COMPOSITIO MATHEMATICA

DANIEL BERTRAND

Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe

Compositio Mathematica, tome 37, n° 1 (1978), p. 21-50

<http://www.numdam.org/item?id=CM_1978__37_1_21_0>

COMPOSITIO MATHEMATICA, Vol. 37, Fasc. 1, 1978, pag. 21–50.
Sijthoff & Noordhoff International Publishers–Alphen aan den Rijn
Printed in the Netherlands

APPROXIMATIONS DIOPHANTIENNES p-ADIQUES SUR LES COURBES ELLIPTIQUES ADMETTANT UNE MULTIPLICATION COMPLEXE

Daniel Bertrand

Introduction

Soient K un corps de nombres, E une courbe elliptique définie sur K, et, pour toute extension $\hat{K}$ de K, $E(\hat{K})$ l'ensemble des points $\hat{K}$-rationnels de E. Généralisant une idée de Gel'fond, Lang a montré dans [8] comment l'étude des points de $E(K)$ à coordonnées entières (théorème de Siegel) peut être ramenée à la minoration de certaines formes linéaires sur l'espace tangent à l'origine du groupe $E(\mathbf{C})$ des points complexes de E. Cette méthode, dont on trouvera un exposé plus complet dans [9], a été développée avec succès par Masser [11] dans le cas où E admet une multiplication complexe. Coates et Lang [6] ont amélioré les résultats de Masser en faisant appel à certaines propriétés galoisiennes des points de division des points de $E(K)$.

Nous présentons ici l'analogue de cette démarche dans le cas p-adique.[1] Plus précisément, on considère les complétés $K_\mathfrak{p}$ de K pour chaque place non archimédienne $\mathfrak{p}$ de K. L'ensemble $E(K_\mathfrak{p})$ peut être muni d'une structure de groupe de Lie $\mathfrak{p}$-adique, et l'application exponentielle $\epsilon_\mathfrak{p}$ sur $E(K_\mathfrak{p})$ permet d'en paramétrer un sous-groupe d'indice fini $\mathscr{E}_\mathfrak{p}$. Nous notons $\mathscr{M}_\mathfrak{p}$ l'ensemble des images réciproques (par $\epsilon_\mathfrak{p}^{-1}$) des points de $\mathscr{E}_\mathfrak{p}$ à coordonnées dans K.

Les éléments de $\mathscr{M}_\mathfrak{p}$ ont été étudiés dans [4] sans hypothèse supplémentaire sur E. Nous nous restreignons ici au cas où E admet une multiplication complexe. Son anneau d'endomorphisme $\operatorname{End} E$ est alors isomorphe à un ordre o d'un corps quadratique imaginaire k, et, si $k \subset K_\mathfrak{p}$, l'ensemble $\mathscr{M}_\mathfrak{p}$ peut être muni d'une structure de o-module.

[1] Je voudrais remercier J. Coates d'avoir attiré mon attention sur ce type de problème.

Dans la première partie de cet article, nous fixons une représentation de $\epsilon_{\mathfrak{p}}$, et nous étudions les combinaisons linéaires Λ d'éléments de $\mathcal{M}_{\mathfrak{p}}$ à coefficients algébriques; nous obtenons ainsi une version elliptique (et "non homogène") du résultat de Brumer concernant les formes linéaires de logarithmes p-adiques de nombres algébriques. La deuxième partie est consacrée à la recherche d'une minoration de la valeur absolue $\mathfrak{p}$-adique de Λ; nos estimations sont comparables à celles qu'ont initialement établies Coates et Sprindžuk dans le cas logarithmique. Lorsque $\mathfrak{p}$ décrit l'ensemble des places de K, on peut alors étudier les dénominateurs des points de $E(K)$. C'est le but de la troisième partie, où l'on énonce une version quantitative d'une généralisation classique du théorème de Siegel, due à Mahler [10]; il convient ici de noter que les méthodes logarithmiques fournissent dans ce domaine des résultats plus généraux, mais moins précis (voir en particulier les travaux de Coates, Kotov, Sprindžuk et Van der Poorten prolongeant au cas p-adique les énoncés du chapître 4 du livre de Baker [2]).

Signalons enfin que Masser a étendu les résultats de [11] aux variétés abéliennes dont l'anneau d'endomorphisme est maximal. C'est en fait sur ces variétés que Coates et Lang ont prouvé l'amélioration mentionée plus haut [6]. Un récent résultat d'analyse p-adique à plusieurs variables, dû à Robba, permet d'en obtenir des versions non archimédiennes, tout au moins pour certaines places de K. Nous reviendrons sur cette généralisation ultérieurement.[2]

I RESULTATS DE TRANSCENDANCE

§1.1 Notations et énoncés

Au moyen d'une transformation birationnelle, on peut donner l'équation de la courbe E sous la forme

$$Y^2Z - X^3 + aXZ^2 + bZ^3 = 0,$$

où a et b désignent des éléments de l'anneau $\mathcal{O}$ des entiers de K, tels que $4a^3 \neq 27b^2$. Quitte à augmenter K, on peut par ailleurs supposer que le corps k de multiplication complexe est un sous-corps de K. C'est sous ces hypothèses que nous nous plaçons désormais.

[2] Les résultats démontrés ci-dessous ont été annoncés aux C.r. Acad. Paris, t. 282 (sér. A), p. 1399. Certains d'entre eux ont indépendamment été obtenus par Lang (voir [9]).

Soient p un nombre premier, $\mathfrak{p}$ une place de K divisant p, $|\ |_{\mathfrak{p}}$ la valeur absolue de K telle que $|p|_{\mathfrak{p}} = p^{-1}$, $K_{\mathfrak{p}}$ le complété de K pour $\mathfrak{p}$, et $\mathcal{O}_{\mathfrak{p}}$ l'anneau des entiers $\mathfrak{p}$-adiques de $K_{\mathfrak{p}}$. (On prendra garde au choix de la normalisation de $|\ |_{\mathfrak{p}}$, qui ne correspond pas à celle de la formule de produit sur K). Dans les démonstrations des deux premières parties, nous poserons, pour alléger l'écriture:

$$|\ | = |\ |_{\mathfrak{p}}.$$

D'après [14], l'équation différentielle

$$y' = (1 - ay^4 - by^6)^{1/2};\ y(0) = 0$$

admet deux solutions φ et $-\varphi$ analytiques sur le disque

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

où $\lambda_{\mathfrak{p}} = (p-1)^{-1}$ si $p \neq 2$, $\lambda_{\mathfrak{p}} = 3$ si $p = 2$. De plus, φ établit une isométrie sur $\mathcal{C}_{\mathfrak{p}}$. (Pour $p = 2$, φ est en fait analytique sur un disque contenant strictement $\mathcal{C}_{\mathfrak{p}}$).

L'application exponentielle $\epsilon_{\mathfrak{p}}$ sur $E(K_{\mathfrak{p}})$ admet dans ces conditions la représentation:

$$z \to \{\varphi(z), -\varphi'(z), \varphi^3(z)\}.$$

C'est un isomorphisme: $\mathcal{C}_{\mathfrak{p}} \tilde{\to} \mathcal{E}_{\mathfrak{p}} = \epsilon_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}})$ de groupes de Lie $\mathfrak{p}$-adiques. L'ensemble $\mathcal{M}_{\mathfrak{p}}$ est alors formé des éléments de $\mathcal{C}_{\mathfrak{p}}$ où φ^2 et φ/φ' prennent des valeurs dans K, et le résultat que nous avons en vue peut s'énoncer comme suit:

THÉORÈME 1: *Soient $u_1, \ldots, u_n$ des éléments de $\mathcal{M}_{\mathfrak{p}}$ linéairement indépendants sur k. Alors, les nombres $1, u_1, \ldots, u_n$ sont linéairement indépendants sur K.*

Le théorème 1 découle de la conjonction des propositions 1 et 2 énoncées ci-dessous. On vérifie aisément qu'il lui est équivalent.

PROPOSITION 1: *Toute combinaison linéaire finie Λ d'éléments de $\mathcal{M}_{\mathfrak{p}}$ à coefficients dans K est nulle ou transcendante.*

C'est l'analogue p-adique du théorème de Masser démontré dans [11] appendice 3. Nous le prouverons aux §§1.2 et 1.3.

La proposition 2, qui précise les cas d'annulation de Λ, se déduit immédiatement du théorème 2 de la deuxième partie, et nous ne la démontrerons pas ici.

PROPOSITION 2: *Si n éléments de $\mathcal{M}_\mathfrak{p}$ sont linéairement indépendants sur k, ils le sont sur K.*

(Autrement dit, l'application K-linéaire de $K \otimes_\sigma \mathcal{M}_\mathfrak{p}$ dans $K_\mathfrak{p}$ qui prolonge l'injection de $\mathcal{M}_\mathfrak{p}$ dans $K_\mathfrak{p}$ est encore une injection).

Avant de passer à la démonstration de la proposition 1, nous indiquons quelques notations supplémentaires, qui seront conservées pendant tout l'article. Nous appelons norme d'un nombre algébrique α, et nous notons $\|\alpha\|$, le maximum des valeurs absolues archimédiennes de ses conjugués. Le dénominateur den α de α est le plus petit entier >0 tel que (den α)α soit un entier algébrique, et la taille $t(\alpha)$ de α est définie par:

$$t(\alpha) = \sup(\|\alpha\|, \text{den } \alpha).$$

La formule du produit sur $\mathbf{Q}$ entraîne alors $|\alpha| < \text{den } \alpha < t(\alpha)$. Inversement, si α est un nombre algébrique non nul de degré N, la formule de produit sur K montre que: $|\alpha| > t(\alpha)^{-2N}$. D'autre part, on a, sous les mêmes conditions: $t(\alpha^{-1}) \leq [2t(\alpha)]^{2N}$.

Par extension, la taille $t(P)$ d'un polynôme P à coefficients algébriques désigne le maximum des tailles de ses coefficients.

