MÉMOIRES DE LA S. M. F.

SINNOU DAVID

Minorations de formes linéaires de logarithmes elliptiques

Mémoires de la S. M. F. 2e série, tome 62 (1995)

<http://www.numdam.org/item?id=MSMF_1995_2_62__1_0>

Société Mathématique de France
Mémoire 62
Supplément au Bulletin de la S. M. F.
Tome 123, 1995, fascicule 3

Minorations de formes linéaires de logarithmes elliptiques

Sinnou DAVID

Résumé : nous obtenons une minoration de formes linéaires de logarithmes elliptiques de points algébriques d'un produit de courbes elliptiques définies sur $\overline{\mathbb{Q}}$. Cette minoration est totalement explicite. On donne également une version quantitative explicite du cas dégénéré.

Abstract : we get a totally explicit lower bounds for linear forms in elliptic logarithms of a product of elliptic curves defined over $\overline{\mathbb{Q}}$. An explicit quantitative version of the degenerate case is also proven.

Classification AMS : 11G, 11J, 14K.

Texte reçu le 21 juin 1993.
Université Pierre et Marie Curie,
Département de Mathématiques, «Problèmes Diophantiens»
4, Place Jussieu,
75005 Paris

Table des Matières

1 Introduction

La théorie des formes linéaires de logarithmes a connu de nombreux développements depuis les premiers travaux d'A. BAKER ([Ba1]). En sus des applications plus théoriques, le fait que les preuves soient effectives a conduit les mathématiciens à s'intéresser à des minorations explicites afin d'appliquer la théorie à la résolution de nombreuses classes d'équations diophantiennes. Ainsi, dès les premiers travaux, on trouve des minorations de formes linéaires explicites dans le cas usuel. Ces bornes ont d'ailleurs été constamment raffinées au fur et à mesure que la théorie progressait (on pourra comparer par exemple [Ba1, IV], [B-G-M-M-S] et [Ba–Wü]). Parallèlement, on s'est aperçu que rien en théorie ne singularisait le cas dit «usuel» et que la technique employée pouvait s'appliquer à n'importe quel groupe algébrique commutatif (on peut vraisemblablement attribuer cette idée à D. MASSER (*voir* [Ma]) qui a étudié le cas des courbes elliptiques à multiplication complexes; J. COATES et S. LANG (*voir* [Co–La]) ont poursuivi avec le cas des variétés abéliennes (toujours à multiplication complexes)). Bien entendu, les difficultés (essentiellement le manque de lemme de zéros performant) ont ralenti l'apparition de ces généralisations. S'il ne nous appartient pas ici de retracer l'historique de cette théorie, signalons simplement que les travaux de P. PHILIPPON et M. WALDSCHMIDT (*voir* [P–W]) raffinés par les textes de N. HIRATA (*voir* [Hi2] et [Hi1]) ont conduit à des énoncés tout à fait généraux, dont la forme est presque satisfaisante en comparaison de ce qui est connu dans le cas usuel (pour les spécialistes, rappelons que N. HIRATA est la première a donner dans ce cadre la «bonne» dépendance en «$\log(B)$», à ε-près). Toutefois, il n'existe à ce jour aucun énoncé dans la littérature fournissant une minoration de formes linéaires de logarithmes *totalement explicite* en dehors du cas usuel. Sans doute les auteurs qui se sont interessés successivement à ce problème avaient en tête des applications de nature théorique. Il semble cependant qu'au moins dans le cas de la recherche des points entiers de certaines classes d'équations de MORDELL (et, plus généralement de genre 1) la connaissance d'une minoration explicite de formes linéaires de logarithmes elliptiques soit utile (*voir* en particulier les travaux de R. STOELKER et N. TZANAKIS [St–Tz], de J. GEBEL, A. PETHÖ et H. ZIMMER ([G–P–Z]) ou le travail de N. HIRATA [Hi3]). C'est en tout cas pour répondre à cette demande précise que nous avons entrepris ce travail. Nous nous sommes également volontairement limités au cas elliptique, où des applications précises sont en vue et où les difficultés techniques sont moindres.

Le résultat que nous obtenons est ainsi une version totalement explicite du travail de N. HIRATA (cas elliptique, *voir* [Hi1]). Nous précisons en sus ce qui se passe lorsque la forme linéaire est nulle. Ceci nous permet d'obtenir en corollaire une version affaiblie mais explicite du théorème d'isogénie de D. MASSER et G. WÜSTHOLZ (*voir* [Ma–Wu1]) pour les courbes elliptiques. Il s'agit donc avant tout d'un travail de mise au point et, en ce sens, on ne trouvera rien dans ce texte de véritablement original, la majeure partie des lemmes présentés se trouvant déjà dans la littérature (bien entendu, la source principale est le texte de N. HIRATA). Toutefois, il est très rare de les trouver sous une forme explicite, comme nous en avons besoin ici. Nous avons donc été contraints de les prouver à nouveau, et en ce sens le travail que nous présentons est raisonnablement «self contained», à quelques exceptions toutefois, notamment dans la preuve du corollaire (paragraphe 10) où nous avons coupé au plus court et, ce qui est plus regrettable, dans la preuve du lemme 6.1 : le lecteur se retrouvera là face à une cascade de renvois bibliographiques, des textes de N. HIRATA ([Hi2] et [Hi1]) vers le travail de P. PHILIPPON et M. WALDSCHMIDT ([P–W]) qui renvoient aux notations et arguments de [Ph1]...

