldschmidt, Formes linéaires de logarithmes sur les groupes algébriques commutatifs, Illinois J. Math. 32 (2) (1988) 281–314.
[10] J.H. Silverman, The Arithmetic of Elliptic Curves, in : Graduate Texts in Math., Vol. 106, Springer-Verlag, 1986.