Notons $\mathcal{P} = \varphi^{-2}$ la fonction elliptique $\mathfrak{p}$-adique associée à $E(K_\mathfrak{p})$ (voir [14]). Elle vérifie l'équation différentielle:

$$(\mathcal{P}'/2)^2 = \mathcal{P}^3 - a\mathcal{P} - b,$$

et le théorème d'addition algébrique déduit de la loi de groupe sur E. En conséquence, pour tout élément non nul γ de l'ordre σ, on peut définir, au moyen d'identités algébriques, deux éléments A_γ et B_γ de $\mathcal{O}[X]$, premiers entre eux et tels que:

$$\mathcal{P}(\gamma z) = A_\gamma(\mathcal{P}(z))/B_\gamma(\mathcal{P}(z)).$$

On retrouve ainsi le fait que $\epsilon_\mathfrak{p}$ établit un isomorphisme de σ-module. En particulier (voir aussi [4], remarque 1), la fonction $B_\gamma \circ \mathcal{P}$ n'a pas de zéro sur $\mathcal{C}_\mathfrak{p}$, et les points de σ-torsion de E ne sont pas paramétrables par $\epsilon_\mathfrak{p}$.

Soient $\{1, \tau\}$ une base de l'ordre o, et, pour tout entier $h > 0$, $o(h)$ l'ensemble des éléments non nuls de o dont les coordonnées sont des entiers rationnels de norme $\leq h$. D'après [11], lemme 6.3, le degré – resp. la taille – des polynômes A_γ et B_γ associés aux éléments de $o(h)$ est majorée par ch^2 – resp. $\exp(ch^2)$ –, où $c = c(a, b)$ désigne un nombre réel >0 ne dépendant que de a et b.

Nous considérons des fonctions de n variables $\boldsymbol{z} = (z_1, \ldots, z_n)$, et nous emploierons les notations qui leur sont habituellement associées. En particulier, nous munissons l'ensemble des n-uples $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_n)$ de $\mathbf{N}^n$ de la relation d'ordre (partiel) produit $\leq$, nous notons $|\boldsymbol{\mu}|$ la longueur $\mu_1 + \cdots + \mu_n$ de $\boldsymbol{\mu}$, et nous posons:

$$D^{\boldsymbol{\mu}} = \partial^{\mu_1 + \cdots + \mu_n} / \partial z_1^{\mu_1} \ldots \partial z_n^{\mu_n},$$
$$\boldsymbol{z}^{\boldsymbol{\mu}} = z_1^{\mu_1} \ldots z_n^{\mu_n},$$

et, pour tout élément ζ de $K_\mathfrak{p}$:

$$\zeta \boldsymbol{z} = (\zeta z_1, \ldots, \zeta z_n).$$

Enfin, nous ferons appel à certains résultats d'analyse p-adique, pour lesquels nous reprenons les notations de [1], chapitre 4. Nous désignons par d l'opérateur de dérivation d/dz, et si f désigne une fonction (strictement) analytique au voisinage de l'origine de $K_\mathfrak{p}$, nous notons $R(f)$ le rayon de convergence de sa série de Taylor en 0. Soient $r < R(f)$ un nombre réel >0, et u un élément de $K_\mathfrak{p}$ de valeur absolue $< R(f)$. L'expression

$$|f|_u(r) = \sup_{m \in N} \frac{|d^m f(u)|}{|m!|} r^m$$

est alors définie, et l'on sait que, pour tout élément v de $K_\mathfrak{p}$ tel que $|v - u| \leq r$, on a:

$$|f|_v(r) = |f|_u(r)$$

mais, $K_\mathfrak{p}$ étant localement compact, le "principe du maximum" n'est en général pas vérifié.

EXEMPLE: Soient u un élément de $\mathscr{C}_\mathfrak{p}$ non nul, $\psi_u(z)$ la fonction $(zu)^2 \mathscr{P}(zu)$, et supposons que p soit un nombre premier impair (le cas $p = 2$ se traite de façon similaire). En vertu de l'équation différentielle satisfaite par φ (voir [14]), les nombres $d^m \varphi(0)$ sont des entiers $\mathfrak{p}$-adiques. Le développement en série de $\varphi(z)/z$ (qui permet d'ailleurs

d'établir le caractère isométrique de φ) montre donc que, pour tout nombre réel ρ tel que $0 \leq \rho < p^{-\lambda_\mathfrak{p}}$, on a: $|\varphi(z)/z|_0(\rho) = 1$. En conséquence, pour $r < p^{-\lambda_\mathfrak{p}}/|u|$, on obtient:

$$|\psi_u|_0(r) = 1,$$

et, si m et λ sont des entiers ≥ 0: $|d^m \psi_u^\lambda|_0(r) \leq r^{-m}$. (On notera cependant que les coefficients b_{2m} du développement

$$\mathscr{P}(z) = z^{-2} + \sum_{m>0} [b_{2m}/(2m)!] z^{2m},$$

qui sont liés aux "nombres de Bernoulli du corps k", ne sont pas tous entiers $\mathfrak{p}$-adiques). Signalons pour conclure que le rayon de convergence $R(\psi_u)$ de ψ_u est strictement supérieur à 1. Plus précisément, si $e_\mathfrak{p}$ désigne l'indice de ramification de p en $\mathfrak{p}$, le groupe des valeurs du groupe multiplicatif $K_\mathfrak{p}^*$ s'écrit, avec la normalisation de $|\ |_\mathfrak{p}$ définie plus haut: $(p^{1/e_\mathfrak{p}})^{\mathbb{Z}}$. La relation $\{u \in K_\mathfrak{p}, |u| < p^{-\lambda_\mathfrak{p}}\}$ entraîne donc:

$$|u| \leq p^{-\lambda_\mathfrak{p} - \rho_\mathfrak{p}},$$

où $\rho_\mathfrak{p} \geq [e_\mathfrak{p}(p-1)]^{-1}$. Ainsi, $R(\psi_u) \geq p^{[e_\mathfrak{p}(p-1)]^{-1}}$. Ces différentes remarques seront utilisées lors de l'application des lemmes d'interpolation p-adique.

La démonstration de la proposition 1 repose sur l'étude d'une fonction auxiliaire à partir des techniques de [11]. On conclut en faisant appel au théorème d'irréductibilité utilisé dans [6]. De plus, le caractère local de la situation simplifie les preuves. Il en sera de même au cours de la deuxième partie.

§1.2 La fonction auxiliaire

Soit $\Lambda = \alpha_1 u_1 + \cdots + \alpha_n u_n$ une combinaison linéaire d'éléments de $\mathscr{M}_\mathfrak{p}$, à coefficients dans K non tous nuls. Nous supposons que Λ est un nombre algébrique α_0 non nul, et nous nous proposons d'en déduire une contradiction. On peut, sans perte de généralité, se ramener au cas où K contient α_0, où $\alpha_0, \alpha_1, \ldots, \alpha_n$ sont des éléments de $\mathscr{O}_\mathfrak{p}$, et où $u_1, \ldots, u_n$ sont linéairement indépendants sur K. En vertu des propriétés de $\epsilon_\mathfrak{p}$ rappelées plus haut, cette dernière condition revient à supposer que les points $\epsilon_\mathfrak{p}(u_1), \ldots, \epsilon_\mathfrak{p}(u_n)$ sont linéairement indépendants sur End E.

La démonstration de la proposition 1 comporte trois étapes. Nous considérons un paramètre entier H arbitrairement grand, et nous désignons par $c_1, \ldots, c_{14}$, des nombres réels >0 ne dépendant que de α_0, $\boldsymbol{\alpha}$, $\boldsymbol{u}$, $\mathfrak{p}$, a, b et K.

PREMIER PAS: Soient $M = H^4$, $L = [M^{1-1/(4(n+1))}]$. Il existe des entiers rationnels $p_{\lambda_0,\ldots,\lambda_n}$, non tous nuls, dont le maximum N des normes est $\leq c_1^{MH}$, tels que la fonction:

$$F(z_1, \ldots, z_n) = \sum_{\substack{0 \leq \lambda_i < L \\ 0 \leq i \leq n}} p_{\lambda_0,\ldots,\lambda_n} \mathscr{P}(z_1)^{\lambda_1} \ldots \mathscr{P}(z_n)^{\lambda} (\alpha_1 z_1 + \cdots + \alpha_n z_n)^{\lambda_0}$$

vérifie:

$$\forall \boldsymbol{\mu} \in \mathbf{N}^n,\ |\boldsymbol{\mu}| < M;\ \forall \boldsymbol{\gamma} \in \mathfrak{o}(H): D^{\mu} F(\boldsymbol{\gamma u}) = 0.$$

Il s'agit en effet de résoudre un système linéaire homogène de $c_2 H^2 M^n$ équations à L^{n+1} inconnues dont les coefficients sont, du fait de l'hypothèse faite sur Λ, des éléments du corps de nombres K. Leur taille est majorée par:

$$2^M c_3^M [(c_5(M+L)H^2)^{c_5 M} \exp(c_5(M+L)H^2)]^{n+1},$$

ainsi que le montre la formule de Leibniz, jointe au lemme suivant.

LEMME 1: *Il existe un nombre réel $c_4 = c_4(a, b, \tau)$ tel que, pour tout couple d'entiers $m \geq 0$, $\lambda > 0$, et tout élément γ de $\mathfrak{o}(h)$, on ait*:

$$d^m[\mathscr{P}^{\lambda}(\gamma z)] = A_{m,\lambda,\gamma}(\mathscr{P}(z), \mathscr{P}'(z)) / B_{\gamma}^{m+\lambda}(\mathscr{P}(z)),$$

où $A_{m,\lambda,\gamma}$ est un élément de $K[X, Y]$ de degré total $\leq c_4(m+\lambda)h^2$ de taille:

$$t(A_{m,\lambda,\gamma}) \leq [c_4(m+\lambda)h^2]^{c_4 m} \exp(c_4(m+\lambda)h^2).$$

DÉMONSTRATION: Voir [4], lemme 1. Le calcul des tailles se déduit alors de la non nullité de $B_{\gamma} \circ \mathscr{P}(u_i)$.