Par commodité pour le lecteur habitué aux textes de P. PHILIPPON–M. WALDSCHMIDT et de N. HIRATA, nous suivons de très près leur plan : on trouvera au paragraphe suivant l'énoncé du résultat principal, au paragraphe 3 les lemmes de croissance analytique des fonctions de WEIERSTRASS, au paragraphe 4 les réductions propres à la technique de N. HIRATA, au paragraphe 5 le choix d'un sous–groupe privilégié, au paragraphe 6, les préparatifs à la construction de la fonction auxiliaire, au paragraphe 7 la preuve de transcendance proprement dite, au paragraphe 8 les lemmes donnant un contrôle effectif des formules de translation et de dérivation, au paragraphe 9 la conclusion de la preuve du théorème 2.1, et enfin, au paragraphe 10 la preuve du corollaire.

Nous nous sommes efforcés de donner des énoncés relativement précis, même là où ce n'était pas vraiment nécessaire pour notre résultat, pour les lemmes qui nous semblaient pouvoir être utiles à d'autres auteurs (en particulier ceux des paragraphes 3 et 8). Cela donne une explication partielle à la présence en de nombreux points de calculs intermédiaires présentant une précision «irrelevante». Une autre explication est également que je mesurais parfois mal l'importance finale de mes calculs intermédiaires avant d'avoir achevé le travail et que je n'ai pas forcément pensé à les simplifier partout... Je prie le lecteur de m'excuser pour ces lourdeurs. Un avertissement enfin. Un certain nombre d'inégalités ne sont démontrées que pour les grandes valeurs d'un paramètre entier. Les vérifications restantes, en nombre *fini* ont été effectuées à l'aide de «Mathematica» de WOLFRAM Research.

2 Notations et résultats

Soit K un corps de nombres de degré D sur $\mathbb{Q}$, plongé dans le corps des nombres complexes $\mathbb{C}$. On notera $\overline{\mathbb{Q}}$ la clôture algébrique de K dans $\mathbb{C}$. Soient également k un entier ≥ 0, et $\mathcal{E}_1, \ldots, \mathcal{E}_k$, k courbes elliptiques définies sur K, que l'on supposera munies d'un modèle de WEIERSTRASS :

$$y^2 = 4x^3 - g_{2,i}x - g_{3,i}, \quad g_{2,i}, g_{3,i} \in K, \quad 1 \leq i \leq k.$$

On notera, $\wp_i, 1 \leq i \leq k$ (resp. σ_i), les fonctions de WEIERSTRASS associées, et $\Lambda_i = \omega_{1,i}\mathbb{Z} + \omega_{2,i}\mathbb{Z}$ le réseau des périodes de $\wp_i$. On désigne par h la hauteur de WEIL logarithmique et absolue sur $\mathbb{P}^N(\overline{\mathbb{Q}})$. Rappelons brièvement sa définition : soit P un point de $\mathbb{P}^N(\overline{\mathbb{Q}})$. Soit L un corps de nombres contenant toutes les coordonnées $X_0, \ldots, X_N$ de P , de degré d sur $\mathbb{Q}$. On pose alors :

$$h(P) = \frac{1}{d}\sum_v n_v \log(\max\{|x_0|_v, \ldots, |x_N|_v\}),$$

où v décrit l'ensemble des places de L et où les valeurs absolues prolongent les valeurs absolues usuelles sur $\mathbb{Q}$, et sont normalisées de telle sorte que la formule du produit soit satisfaite :

$$\forall x, x \in L, x \neq 0, \quad \sum_v n_v \log|x|_v = 0; \quad \sum_{v|\infty} n_v = d.$$

On notera $j_{\mathcal{E}_i}$ l'invariant modulaire de la courbe $\mathcal{E}_i$, l'on posera $h = \max\{1, h(1, g_{2,i}, g_{3,i}), h(j_{\mathcal{E}_i}), 1 \leq i \leq k\}$ et on notera $\tau_i = \frac{\omega_{2,i}}{\omega_{1,i}}$. Il n'y a pas de restriction à supposer que τ_i est un élément du demi-plan de POINCARÉ $\mathfrak{H}$ (*ie.* que $\Im m\ \tau_i > 0$). Nous supposerons plus précisément que $\tau_i \in \mathfrak{F}$, où $\mathfrak{F}$ désigne le domaine fondamental usuel de $\mathfrak{H}$ pour l'action de $\mathrm{Sl}_2(\mathbb{Z})$. Cela suppose simplement que l'on choisisse une base adéquate de Λ_i, mais ne change pas les invariants $g_{2,i}$, $g_{3,i}$ ou à fortiori $j_{\mathcal{E}_i}$. Si u_i est un nombre complexe tel que $\gamma_i = (\sigma_i^3(u_i), \sigma_i^3(u_i)\wp_i(u_i), \sigma_i^3(u_i)\wp_i'(u_i)) \in \mathcal{E}_i(\overline{\mathbb{Q}})$, nous noterons $\hat{h}(\gamma_i)$ la