Astérisque

DANIEL BERTRAND

Sur les dénominateurs des points rationnels des courbes elliptiques

Astérisque, tome 41-42 (1977), p. 173-178

<http://www.numdam.org/item?id=AST_1977__41-42__173_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.173-178

SUR LES DÉNOMINATEURS DES POINTS RATIONNELS DES COURBES ELLIPTIQUES

Daniel BERTRAND

§ 1. INTRODUCTION. RAPPEL DES RÉSULTATS ARCHIMEDIENS.

Soit E une courbe elliptique définie sur un corps de nombres K par l'équation : $y^2 = x^3 + Ax + B$. Pour tout plongement $K \hookrightarrow L$, et tout sous-groupe E' de E, on note E'(L) l'ensemble des points L-rationnels de E'.

On appelle hauteur d'un nombre algébrique α, et on note $H(\alpha)$, le maximum des valeurs absolues archimédiennes des coefficients de son polynôme minimal sur $\mathbb{Z}$; on note $den(\alpha)$ son dénominateur. Par ailleurs, si x(Q) désigne l'abscisse d'un élément Q de E(K), on pose :

$$H(Q) = H(x(Q)) \; ; \; D(Q) = den(x(Q)) \quad .$$

Rappelons qu'il n'y a qu'un nombre fini de points Q de E(K) tels que H(Q) soit borné.

Soit $\mathcal{M}_\infty$ l'ensemble des valeurs des intégrales elliptiques $\int_0^Q dx/y$ prises entre l'origine de E et les points Q de $E(\mathbb{C})$ à coordonnées algébriques.

D'après un théorème classique de Schneider, les éléments non nuls de $\mathcal{M}_\infty$ sont transcendants. Dans le cas (M.C.) où E admet une multiplication complexe, Masser [4] a obtenu des minorations explicites -améliorées par Coates et Lang [2]- des combinaisons linéaires d'éléments de $\mathcal{M}_\infty$ à coefficients algébriques. Ces minorations fournissent une nouvelle preuve du théorème de finitude de Siegel sur E. Ainsi, dans le cas où E est définie sur $\mathbb{Q}$, on peut énoncer :

Proposition 1 (M.C.) : (Voir [4], thm. A4) : il existe un nombre réel $c_1 > 0$ ne dépendant que de A et B tel que, pour tout élément Q de $E(\mathbb{Q})$, on ait :

$$\mathrm{Log}(D(Q)) > c_1 \, \mathrm{Log}(H(Q)) \quad .$$

Nous présentons ici l'analogue ultramétrique de ces résultats. Soient p un nombre premier, $\mathbb{C}_p$ le complété de la clôture algébrique du corps $\mathbb{Q}_p$, et $|\ |_p$ la valeur absolue normalisée de $\mathbb{C}_p$. Alors il existe une isométrie t (voir [3], § 2), analytique sur un sous-groupe non trivial $\mathcal{C}_p$ de $\mathbb{C}_p$, telle que l'application e_p :

$$z \longmapsto \{\wp(z) = 1/t^2(z) \ ; \ \wp'(z)/2 = -t'(z)/t^3(z); 1\}$$

représente l'application exponentielle p-adique au voisinage de l'origine de $E(\mathbb{C}_p)$. Nous notons $\mathcal{M}_p$ l'ensemble des éléments de $\mathcal{C}_p$ où t prend des valeurs algébriques.

§ 2. VERSION p-ADIQUE DU THÉORÈME DE SCHNEIDER.

Théorème 1 ([1], thm. 1) : *les éléments non nuls de $\mathcal{M}_p$ sont transcendants.*

Démonstration (nous indiquons comment le lemme 1 de [1] permet de prouver le théorème 1). Soit k un entier arbitrairement grand. La notation $\ll$ se rapporte à la variable k tendant vers $+\infty$.

Supposons qu'il existe un élément $u \neq 0$ de $\mathcal{M}_p$, algébrique. Le "lemme de Siegel" permet alors de construire une fonction non identiquement nulle :

$$\Phi(z) = \sum_{0 \leq \lambda_1, \lambda_2 \leq r} p_{\lambda_1,\lambda_2} z^{\lambda_1} \wp(z)^{\lambda_2}$$

avec $r = [k^{3/4}]$, $p_{\lambda_1,\lambda_2} \in \mathbb{Z}$, $H(p_{\lambda_1,\lambda_2}) \ll e^r$, admettant le point u pour zéro d'ordre k.

Pour tout entier $n > 0$, soit k_n l'ordre de la fonction Φ au point nu (de sorte que $k_1 \geq k$ et $k_n = 0$ pour n suffisamment grand). Le lemme 1 de [1] entraîne :

$$\text{Log } H(\Phi^{(k_n)}(nu)) \ll rn^2 + k_n(\text{Log } k_n + \text{Log } k + \text{Log } n) \quad ,$$

et le lemme de Schwarz appliqué à la fonction $z^{2r}\Phi$, joint aux inégalités de Cauchy au point nu, fournit uniformément en n l'inégalité :

$$(I_n) \qquad \sum_{i=1}^{+\infty} k_i \ll rn^2 + k_n(\text{Log } k_n + \text{Log } k + \text{Log } n) \quad .$$

Soit N le plus petit entier tel que $k_N < k_1^{11/12}$. On tire de (I_N) :

$$k_1 + (N-2)k_1^{11/12} \ll k^{3/4} N^2 + k_1^{11/12}(\text{Log } k_1 + \text{Log } N) \quad ,$$

d'où : $N \gg k_1^{1/6}$. En conséquence :

$$\sum_{i=1}^{+\infty} k_i > (N-1)k_1^{11/12} \gg k_1^{13/12} .$$

Mais l'inégalité (I_1) entraîne alors :

$$k_1^{13/12} \ll k_1 \operatorname{Log} k_1 ,$$

ce qui fournit la contradiction recherchée.