Le lemme de Siegel (voir par exemple [11], lemma 1.7) permet donc de choisir une solution non triviale du système, à coefficients $p_{\lambda_0,\ldots,\lambda_n}$ entiers rationnels de norme $\leq N$, avec:

$$N \leq \exp(c_1 M H^2 \cdot M^n H^2 / L^{n+1}) \leq \exp(c_1 M H).$$

DEUXIEME PAS: Posons $\delta = [16(n+1)]^{-1}$, et pour tout entier $j \geq 0$,

$$M_j = M/2^j;\ H_j = HM^{j\delta}.$$

Nous dirons que la fonction F vérifie la propriété $\mathscr{D}_j$ si:

$$\forall \boldsymbol{\mu}, |\boldsymbol{\mu}| < M_j;\ \forall \gamma \in \mathscr{o}(H_j) : D^{\boldsymbol{\mu}} F(\gamma \boldsymbol{u}) = 0.$$

Par construction, F vérifie $\mathscr{D}_0$. Nous allons montrer que la propriété $\mathscr{D}_j$ est satisfaite pour tout entier $j \leq J = 16(n+1)^2$. Nous procédons par récurrence, et nous admettons $\mathscr{D}_{j-1}$. Supposons que F ne vérifie pas $\mathscr{D}_j$, i.e. qu'il existe un élément g de $\mathscr{o}(H_j)$ et un n-uple $\boldsymbol{m}$ de longueur $< M_j$ tel que:

$$\xi = D^{\boldsymbol{m}} F(g\boldsymbol{u}) \neq 0.$$

Nous convenons de choisir un n-uple de longueur minimale vérifiant cette propriété. Le lemme 2 énoncé ci-dessous fournit alors une majoration de la taille de ξ, d'où l'on déduit, d'après la formule du produit sur K:

$$|\xi| \geq \exp(-c_6 L H^2 M^{2j\delta}).$$

LEMME 2: *Il existe un nombre réel $c_7 = c_7(a, b, \tau)$ vérifiant la propriété suivante: soient γ un point de $\mathscr{o}(h)$, et $\boldsymbol{m}$ un élément de $\mathbf{N}^n$ de longueur m tel que*:

$$\forall \boldsymbol{\mu}, |\boldsymbol{\mu}| < m : D^{\boldsymbol{\mu}} F(\gamma \boldsymbol{u}) = 0.$$

Alors:

$$D^{\boldsymbol{m}} F(\gamma \boldsymbol{u}) = R_{\boldsymbol{m},F,\gamma}(\mathscr{P}(u_1), \mathscr{P}'(u_1), \ldots, \mathscr{P}'(u_n), \alpha_0) \Big/ \prod_{i=1}^{n} B_\gamma^L(\mathscr{P}(u_i)),$$

où $R_{\boldsymbol{m},F,\gamma}$ est un élément de $K[X_1, \ldots, Y_n, X_0]$ de degré total $\leq c_7(m + Lh^2)$, de taille

$$t(R_{\boldsymbol{m},F,\gamma}) \leq N(c_5(m + Lh^2))^{c_5 m} \exp(c_5(m + Lh^2)).$$

DÉMONSTRATION: Considérons (cf. [11], lemma 7.7, [4], lemme 2) la fonction:

$$\Phi(\boldsymbol{z}) = \left(\prod_{i=1}^{n} B_\gamma^L(\mathscr{P}(z_i)) \right) F(\gamma \boldsymbol{z}).$$

Cette fonction s'écrit sous la forme $R(\mathscr{P}(z_1), \ldots, \mathscr{P}(z_n), \alpha_1 z_1 + \cdots + \alpha_n z_n)$ où R est un élément de $K[X_1, \ldots, X_n X_0]$ de degré total $\leq c_8 L h^2$, de taille $\leq N \exp(c_8 L h^2)$.

On déduit de la formule de Leibniz et du lemme 1 (avec $\gamma = 1$) qu'il existe an élément $R'_{\boldsymbol{m},F,\gamma}$ de $K[X_1, \ldots, Y_n, X_0]$, dont le degré total et la taille vérifient les conditions du lemme 2, et tel que:

$$D^{\boldsymbol{m}}\Phi(\boldsymbol{z}) = R'_{\boldsymbol{m},F,\gamma}(\mathscr{P}(z_1), \ldots, \mathscr{P}'(z_n), \alpha_1 z_1 + \cdots + \alpha_n z_n).$$

Mais l'hypothèse du lemme 2 entraîne:

$$D^{\boldsymbol{m}}\Phi(\boldsymbol{u}) = \gamma^m \left(D^{\boldsymbol{m}} F(\gamma \boldsymbol{u}) \prod_{i=1}^{n} B_\gamma^L(\mathscr{P}(u_i)) \right),$$

ce qui en achève la démonstration.

Il reste à majorer $|\xi|$. Pour cela, nous posons

$$\Theta(\boldsymbol{z}) = z_1^{2L} \ldots z_n^{2L},$$

et nous considérons la fonction d'une variable:

$$f(z) = [D^{\boldsymbol{m}}(\Theta F)](z\boldsymbol{u}).$$

La minimalité de $\boldsymbol{m}$ entraîne:

$$f(g) = \Theta(g\boldsymbol{u}) D^{\boldsymbol{m}} F(g\boldsymbol{u}),$$

d'où: $|\xi| \leq (c_7 |g|)^{-2nL} |f(g)|$, soit:

$$|\xi| \leq (c_8 H_j)^{c_8 L} |f(g)|.$$

En effet:

LEMME 3: *Il existe un nombre réel $c_9 = c_9(\tau) > 0$ tel que, pour tout élément γ de $o(h)$, on ait*
– si p se décompose dans k : $|\gamma| > c_9 h^{-2}$
– si p reste inerte ou se ramifie dans k : $|\gamma| > c_9 h^{-1}$.

DÉMONSTRATION: Il suffit d'appliquer la formule du produit sur k. Nous n'aurons en fait à utiliser ici que la minoration banale: $|\gamma| > c_9 h^{-2}$.

En vertu de l'observation faite au §1.1 (exemple), le rayon de convergence $R(f)$ de la fonction f est >1. Par ailleurs, f admet les points de $o(H_{j-1})$ pour zéros d'ordre $\geq M_j$. Ceci résulte de la formule:

$$d^s f(\gamma) = \sum_{\mu \leq m} \binom{m}{\mu} \sum_{|\sigma|=s} [s!/(\sigma!)] u^\sigma \sum_{\kappa \leq \sigma} \binom{\sigma}{\kappa} [D^{\mu+\kappa} F](\gamma u) \times [D^{m+\sigma-\mu-\kappa} \Theta](\gamma u)$$

jointe à la propriété $\mathscr{D}_{j-1}$, et à la relation:

$$\{|\mu| \leq |m| < M/2^j, |\kappa| \leq |\sigma| < M/2^j\} \Rightarrow |\mu + \kappa| < M/2^{j-1}.$$

Comme $o(H_{j-1})$ est inclus dans l'anneau $\mathscr{O}_\mathfrak{p}$, et que, pour $r < R(f)$, on a $|f|_0(r) \leq 1$, le lemme de Schwarz rappelé plus bas fournit la majoration:

$$|f(g)| \leq [R(f)]^{-c_2 M_j H_{j-1}^2} \leq \exp(-c_{10} M H^2 M^{2(j-1)\delta}/2^j).$$

Si $j \leq J$, cette inégalité est incompatible avec la minoration de $|\xi|$ obtenue par le lemme 2, et la proposition $\mathscr{D}_j$ est démontrée. (On notera que l'extrapolation aurait pu être poussée jusqu'à $j = c_{11} \operatorname{Log} H$).

LEMME 4: (Lemme de Schwarz): *Soient f une fonction analytique au voisinage de l'origine, $0 < r_1 < r_2$ deux nombres réels $< R(f)$. Si f admet ν zéros (comptés avec leurs ordres de multiplicité) de valeur absolue $\leq r_1$, alors*:

$$|f|_0(r_1) \leq \left(\frac{r_1}{r_2}\right)^\nu |f|_0(r_2).$$

§1.3 Fin de la démonstration

TROISIÈME PAS: Nous ne considérons désormais que les valeurs de F aux points de division de $u_1, \ldots, u_n$. De façon précise, nous allons montrer que, pour tout entier q de l'ensemble $\mathscr{Q} = \{q$ premier, $q \neq p$, $L^{1/2} < q < 2L \operatorname{Log} L\}$, on a $F(q^{-1}u) = 0$.

Supposons qu'il existe un nombre premier q de l'intervalle consi-

déré tel que $\eta = F(q^{-1}\boldsymbol{u}) \neq 0$. La minoration

$$|\eta| > \exp(-c_{11}q^{2n}(MH + L \operatorname{Log} q)$$
$$> \exp(-c_{12}L^{2n}MH(\operatorname{Log} L)^{2n})$$

se déduit du lemme suivant.

LEMME 5: *Si l est un nombre premier à p, $\mathscr{P}(l^{-1}u_i)$, est, pour $i = 1, \ldots, n$, un nombre algébrique de degré $\leq l^2$ sur K, de taille $\leq c_{12}l^2$.*

DÉMONSTRATION: Voir par exemple [4], lemme 6.

Une majoration de $|\eta|$ est fournie par le lemme de Schwarz, appliqué cette fois à la fonction $f_1(z) = (\Theta F)(z\boldsymbol{u})$. Son rayon de convergence est >1, et on vérifie, par un raisonnement similaire à celui du §1.2, qu'elle admet les points de $o(H_J)$ pour zéros d'ordre $\geq M_J$. En conséquence:

$$|\eta| \leq c_7^{2nL}|f_1(q^{-1})| \leq c_7^{2nL} \exp(-c_{13}M_JH_J^2)$$
$$\leq \exp(-c_{14}MH^2M^{2(n+1)}).$$

En comparant les différentes estimations de $|\eta|$, on conclut à une contradiction.

En définitive, nous avons construit un élément P de $Z[X_1, \ldots, X_n, X_0]$, de degré $<L$ en chaque variable, vérifiant:

$$\forall q \in \mathscr{Q} : P\left(\mathscr{P}\left(\frac{u_1}{q}\right), \ldots, \mathscr{P}\left(\frac{u_n}{q}\right), \frac{\alpha_0}{q}\right) = 0.$$

et tel que les polynômes

$$p_{\lambda_1, \ldots, \lambda_n}(X_0) = \sum_{0 \leq \lambda_0 < L} p_{\lambda_0, \lambda_1, \ldots, \lambda_n} X_0^{\lambda_0};$$
$$(\text{pour } \lambda_i = 0, \ldots, L-1;\ i = 1, \ldots, n)$$

ne soient pas tous identiquement nuls.

Comme α_0 est non nul, le cardinal de l'ensemble $\{q^{-1}\alpha_0,\ q \in \mathscr{Q}\}$ majore le degré de chacun de ces polynômes. Il existe donc un nombre $l \in \mathscr{Q}$ tel que la relation:

$$\sum_{\substack{0 \leq \lambda_i < L \\ 1 \leq i \leq n}} p_{\lambda_1, \ldots, \lambda_n}\left(\frac{\alpha_0}{l}\right)\mathscr{P}\left(\frac{u_1}{l}\right)^{\lambda_1} \ldots \mathscr{P}\left(\frac{u_n}{l}\right)^{\lambda_n} = 0$$

ne soit pas triviale, et l'un au moins des nombres $\mathscr{P}(u_1/l), \ldots, \mathscr{P}(u_n/l)$, soit $\mathscr{P}(u_i/l)$, vérifie une équation algébrique à coefficients non tous nuls, de degré $< L < l^2$ sur le corps $K(\mathscr{P}(u_1/l), \ldots, \mathscr{P}(u_{i-1}/l))$. Or ceci est impossible, car en vertu de l'indépendance linéaire des points $\epsilon_{\mathfrak{p}}(u_1), \ldots, \epsilon_{\mathfrak{p}}(u_n)$ sur End E, on a:

LEMME 6 (Bašmakov): *Il existe un entier* $l_0 = l_0\ (a, b, u_1, \ldots, u_n)$ *tel que, pour tout nombre premier* $l > l_0$, *l'extension* $K(\mathscr{P}(u_1/l), \ldots, \mathscr{P}(u_n/l))$ *soit de degré* l^{2n} *sur* K.

DÉMONSTRATION: Une généralisation du lemme 6 est prouvée dans [12].

Cette dernière contradiction achève la démonstration de la proposition 1.

II MINORATIONS EFFECTIVES

§2.1 Enoncé du résultat

La méthode utilisée dans la première partie permet de montrer que, si $u_0, u_1, \ldots, u_n$ sont $n+1$ éléments de $\mathscr{M}_{\mathfrak{p}}$ linéairement indépendants sur k, la forme linéaire $\Lambda = \alpha_1 u_1 + \cdots + \alpha_n u_n$ ne peut valoir u_0 (proposition 2). Il suffit pour cela de remplacer, dans l'expression de la fonction auxiliaire F, les monômes $(\alpha_1 z_1 + \cdots + \alpha_n z_n)^{\lambda_0}$ par: $\mathscr{P}^{\lambda_0}(\alpha_1 z_1 + \cdots + \alpha_n z_n)$, et de modifier en conséquence la conclusion de §1.3.

Nous donnons ici une version quantitative de la proposition 2: il s'agit d'une minoration de $|\Lambda - u_0|$ en fonction de grandeurs arithmétiques liées à $\alpha_1, \ldots, \alpha_n$, $u_0, \ldots, u_n$ et $\mathfrak{p}$. A cet effet, nous conviendrons d'appeler taille d'un point de $E(K)$ la taille de son abscisse (sur le modèle $\{Z = 1\}$ de E). Ainsi:

$$t(\epsilon_{\mathfrak{p}}(u_i)) = t(\mathscr{P}(u_i)).$$

THÉORÈME 2: *Soit* U *un entier* > 0, *et* $\epsilon_{\mathfrak{p}}(u_0), \ldots, \epsilon_{\mathfrak{p}}(u_n)$, $n+1$ *points de* $\mathscr{E}_{\mathfrak{p}}$ *linéairement indépendants sur* End E, *de taille* $< U$. *Il existe un nombre réel* $C = C(a, b, K, n) > 0$, *effectivement calculable, tel que l'inéquation*

$$|\alpha_0 u_0 + \cdots + \alpha_n u_n|_{\mathfrak{p}} < \exp[-C(\operatorname{Log} A)^{8(n+1)} p^{16(n+1)^2} (\operatorname{Log} U)^{16(n+1)^2}].$$

n'ait pas de solutions en éléments $\alpha_0, \ldots, \alpha_n$ *de* K, *de taille* $< A$, *non tous nuls.*

Soient $\alpha_1, \ldots, \alpha_n$ des éléments de $K \cap \mathcal{O}_\mathfrak{p}$ de taille $< A$, non tous nuls, et posons:

$$\Omega = \Omega(A, p, U) = (\operatorname{Log} A)^{8n+7} p^{16(n+1)^2} (\operatorname{Log} U)^{16(n+1)^2}.$$

La validité du théorème 2 sera assurée si l'on prouve que, dès que A est suffisamment grand (en fonction de a, b, K et n), on a:

$$|\alpha_1 u_1 + \cdots + \alpha_n u_n - u_0| = |\Lambda - u_0| \geq \exp(-2\Omega).$$

Nous allons déduire cette assertion des propositions 3 et 4 énoncées ci-dessous.

PROPOSITION 3: *Il existe un entier* $A_0 = A_0(a, b, K, n)$ *effectivement calculable et vérifiant la propriété suivante: supposons que l'inégalité* $|\Lambda - u_0| < \exp(-2\Omega)$ *soit satisfaite pour un nombre réel* $A > A_0$, *et posons*

$$H = [(\operatorname{Log} A)(p \operatorname{Log} U)^{2(n+1)}].$$

Alors, il existe un élément non nul P *de* $\mathbb{Z}[X_1, \ldots, X_n, X_0]$, *de degré* $< L = H^{4-1/(n+1)}$ *en chaque variable, et un nombre premier* $q > L^{1/2}$, *tels que*:

$$P(\mathcal{P}(u_1/q), \ldots, \mathcal{P}(u_n/q), \mathcal{P}(u_0/q)) = 0.$$

La preuve de la proposition 3 fait l'objet des §§2.2 et 2.3.

PROPOSITION 4 (Cassels): *On reprend les hypothèses du théorème 2. Il existe un nombre réel* $C' = C'(a, b, K, n)$ *effectivement calculable, tel que, pour tout nombre premier* $l > l_0 = C'(\operatorname{Log} U)^{n+1}$, *l'extension* $K(\mathcal{P}(u_0/l), \ldots, \mathcal{P}(u_n/l))$ *soit de degré* $l^{2(n+1)}$ *sur* K.

La démonstration de cette proposition (qui précise le lemme 6) repose sur une propriété de la fonction hauteur, rappelée dans la troisième partie de l'article. Elle sera reproduite au §3.1.

Montrons comment ces deux résultats entraînent le théorème 2. D'après la proposition 3, il existe un indice i, $0 \leq i \leq n$, tel que le nombre $\mathcal{P}(u_i/q)$ vérifie une équation algébrique non triviale de degré $< q^2$ sur le corps $K(\mathcal{P}(u_0/q), \ldots, \mathcal{P}(u_{i-1}/q))$. Mais ceci contredit la

proposition 4, car, pour A suffisamment grand:

$$q > L^{1/2} > C'(\text{Log } U)^{n+1}$$

et l'hypothèse de la proposition 3 ne peut avoir lieu.

Mis a part le calcul de la dépendance en p, la démonstration de la proposition 3 suit la démarche de [11], théorème 5 et [6].

§2.2 Quelques préparatifs

Nous donnons tout d'abord une série de résultats qui répondent, dans la situation quantitative étudiée ici, aux lemmes de la première partie. Nous reprenons les notations des §§1.1 et 2.1. En particulier, on gardera à l'esprit le fait que $\alpha_1, \ldots, \alpha_n$ sont des entiers $\mathfrak{p}$-adiques, et que, U majorant le taille des points $\epsilon_{\mathfrak{p}}(u_i)$, on a: $|u_i| = |\mathscr{P}(u_i)|^{-1/2} > U^{-1/2}$.

Nous définissons A_0 comme le plus petit entier tel que, si $A > A_0$, les estimations qui suivent soient justifiées, les lettres $C_1, \ldots, C_{18}$ désignant alors des nombres réels >0 effectivement calculables en fonction de a, b, K et n.

Nous considérons des fonctions de la forme:

$$F(z) = \sum_{\substack{0 \le \lambda_i < L \\ 0 \le i \le n}} p_{\lambda_0, \ldots, \lambda_n} \mathscr{P}(z_1)^{\lambda_1} \ldots \mathscr{P}(z_n)^{\lambda_n} \mathscr{P}(\alpha_1 z_1 + \cdots + \alpha_n z_n)^{\lambda_0}.$$

où L est un entier >0, et dont les coefficients $p_{\lambda_0, \ldots, \lambda_n}$ sont des entiers rationnels. A tout n-uple $\boldsymbol{m}$ de $\mathbf{N}^n$, on associe la dérivée de F pour l'operateur de dérivation $D^{\boldsymbol{m}}$:

$$D^{\boldsymbol{m}} F(z) = \sum_{(\lambda)} p_{\lambda_0, \ldots, \lambda_n} \sum_{\boldsymbol{\mu} \le \boldsymbol{m}} \binom{\boldsymbol{m}}{\boldsymbol{\mu}} \boldsymbol{\alpha}^{\boldsymbol{\mu}} (d^{m_1 - \mu_1} \mathscr{P}^{\lambda_1})(z_1) \ldots$$
$$\ldots (d^{m_n - \mu_n} \mathscr{P}^{\lambda_n})(z_n) (d^{\mu_1 + \cdots + \mu_n} \mathscr{P}^{\lambda_0})(\alpha_1 z_1 + \cdots + \alpha_n z_n).$$

et la fonction des $n+1$ variables $\{z_1, \ldots, z_n, z_0\} = (z, z_0)$

$$L^{\boldsymbol{m}} F(z, z_0) = \sum_{(\lambda)} p_{\lambda_0, \ldots, \lambda_n} \sum_{\boldsymbol{\mu} \le \boldsymbol{m}} \binom{\boldsymbol{m}}{\boldsymbol{\mu}} \boldsymbol{\alpha}^{\boldsymbol{\mu}} (d^{m_1 - \mu_1} \mathscr{P}^{\lambda_1})(z_1) \ldots$$
$$\ldots (d^{m_n - \mu_n} \mathscr{P}^{\lambda_n})(z_n) (d^{\mu_1 + \cdots + \mu_n} \mathscr{P}^{\lambda_0})(z_0)$$

(de sorte que: $L^{\boldsymbol{m}} F(z, \alpha_1 z_1 + \cdots + \alpha_n z_n) = D^{\boldsymbol{m}} F(z)$).

Le lemme 1 de la première partie entraîne que, pour tout élément γ de o non nul, les nombres $L^{\mathbf{m}}F(\gamma \mathbf{u}, \gamma u_0)$ appartiennent à K, et permet d'en majorer les tailles. Voici l'analogue du lemme 2. On note N un majorant des normes des entiers $p_{\lambda_0,\ldots,\lambda_n}$.