§ 3. VERSION p-ADIQUE DES RÉSULTATS DE MASSER, COATES ET LANG.

Nous supposons désormais que E admet une multiplication complexe. On considère n éléments $u_1,\dots,u_n$ de $\mathfrak{m}_p$ tels que $e_p(u_1),\dots,e_p(u_n)$ soient des points de E(K) linéairement indépendants sur l'anneau des endomorphismes de E, et on note $U = \sup_{i=1,\dots,n} H(e_p(u_i))$.

Proposition 2 (M.C.) (Voir [1], § 3) : soient d et h des nombres entiers > 0. Il existe un nombre réel $c_2 = c_2(n,d,A,B,K) > 0$ effectivement calculable tel que l'inégalité

$$|\alpha_1 u_1 + \dots + \alpha_n u_n|_p > \exp(-c_2(\operatorname{Log} h)^{16n} (p \operatorname{Log} U)^{32n^2})$$

soit satisfaite par tout n-uple $\{\alpha_1,\dots,\alpha_n\}$ de nombres algébriques de degré $\leq d$ et de hauteur $\leq h$.

Si S désigne un ensemble fini de places de K contenant les places archimédiennes, on peut déduire des propositions 1 et 2 une démonstration du théorème de finitude de Siegel-Mahler sur les points de E(K) à coordon-

nées entières hors de S. Ainsi, dans le cas où A et B sont des entiers rationnels, on a, en notant P(x) le plus grand facteur premier de l'entier x :

Théorème 2 (M.C.) ([1], thm. 5) : il existe un nombre réel $c_3 > 0$ ne dépendans que de A et B tel que, pour tout élément Q de $E(\mathbb{Q})$, on ait :

$$P(D(Q)) > c_3[\mathrm{Log}(H(Q))]^{1/(100r^2)} ,$$

où r désigne le rang du groupe de Mordell $E(\mathbb{Q})$.

Démonstration : soit $E(\mathbb{Q})_t$ le sous-groupe de torsion de $E(\mathbb{Q})$, et $P_1,\ldots,P_r$ des représentants d'une base de $E(\mathbb{Q})/E(\mathbb{Q})_t$. Les lettres $c_4,\ldots,c_8$ apparaissant ci-dessous désignent des nombres réels > 0 ne dépendant que de A, B, $P_1,\ldots,P_r$.

Tout élément Q de $E(\mathbb{Q})$ s'écrit sous la forme $Q = h_1P_1 + \ldots + h_rP_r + P_t$, où $P_t \in E(\mathbb{Q})_t$, et $h_1,\ldots,h_r$ sont des entiers de module majoré par h, avec : $H(Q) > c_4^{h^2}$.

Pour tout nombre premier p, l'ensemble $E^{(p)}(\mathbb{Q}_p) = e_p(\mathcal{C}_p \cap \mathbb{Q}_p)$ est un sous-groupe d'indice fini du groupe $E_1^{(p)}(\mathbb{Q}_p)$ des points de $E(\mathbb{Q}_p)$ dont l'image par la réduction modulo p est le point à l'infini de la courbe réduite. Dans le cas considéré, les estimations de [3], § 2 montrent que $E^{(p)}(\mathbb{Q}_p) = E_1^{(p)}(\mathbb{Q}_p)$ dès que $p > 2$. On déduit donc du théorème 3 de [5] que l'indice γ_p de $E^{(p)}(\mathbb{Q}_p)$ dans $E(\mathbb{Q}_p)$ est, pour tout p, majoré par c_5p. Alors $\gamma_pQ = h_1(\gamma_pP_1) + \ldots + h_r(\gamma_pP_r)$, où γ_pP_i pour $i = 1,\ldots,r$, est un point de $E^{(p)}(\mathbb{Q})$ vérifiant : $H(\gamma_pP_i) < c_6^{p^2}$. Dans ces conditions, on tire de la proposition 2 :

$$|e_p^{-1}(\gamma_pQ)|_p > \exp[-c_2(\mathrm{Log}\ h)^{16r}(p^3\ \mathrm{Log}\ c_6)^{32r^2}]$$

soit :

$$|x(Q)|_p \leq |x(\gamma_p Q)|_p \leq \exp\left[c_8\, p^{96r^2}\, (\text{Log Log } H(Q))^{16r}\right] .$$

L'égalité $D(Q) = \prod_{p \mid D(Q)} |x(Q)|_p$, jointe à la proposition 1, permet de conclure.

Remarque : On notera que le seul point ineffectif de ce type de démonstration réside dans la détermination d'une base du groupe de Mordell-Weil.

***

[1] D. Bertrand, Note aux C. R. Acad. Sc. Paris, t. 282 (1976), série A, p. 1399.

[2] J. Coates, S. Lang, Inventiones Maths., 34 (1976), p. 129-133.

[3] E. Lutz, J. r. ang. Math., 177 (1937), p. 238-247.

[4] D.W. Masser, Elliptic functions and transcendence, S. L. N. No 437.

[5] J. Tate, Invent. Maths., 23 (1974), p. 179-206.

Centre de Mathématiques
de l'Ecole Polytechnique
Route de Saclay
91120 PALAISEAU (France)