LEMME 7: *Il existe un nombre réel $C_1 = C_1(a, b, \tau)$ vérifiant la propriété suivante: soit γ un point de $o(h)$, et $\mathbf{m}$ un élément de longueur m tel que:*

$$\forall \boldsymbol{\mu}, |\boldsymbol{\mu}| < m : L^{\boldsymbol{\mu}}F(\gamma \mathbf{u}, \gamma u_0) = 0.$$

Alors:

$$L^{\mathbf{m}}F(\gamma \mathbf{u}, \gamma u_0) = R^0_{\mathbf{m},F,\gamma}(\mathcal{P}(u_1), \ldots, \mathcal{P}'(u_n), \mathcal{P}(u_0), \mathcal{P}'(u_0)) \Big/ \prod_{i=0}^{n} B^L_\gamma(\mathcal{P}(u_i))$$

où $R^0_{\mathbf{m},F,\gamma}$ est un élément de $K[X_1, \ldots, Y_0]$ de degré total $\leq C_1(m + Lh^2)$, de taille

$$t(R^0_{\mathbf{m},F,\gamma}) \leq N(C_1(m + Lh^2))^{C_1 m} \exp(C_1(m + Lh^2)).$$

DÉMONSTRATION: Considérons (voir [11], lemme 7.7, [4] lemme 4) l'application affine: $V(z) = \alpha_1(z_1 - u_1) + \cdots + \alpha_n(z_n - u_n) + u_0$, et la fonction:

$$F^0_\gamma(\mathbf{z}) = \sum_{(\lambda)} p_{\lambda_0,\ldots,\lambda_n} \mathcal{P}^{\lambda_1}(\gamma z_1) \ldots \mathcal{P}^{\lambda_n}(\gamma z_n) \mathcal{P}^{\lambda_0}(\gamma V(\mathbf{z})),$$

qui vérifie, pour tout $\boldsymbol{\mu} \in N^n$:

$$D^{\boldsymbol{\mu}}F^0_\gamma(\mathbf{u}) = \gamma^{|\boldsymbol{\mu}|} L^{\boldsymbol{\mu}}F(\gamma \mathbf{u}, \gamma u_0),$$

Si $\Phi^0(\mathbf{z}) = (\prod_{i=1}^n B^L_\gamma(\mathcal{P}(z_i)))B^L_\gamma(\mathcal{P}(V(\mathbf{z}))F^0_\gamma(\mathbf{z})$, on a sous les hypothèses du lemme 7:

$$D^{\mathbf{m}}\Phi^0(\mathbf{u}) = \left(\prod_{i=0}^{n} B^L_\gamma(\mathcal{P}(u_i))\right)\gamma^m L^{\mathbf{m}}F(\gamma \mathbf{u}, \gamma u_0).$$

La fonction Φ^0 s'écrit sous la forme $R^0(\mathcal{P}(z_1), \ldots, \mathcal{P}(z_n), \mathcal{P}(V(\mathbf{z})))$, où R^0 est un élément de $K[X_1, \ldots, X_n, X_0]$, et un raisonnement similaire à celui du lemme 2 permet de conclure.

Le résultat suivant précise le lemme 5.

LEMME 8: *Si l est un nombre premier à p, $\mathscr{P}(l^{-1}u_i)$ est, pour $i = 0, \ldots, n$, un nombre algébrique de degré $\leq l^2$ sur K, de taille $\leq C_2 U l^2$.*

DÉMONSTRATION: L'équation de division par l de $\mathscr{P}(u_i)$ montre que den $\mathscr{P}(u_i/l)$ divise den $\mathscr{P}(u_i)$ (voir [11], lemme 6.4; [4], lemme 5). Soient d'autre part $|\ |_\infty$ la valeur absolue de $\mathbf{C}$, σ un plongement de $K(\mathscr{P}(u_i/l))$ dans $\mathbf{C}$, $\mathscr{P}^\sigma$ la fonction elliptique de Weierstrass (complexe) d'invariants $4\sigma(a)$, $4\sigma(b)$, Λ^σ le réseau des périodes de $\mathscr{P}^\sigma$, et u_i^σ un nombre complexe tel que: $\mathscr{P}^\sigma(u_i^\sigma) = \sigma(\mathscr{P}(u_i))$. Il existe alors un élément ω_i^σ de Λ^σ tel que $\mathscr{P}^\sigma[(u_i^\sigma + \omega_i^\sigma)/l] = \sigma(\mathscr{P}(u_i/l))$, et les relations:

$$\inf_{\omega \in \Lambda^\sigma} |z - \omega|_\infty^{-2} - C_3 \leq |\mathscr{P}^\sigma(z)|_\infty \leq \inf_{\omega \in \Lambda^\sigma} |z - \omega|_\infty^{-2} + C_3,$$

où $C_3 = C_3(a, b, \sigma)$, entraînent:

$$|\sigma(\mathscr{P}(u_i/l))|_\infty \leq l^2(|\sigma(\mathscr{P}(u_i))|_\infty + C_3) + C_3.$$

Ainsi

$$\|\mathscr{P}(u_i/l)\| \leq C_2 U l^2,$$

et le lemme 8 est démontré.

Nous ferons par ailleurs appel à deux lemmes de nature analytique.

LEMME 9: *Supposons que $|\Lambda - u_0| < \exp(-2\Omega)$, et posons: $H = (\operatorname{Log} A)(p \operatorname{Log} U)^{2(n+1)}$. Soient $\boldsymbol{m}$ un élément de $\mathbf{N}^n$ de longueur $m \leq H^4$, ζ un entier $\mathfrak{p}$-adique de valeur absolue $\geq H^{-4(n+1)-3}$. Si $L \leq H^4$, on a:*

$$|D^{\boldsymbol{m}}F(\zeta \boldsymbol{u}) - L^{\boldsymbol{m}}F(\zeta \boldsymbol{u}, \zeta u_0)| < \exp(-\Omega).$$

DÉMONSTRATION: Des expressions de $D^{\boldsymbol{m}}F$ et $L^{\boldsymbol{m}}F$, on tire:

$$|D^{\boldsymbol{m}}F(\zeta \boldsymbol{u}) - L^{\boldsymbol{m}}F(\zeta \boldsymbol{u}, \zeta u_0)| \leq \sup_{(\lambda_i), \boldsymbol{\mu}} \left\{ \left| \prod_{i=1}^{n} (d^{m_i - \mu_i} \mathscr{P}^{\lambda_i})(\zeta u_i) \right| \right.$$
$$\left. \times |(d^{|\boldsymbol{\mu}|} \mathscr{P}^{\lambda_0})(\zeta \Lambda) - (d^{|\boldsymbol{\mu}|} \mathscr{P}^{\lambda_0})(\zeta u_0)| \right\}.$$

Or, en vertu des remarques faites au §1.1:

$$|\mathscr{P}^\lambda|_{\zeta u_i}(|\zeta u_i|/2) = |\zeta u_i|^{-2\lambda},$$

d'où:

$$|(d^{m_i-\mu_i}\mathscr{P}^{\lambda})(\zeta u_i)| \leq |(m_i-\mu_i)!|(|\zeta u_i|/2)^{-2\lambda-(m_i-\mu_i)} \leq (HU)^{C_4(L+m)}$$

De même, si $|\Lambda - u_0| < \exp(-2\Omega)$, alors $|\zeta\Lambda - \zeta u_0| < |\zeta u_0|/2$, et:

$$\begin{aligned}|(d^{|\mu|}\mathscr{P}^{\lambda_0})(\zeta\Lambda) - (d^{|\mu|}\mathscr{P}^{\lambda_0})(\zeta u_0)| &\leq \sup_{k\geq 1} \frac{|(d^{|\mu|+k}\mathscr{P}^{\lambda_0})(\zeta u_0)|}{|k!|}|\zeta\Lambda - \zeta u_0|^k \\ &\leq |\Lambda - u_0|(|\zeta u_0|/2)^{-2\lambda_0-|\mu|-1} \\ &\leq (HU)^{C_4(L+m+1)}\exp(-2\Omega).\end{aligned}$$

En comparant ces estimations à la valeur de Ω, on obtient l'inégalité recherchée.

Le lemme d'interpolation suivant précise le lemme de Schwarz.

LEMME 10: *Soient f une fonction analytique au voisinage de l'origine, $0 < r_1 < r_2$ deux nombres réels $< R(f)$, Γ un ensemble fini de points de $K_{\mathfrak{p}}$ de valeur absolue $< r_1$, et m un entier > 0. Posons*:

$$\omega = \sup_{\substack{\gamma\in\Gamma \\ s\leq m-1}} \frac{|d^s f(\gamma)|}{|s!|}; \quad \delta = \inf_{\substack{\gamma\neq\gamma' \\ \gamma,\gamma'\in\Gamma}} |\gamma - \gamma'|.$$

Alors:

$$|f|_0(r_1) \leq \sup\{(r_1/r_2)^{hm}|f|_0(r_2), (r_1/\delta)^{hm-1}\omega\}.$$

DÉMONSTRATION: Voir [3], proposition 4.

§2.3 Démonstration de la proposition 3

Nous reprenons les notations du §2.2. On suppose que

$$|\Lambda - u_0| < \exp(-2\Omega)$$

où, dans l'expression de Ω, A est un majorant des tailles de $\alpha_1, \ldots, \alpha_n$, supérieur à A_0. On pose $H = [(\operatorname{Log} A)(p \operatorname{Log} U)^{2(n+1)}]$, $M = H^4$. La démonstration de la proposition 3 se fait en trois étapes.

PREMIER PAS: Il existe un élément non nul P de $\mathbb{Z}[X_1, \ldots, X_n, X_0]$

de degré $< L = [M^{1-1/4(n+1)}]$ en chaque variable, de taille $\leq U^{C_5 MH}$, tel que la fonction

$$F(z) = P(\mathscr{P}(z_1), \ldots, \mathscr{P}(z_n), \mathscr{P}(\alpha_1 z_1 + \cdots + \alpha_n z_n))$$

vérifie:

$$\forall \mu \in \mathbf{N}^n, |\mu| < M; \forall \gamma \in o(H): L^{\mu} F(\gamma u, \gamma u_0) = 0.$$

Cela revient en effet à résoudre un système linéaire homogène de $C_4 H^2 M^n$ équations à L^{n+1} inconnues, dont les coefficients sont des éléments de K de taille majorée par:

$$2^M A^M [(C_6(M+L)H^2)^{C_6 M} \exp(C_6(M+L)H^2 \operatorname{Log} U)]^{n+1},$$

en vertu du lemme 1.

Le lemme de Siegel permet d'en choisir une solution non triviale à coefficients entiers rationnels de norme $\leq N \leq \exp(C_5 MH \operatorname{Log} U)$.

Deuxième pas: Posons $\delta = [16(n+1)]^{-1}$, et, pour tout entier $j \geq 0$:

$$M_j = M/2^j, H_j = HM^{j\delta}.$$

Nous dirons que la fonction F vérifie la propriété $\mathscr{L}_j$ si:

$$\forall \mu \in \mathbf{N}^n, |\mu| < M_j; \quad \forall \gamma \in o(H_j): L^{\mu} F(\gamma u, \gamma u_0) = 0.$$

Par construction, F vérifie $\mathscr{L}_0$, et nous allons montrer par récurrence que $\mathscr{L}_j$ est satisfaite pour tout entier $j \leq J = 8(n+1)^2$. Nous admettons $\mathscr{L}_{j-1}$. Si F ne vérifie pas $\mathscr{L}_j$, il existe un élément g de $o(H_j)$ et un n-uple m, que nous convenons de choisir de longueur minimale, tel que $|m| < M_j$ et:

$$\xi = L^m F(gu, gu_0) \neq 0.$$

On tire du lemme 7 la minoration:

$$|\xi| > \exp(-C_7 L H_j^2 \operatorname{Log} U).$$

Dans ces conditions, considérons la fonction:

$$f(z) = [D^m(\Theta F)](zu),$$

où $\Theta(z) = z_1^{2L} \dots z_n^{2L}$. L'égalité

$$f(g) - \Theta(gu)D^m F(gu) = \sum_{\mu<m} \binom{m}{\mu} [D^\mu F D^{m-\mu}\Theta](gu)$$

entraîne, d'après la minimalité de m, et le lemme 9:

$$|f(g) - \Theta(gu)\xi| \leq \exp(-\Omega).$$

En vertu de la relation: $C_7 L H_j^2 \operatorname{Log} U < \Omega$, et du lemme 3, on a alors:

$$|f(g)| = |\Theta(gu)||\xi| \geq \exp(-C_8 L H^2 M^{2j\delta} \operatorname{Log} U).$$

D'autre part, les premières dérivées de f prennent des valeurs petites aux points de $o(H_{j-1})$. De façon précise:

$$\forall s < M_j, \forall \gamma \in o(H_{j-1}), |d^s f(\gamma)| < \exp(-\Omega).$$

Ceci découle en effet de la propriété $\mathscr{L}_{j-1}$, jointe à la relation:

$$\{|\mu| \leq |m| < M/2^j; |\kappa| \leq |\sigma| < M/2^j\} \Rightarrow |\mu + \kappa| < M/2^{j-1},$$

et au lemme 9 (on reprendra l'expression de $d^s f(\gamma)$ donnée à la première partie).

Mais le rayon de convergence $R(f)$ de f est minoré par $p^{1/C_9 p}$ d'après le §1.1 (exemple), et, pour $r < R(f)$, on a: $|f|_0(r) \leq 1$. Une estimation de la distance minimale des points de $o(H_{j-1})$ est fournie par le lemme 3, et on déduit du lemme 10 que:

$$|f(g)| \leq \sup\{(p^{-C_{10} H_{j-1}^2 M_j / C_9 p}, H_j^{C_{11} H_{j-1}^2 M_j} \exp(-\Omega)\}$$

soit (puisque, pour $j \leq J : \Omega > H^{4(n+1)+7} > M H^2 M^{2j\delta} \operatorname{Log} H$)

$$|f(g)| \leq \exp(-C_{13} H_{j-1}^2 M_j / p).$$

En définitive, on a obtenu:

$$C_7 L H^2 M^{2j\delta} \operatorname{Log} U > -\operatorname{Log}|f(g)| > C_{13} M H^2 M^{2(j-1)\delta} \operatorname{Log} p/(2^j p)$$

d'où:

$$C_{14} p \operatorname{Log} U > H^{1/[2(n+1)]}.$$

C'est la contradiction recherchée. La proposition $\mathscr{L}_j$ est ainsi vérifiée pour tout entier $j \leq 8(n+1)^2$.

TROISIÈME PAS: Soit q le plus petit nombre premier $> L^{1/2}$ (en particulier, $q \neq p$ et $q \leq 2L^{1/2}$). Nous allons montrer que $\eta = L^{\circ}F(q^{-1}\boldsymbol{u})$ est nul. La proposition 3 en résultera.

Supposons $\eta \neq 0$. On tire alors du lemme 8:

$$|\eta| \geq \exp(-C_{15}q^{2(n+1)}(MH \operatorname{Log} U + L(\operatorname{Log} q + \operatorname{Log} U))$$
$$\geq \exp(-C_{16}L^{n+1}MH \operatorname{Log} U).$$

Soit $f_1(z)$ la fonction $\Theta F(z\boldsymbol{u})$. Par un raisonnement similaire à celui du deuxième pas, on montre que:

$$|f_1(q^{-1})| \geq \exp(-C_{16}L^{n+1}MH \operatorname{Log} U),$$

tandis qu'en vertu de la propriété $\mathscr{L}_J$:

$$|f_1(q^{-1})| \leq \exp(-C_{17}M_JH^2H^{2J\delta}/p) \leq \exp(-C_{18}MH^2M^{n+1}/p).$$

Ces estimations sont incompatibles (elles entraînent en effet l'inégalité $p \operatorname{Log} U > H^2$) et cette dernière contradiction conclut la démonstration du théorème 2.

III APPLICATIONS

§3.1 Rappels sur les hauteurs

Le groupe des points rationnels d'une courbe elliptique E est muni d'une fonction hauteur, plus maniable que la fonction taille introduite au §2.1. Les propriétés de la hauteur sont bien connues, et nous nous bornons ici à rappeler celles qui seront utilisées au cours de la démonstration du résultat principal de cette troisième partie (théorème 3). Nous précisons tout d'abord la définition de la hauteur (multiplicative) d'un élément x du corps de nombres K.

Soient M l'ensemble des places de K, M_∞ (resp. M_0) l'ensemble ses places archimédiennes (resp. ultramétriques), N le degré de K sur $\mathbf{Q}$. Nous notons $|$ la relation de divisibilité dans l'anneau $\mathcal{O}$ des entiers de K. Si p est un nombre premier, et $\mathfrak{p}$ un idéal premier de $\mathcal{O}$ divisant

p, le degré $N_\mathfrak{p}$ du corps $K_\mathfrak{p}$ sur le corps $\mathbf{Q}_p$ des nombres p-adiques ordinaires est égal à $e_\mathfrak{p} f_\mathfrak{p}$, où $e_\mathfrak{p}$ désigne l'indice de ramification de p en $\mathfrak{p}$, et $f_\mathfrak{p}$ le degré du corps résiduel $\bar{K}_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$ sur le corps à p éléments $\boldsymbol{F}_p$. La norme $q_\mathfrak{p}$ de $\mathfrak{p}$ est alors égale à $p^{f_\mathfrak{p}}$. Enfin, le symbole $|\ |_\infty$ (resp. $|\ |_p$) représente la valeur absolue habituelle de $\mathbf{C}$ (resp. $\mathbf{Q}_p$).

A tout élément v de M, on associe une valeur absolue normalisée $\|\ \|_v$ compatible avec la formule du produit sur K (voir par example [1], théorème 1.8.4). Ainsi:

– si $v \in M_\infty$ est une place réelle: $\|x\|_v = |x|_\infty$

– si $v \in M_\infty$ est une place complexe: $\|x\|_v = |x|_\infty^2$.

– si $v \in M_0$ correspond à l'idéal premier $\mathfrak{p}$ de $\mathcal{O}$ (par abus de langage, on confond alors v et $\mathfrak{p}$):

$$\|x\|_v = \|x\|_\mathfrak{p} = |x|_\mathfrak{p}^{N_\mathfrak{p}}$$

où $|\ |_\mathfrak{p}$ désigne la valeur absolue introduite au §1.1 (c'est celle qui prolonge la valeur absolue $|\ |_p$ de $\mathbf{Q}_p$).

Dans ces conditions, le hauteur $H(x)$ d'un élément x de K est définie par l'expression:

$$H(x) = \prod_{v \in M} \sup(1, \|x\|_v).$$

LEMME 11: *Soient x un élément du K, et $A(x)$ le plus petit dénominateur commun des coefficients de polynôme caractéristique de x relatif à $K/\mathbf{Q}$.*

(i) *Pour tout nombre premier p, on a*:

$$|A(x)|_p^{-1} = \prod_{\mathfrak{p} \in M_0, \mathfrak{p}|p} \sup(1, \|x\|_\mathfrak{p}).$$

(ii) *Par conséquent*:

$$H(x) = A(x) \prod_{v \in M_\infty} \sup(1, \|x\|_v).$$

DÉMONSTRATION: (i) Les expressions obtenues en élevant chacun des termes de l'égalité (i) à la puissance $[K: \mathbf{Q}(x)]^{-1}$ sont invariantes par extension du corps K. Il suffit donc de démontrer cette égalité quand $K = \mathbf{Q}(x)$. Dans ces conditions, soient $\Delta = \Delta_1 \ldots \Delta_r$ la décomposition du polynôme caractéristique de x en polynômes unitaires irréductibles sur $\mathbf{Q}_p$, et $p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ la décomposition correspondante de l'idéal $p\mathcal{O}$.

On a, avec les notations du §1.1:

$$|\Delta|_0(1) = |A(x)|_p^{-1}.$$

Par ailleurs, on déduit de la définition des polynômes Δ_i:

$$|\Delta_i|_0(1) = 1 \quad \text{si } x \text{ est un entier } \mathfrak{p}_i\text{-adique},$$
$$|\Delta_i|_0(1) = |N_{K_{\mathfrak{p}_i}/\mathbf{Q}_p} x|_p = \|x\|_{\mathfrak{p}_i} \quad \text{dans le cas contraire.}$$

Le lemme de Gauss permet alors de conclure.

(ii) Pour déduire (ii) de (i), il suffit d'appliquer la formule du produit sur $\mathbf{Q}$.

Notons que (ii) permet de retrouver certaines relations classiques liant les fonctions hauteur et taille. En effet, pour tout élément x de K, den x divise $A(x)$, lequel divise $(\text{den } x)^N$. En conséquence:

$$t(x) \leq H(x) \leq (t(x))^{2N}.$$

Dans le même ordre d'idées, l'égalité (i) entraîne que tout facteur premier p de den x divise l'entier $\Pi_{\mathfrak{p}|p} \sup(1, \|x\|_{\mathfrak{p}})$.

Nous considérons désormais le modèle affine:

$$y^2 = x^3 - ax - b$$

de E. Les définitions qui suivent se prolongent sans difficulté à l'élément neutre de E. Suivant [5], §21, on appelle hauteur $H(Q)$ d'un élément Q de $E(K)$ la hauteur de son abscisse $x(Q)$. En particulier, pour tout nombre réel $H_0 > 0$, il n'y a qu'un nombre fini de points de $E(K)$ de hauteur $< H_0$.

La propriété fondamentale de la hauteur sur E peut être formulée de la façon suivante. Nous notons $E_t(K)$ le sous-groupe des points de torsion de $E(K)$.

LEMME 12 (Néron–Tate): *Il existe une fonction* $h_0: E(K) \to \mathbf{R}$ *bornée telle que la fonction* $\hat{h} = \text{Log } H + h_0$ *induise sur* $E(K)/E_t(K)$ *une forme quadratique définie positive.*

DÉMONSTRATION: Voir [5], formule 21.23, [8], théorème 1.

Nous sommes maintenant en mesure de donner la démonstration de la proposition 4 promise au §2.1. On considère n éléments $Q_1, \ldots, Q_n$ de $E(K)$ linéairement indépendants sur End E, de taille $< U$. Pour

tout nombre premier l, on note E_l le groupe des points de l-torsion de E, et k_l le corps engendré par leurs coordonnées sur K. Pour $i = 1, \ldots, n$, soient Q_i/l un point de l-division de Q_i, et $Q_i(l)$ l'image de Q_i dans $E(K)/lE(K)$. On note K_l l'extension abélienne de k_l obtenue en adjoignant à k_l les coordonnées des points $Q_1/l, \ldots, Q_n/l$, et H_l (resp. G_l) le groupe de Galois de K_l sur k_l (resp. de k_l sur K). Enfin, on définit, pour $i = 1, \ldots, n$, un homomorphisme $\varphi_i : H_l \to E_l$ en posant, pour tout élément σ de H_l:

$$\varphi_i(\sigma) = \sigma(Q_i/l) - Q_i/l.$$

(On vérifie aisément que φ_i est indépendant du choix de Q_i/l.) Enfin, on considère l'application $\Phi = \varphi_1 \times \cdots \times \varphi_n : H_l \to E_l^n$.

Le groupe G_l (resp. H_l) s'identifie à un sous-groupe de Aut E_l (resp. de E_l^n), et l'action de G_l sur H_l (par conjugaison) correspond à l'action de Aut E_l sur $\Phi(H_l)$.

Dans ces conditions, le résultat principal de [12] énonce que H_l est isomorphe à E_l^n (et donc, d'ordre l^{2n}) dès que les hypothèses suivantes sont simultanément satisfaites ([12], corollaire de §1]:

(i) l ne se remifie pas dans $\mathcal{O} \cap k = O$.

(ii) l est premier à l'indice $[O : o]$. Alors $o/lo = \text{End } A/l \text{ End } A \simeq O/lO$, et Aut $E_l \simeq (O/lO)^*$.

(iii) $G_l \simeq (O/lO)^*$. Alors $\boldsymbol{F}_l[G_l] \simeq O/lO$.

(iv) les homomorphismes $\varphi_1, \ldots, \varphi_n$ sont linéairement indépendants sur O/lO. D'après [12], corollaire du §3, cela revient à dire que les points $Q_1(l), \ldots, Q_n(l)$ sont linéairement indépendants sur o/lo.

Des raisons élémentaires, d'une part, et la théorie locale des points d'ordre l, d'autre part, assurent l'existence d'une entier $l_1 = l_1(a, b, \tau) > 0$ tel que les conditions (i), (ii) et (iii) soient satisfaites par tout nombre premier $l > l_1$. Supposons que (iv) ne soit pas vérifiée. Il existe alors des éléments $\gamma_1, \ldots, \gamma_n$ de o, dont l'un au moins n'est pas dans lo et un point Q de $E(K)$ tels que:

$$lQ = \gamma_1 Q_1 + \cdots + \gamma_n Q_n.$$

Le principe des tiroirs de Dirichlet permet d'obtenir des approximations simultanées des quotients par l des $2n$ coordonnées des nombres γ_i sur la base $\{1, \tau\}$. De façon précise, il existe un entier q compris entre 1 et $l-1$, et n éléments $g_1, \ldots, g_n$ de o tels que les nombres $\gamma_i' = q\gamma_i - lg_i$ soient des éléments de $o(l^{1-1/(2n)}) \cup \{0\}$. Alors le point

$$P = \gamma_1' Q_1 + \cdots + \gamma_n' Q_n$$

s'écrit sous la forme lQ', où Q' est un élément de $E(K)$. De plus, les hypothèses faites sur $\gamma_1, \ldots, \gamma_n$ entraînent que les nombres γ_i' ne sont pas tous nuls, et, puisque les points Q_i sont linéairement indépendants sur End A, le point Q' ne peut être d'ordre fini. Le lemme 12 permet alors d'estimer la hauteur de P. On a d'une part

$$\hat{h}(P) = \hat{h}(\gamma_1' Q_1 + \cdots + \gamma_n' Q_n) \leq (l^{1-1/(2n)})^2 n^2 \sup_{i,j} ((\hat{h}(Q_i)\hat{h}(Q_j)^{1/2})$$
$$\leq C_1' l^{2-1/n} \operatorname{Log} U.$$

D'autre part, il résulte de la remarque précédant l'énoncé du lemme 12 que la fonction $\hat{h}$ est bornée inférieurement sur $E(K)/E_t(K)$ par un nombre réel $C_2' > 0$ effectivement calculable en fonction de a, b et K. En conséquence:

$$\hat{h}(P) = \hat{h}(lQ') \geq C_2' l^2.$$

La comparaison de ces inégalités fournit la condition: $l < C_3'(\operatorname{Log} U)^n$. Ainsi, dès que $l > \sup(l_1, C_3'(\operatorname{Log} U)^n)$, le groupe H_l est isomorphe à E_l^n, et la proposition 4 est démontrée.

§3.2 Facteurs premiers des dénominateurs des points rationnels de E

Soient E une courbe elliptique définie sur un corps de nombres K, S un ensemble fini de places de K contenant M_∞, et $E_S(K)$ l'ensemble des points de $E(K)$ dont les coordonnées (sur le modèle $y^2 = x^3 - ax - b$) sont entières hors de S. Autrement dit:

$$E_S(K) = \{Q \in E(K) / \forall \mathfrak{p} \notin S, \|x(Q)\|_{\mathfrak{p}} \leq 1\}.$$

Le théorème de Siegel et Mahler [10], dont la démonstration repose sur le théorème de Thue–Siegel–Roth, affirme que l'ensemble $E_S(K)$ est fini. Nous conservons dans cette dernière section l'hypothèse que E admet une multiplication complexe (que nous supposons toujours définie sur K), et nous nous proposons de préciser alors l'énoncé de Mahler, à partir des résultats du §2.1 et du chapitre 6 de [11]. Ainsi qu'on l'a rappelé dans l'introduction, le résultat de Masser permet de traiter le cas où S est réduit à M_∞ (théorème de Siegel).

Nous ferons ici appel au théorème de Mordell–Weil, d'après lequel le groupe $E(K)$ est de type fini. Soit r son rang (sur $\mathbf{Z}$). Si Q désigne

un élément de $E(K)$, nous notons $D(Q)$ le dénominateur de son abscisse $x(Q)$ et $P(Q) = P(D(Q))$ le plus grand facteur premier de $D(Q)$. Nous rappelons que N désigne le degré de K sur $\mathbf{Q}$. Alors:

THÉORÈME 3: *Il existe un nombre réel $\kappa > 0$ ne dépendent que de a, b, et K tel que, pour tout élément Q de $E(K)$, on ait*:

$$P(Q) > \kappa(\operatorname{Log} H(Q))^{1/(13Nr^2)}.$$

La démonstration de ce théorème sera donnée au §3.3. Nous en discutons maintenant l'énoncé.

REMARQUE 1: Le théorème 3 améliore l'inégalité suivante, qu'a récemment établie Kotov [7] par une méthode différente:

$$P(Q) > \kappa'(\operatorname{Log}\operatorname{Log} H(Q) \cdot \operatorname{Log}\operatorname{Log}\operatorname{Log} H(Q))^{1/2}.$$

Mais le résultat de Kotov vaut même si E n'admet pas de multiplication complexe. D'autre part, il est entièrement effectif, alors que la preuve donnée ci-dessous repose sur la connaissance d'une base du groupe $E(K)$. C'est d'ailleurs là que réside le seul point ineffectif de cette démonstration.

REMARQUE 2: Considérons l'ensemble $E_S(K)$ défini plus haut; soit P_S le plus grand nombre premier divisible par l'un au moins des idéaux de S, et Q un élément de $E_S(K)$. La démonstration du lemme 11(i) montre que $P(Q)$ divise $\Pi_{\mathfrak{p}|P(Q)} \sup(1, \|x(Q)\|_{\mathfrak{p}})$. En conséquence, $P(Q) \leq P_S$ et on déduit du théorème 3 que les points de $E_S(K)$ sont de hauteur bornée. On retrouve ainsi le fait que cet ensemble est fini. Plus précisément le lemme 12 (voir [8], corollaire 3) entraîne que $E_S(K)$ a au plus $\kappa'' P_S^{7Nr^3}$ éléments, pour une constante $\kappa'' = \kappa''(a, b, K)$.

REMARQUE 3: Lorsque E est définie sur $\mathbf{Q}$, et qu'on s'intéresse au groupe $E(\mathbf{Q})$ lui-même, on obtient, pour tout élément Q de $E(\mathbf{Q})$:

$$P(Q) > \kappa_0(\operatorname{Log} H(Q))^{1/50r_0^2}$$

où r_0 désigne le rang de $E(\mathbf{Q})$ (sur $\mathbf{Z}$), et $\kappa_0 = \kappa_0(a, b)$. Pour établir cette formule, on observera que des points de $E(\mathbf{Q})$ linéairement indépendants sur, $\mathbf{Z}$ le sont encore sur $o = \operatorname{End} E$. On peut alors reprendre la démonstration du §3.3, en omettant le premier pas.

REMARQUE 4: Nous nous sommes jusqu'à présent limités aux équations de Weierstrass de E. Soit, de façon générale, $E_F = \{F(\xi, \eta) = 0\}$ un modèle de E, défini sur K. On peut déduire du théorème 3 un énoncé similaire, où ξ joue maintenant le rôle de la fonction x. En effet, le théorème de Riemann–Roch permet d'associer à tout point à l'infini Q_0 de E_F un modèle de Weierstrass $E_G = \{G(x, y) = 0\}$ de E, défini sur le corps de nombres $L = K(Q_0)$ et admettant Q_0 pour élément neutre. Dans ces conditions, tout point Q de $E_F(K)$ appartient à $E_G(L)$. De plus, le raisonnement de [2], 4, §4 (voir également [7], [8], et [2], p. 45) montre qu'il existe un entier rationnel c, indépendant de Q, tel que chaque facteur premier du dénominateur de $cx(Q)$ divise $\operatorname{den}\xi(Q)$. Notant enfin que les fonctions hauteurs associées à x et ξ sont (multiplicativement) équivalentes, on conclut à l'inégalité:

$$P(\operatorname{den}\xi(Q)) > \kappa_0'(\operatorname{Log} H(\xi(Q)))^{\kappa_0''},$$

où κ_0' et κ_0'' désignent des nombres réels >0 ne dépendant que de K et des coefficients du polynôme F.

REMARQUE 5: Le théorème 3 exprime que le plus grand facteur premier $P(Q)$ de $\operatorname{den} x(Q)$ croît avec la hauteur de Q. Ainsi que l'a souligné Coates, il serait très intérressant d'établir un résultat du même type pour le nombre $\omega(Q)$ de facteurs premiers de $\operatorname{den} x(Q)$.[3]

§3.3 Démonstration du théorème 3

Elle consiste essentiellement en une réduction à la situation considérée au théorème 2. Nous rappelons que K contient le corps de multiplication complexe $k = \mathbb{Q}(\tau)$. Ainsi que le montre un argument classique, le rang r de $E(K)$ est donc un entier $2n$ pair.

Soient $Q_1, \ldots, Q_r$ des représentants d'un système de générateurs du groupe $E(K)/E_t(K)$. Par $\kappa_1, \ldots, \kappa_{13}$, on signifie des nombres réels >0 effectivement calculables en fonction de $a, b, Q_1, \ldots, Q_r$ et K.

Tout élément Q de $E(K)$ s'écrit sous la forme:

$$Q = m_1 Q_1 + \cdots + m_r Q_r + Q_t,$$

[3] G.V. Čudnovskij a obtenu quelques résultats dans cette direction (voir les C.r. du Colloque de Théorie des Nombres, Debrecen, 1974 [North-Holland]).

où Q_t désigne un point de $E_t(K)$, et $m_1, \ldots, m_r$ des entiers rationnels. Si h désigne le maximum de leur norme, et si Q est d'ordre infini, on a en vertu de lemme 12:

$$H(Q) > \kappa_1^{h^2}.$$

Nous supposerons désormais que Q n'est pas un point de torsion.

PREMIER PAS: Quitte à permuter les indices, on peut supposer que les points $Q_1, \ldots, Q_n$ sont linéairement indépendants sur End A. Des relations $\mathbf{Z}$-linéaires lient alors chacun des points $Q_{n+1}, \ldots, Q_r$ au système $Q_1, \tau Q_1, \ldots, Q_n, \tau Q_n$. (En outre, le raisonnement suivi à la fin du §3.1 permet d'obtenir une majoration effective de leurs coefficients – cf. [9]). Dans ces conditions, notons Γ le groupe engendré par $Q_1, \tau Q_1, \ldots, Q_n, \tau Q_n$, et μ l'indice de Γ dans $E(K)$. Le point μQ est un élément non nul de Γ; il s'écrit:

$$\mu Q = \gamma_1 Q_1 + \cdots + \gamma_n Q_n,$$

où les nombres $\gamma_1, \ldots, \gamma_n$ désignent des éléments de $o(\kappa_2 h) \cup \{0\}$ non tous nuls.

DEUXIÈME PAS (places finies): Soient $\mathfrak{p}$ un idéal premier de $\mathcal{O}$ et p le nombre premier qu'il devise, de sorte que: $q_\mathfrak{p} = p^{f_\mathfrak{p}}$. Le théorème 2 concerne le groupe $\mathcal{E}_\mathfrak{p}$ qui, rappelons – le, est d'indice fini dans $E(K_\mathfrak{p})$. De façon précise:

LEMME 13: *Il existe un nombre réel $\kappa_3 > 0$ effectivement calculable en fonction de a, b, et K, tel que l'exposant $\nu_\mathfrak{p}$ du groupe $E(K_\mathfrak{p})/\mathcal{E}_\mathfrak{p}$ soit majoré par $\kappa_3 q_\mathfrak{p}$.*

DÉMONSTRATION: (La discussion suivante vaut si l'équation de Weierstrass de E considérée dans cet article est minimale en $\mathfrak{p}$, au sens de [13], §6. On passe au cas général au moyen des formules (7) de [13].) Soient $\bar{E}_{ns}$ la partie régulière de la courbe de $\mathbf{P}_2(\bar{K}_\mathfrak{p})$ obtenue par réduction de E *modulo* $\mathfrak{p}$ et $E_0(K_\mathfrak{p})$ (resp. $E_1(K_\mathfrak{p})$) l'ensemble des points de $E(K_\mathfrak{p})$ dont la réduction *modulo* $\mathfrak{p}$ est un point de $\bar{E}_{ns}(\bar{K}_\mathfrak{p})$ (resp. le point à l'infini de $\bar{E}_{ns}(\bar{K}_\mathfrak{p})$).

D'après l'additif au théorème 3 de [13], l'ensemble $E_0(K_\mathfrak{p})$ est un sous-groupe de $E(K_\mathfrak{p})$ d'indice fini majoré soit par 4, soit par la valuation $\mathfrak{p}$-adique de $(4a^3 - 27b^2)/(4.1728a^3)$. Par ailleurs, $\bar{E}_{ns}(\bar{K}_\mathfrak{p})$ est un groupe, et la relation $\bar{E}_{ns}(\bar{K}_\mathfrak{p}) = E_0(K_\mathfrak{p})/E_1(K_\mathfrak{p})$, que fournit le

théorème 3 de [13], entraîne que l'indice de $E_1(K_\mathfrak{p})$ dans $E_0(K_\mathfrak{p})$ est majoré par:

$$2 \operatorname{card} \bar{K}_\mathfrak{p} = 2q_\mathfrak{p}.$$

Enfin,[4] l'application $\chi: Q \to -x(Q)/y(Q)$ établit un isomorphisme analytique de $E_1(K_\mathfrak{p})$ sur $\mathfrak{p}$. Or, si u désigne un élément de $\mathscr{C}_\mathfrak{p}$, la relation $\chi(\epsilon_\mathfrak{p}(u)) = \varphi(u)/\varphi'(u)$ montre que:

$$\chi(\epsilon_\mathfrak{p}(u))/u = 1 \pmod{\mathfrak{p}},$$

et permet de définir un automorphisme analytique de $\mathscr{C}_\mathfrak{p}$. La propriété d'isomorphisme de l'exponentielle $\mathfrak{p}$-adique entraîne alors que χ applique $\mathscr{E}_\mathfrak{p}$ sur $\mathscr{C}_\mathfrak{p}$. Mais dès que $p > 2$ ne se ramifie pas dans K (ou dès que $p \geq N$), le disque $\mathscr{C}_\mathfrak{p} = \{z \in K_\mathfrak{p}, \|z\|_\mathfrak{p} < q_\mathfrak{p}^{-e_\mathfrak{p}/(p-1)}\}$ coïncide avec $\mathfrak{p}$, et $\mathscr{E}_\mathfrak{p} = E_1(K_\mathfrak{p})$. Ainsi:

$$|E(K_\mathfrak{p})/\mathscr{E}_\mathfrak{p}| < \kappa_3 q_\mathfrak{p}.$$

(Si $p = 2$, ou si p se ramifie dans K, la considération du polygone de Newton de la série $[p](\chi(Q)) = \chi(pQ)$ associée à la loi de multiplication formelle par p permet de majorer, de façon effective, l'ordre des éléments de $E_1(K_\mathfrak{p})/\mathscr{E}_\mathfrak{p}$).

En regroupant ces différents résultats, on obtient la conclusion recherchée.

Nous sommes maintenant en mesure d'appliquer le théorème 2. Notons tout d'abord que le point $\mu\nu_\mathfrak{p}Q$ appartient à $\mathscr{E}_\mathfrak{p}$. On vérifie alors aisément que:

$$|x(\mu\nu_\mathfrak{p}Q)|_\mathfrak{p} \geq |x(Q)|_\mathfrak{p},$$

et l'on a: $|x(\mu\nu_\mathfrak{p}(Q)|_\mathfrak{p} = |\epsilon_\mathfrak{p}^{-1}(\mu\nu_\mathfrak{p}Q)|_\mathfrak{p}^{-2}$. Par ailleurs, les points $\nu_\mathfrak{p}Q_1, \ldots, \nu_\mathfrak{p}Q_N$ sont des éléments de $\mathscr{E}_\mathfrak{p}$ linéairement indépendants sur End E. Leurs hauteurs, et donc leurs tailles (lemme 11), sont, en vertu du lemme 12, majorées par: $\kappa_4^{\nu_\mathfrak{p}^2}$. En conséquence, le théorème 2 entraîne:

$$\begin{aligned} &|\gamma_1\epsilon_\mathfrak{p}^{-1}(\nu_\mathfrak{p}Q_1) + \cdots + \gamma_n\epsilon_\mathfrak{p}^{-1}(\nu_\mathfrak{p}Q_n)|_\mathfrak{p} \\ &> \exp(-\kappa_5(\operatorname{Log} h)^{8n}(p\nu_\mathfrak{p}^2 \operatorname{Log} \kappa_4)^{16n^2}). \end{aligned}$$

[4] Pour cette dernière réduction, voir également le livre de Fröhlich "Formal Groups", p. 109, théorème 3.

Ainsi:

$$\|x(Q)\|_{\mathfrak{p}} \leq \exp(\kappa_6(\operatorname{Log} h)^{8n} p^{16n^2(2f_{\mathfrak{p}}+1)}).$$

Mais, dès que $\mathfrak{p}$ ne divise pas $\operatorname{den} x(Q)$, le nombre $x(Q)$ est un élément de $\mathcal{O}_{\mathfrak{p}}$. On a donc, en reprenant les notations du lemme 11:

$$A(x(Q)) \leq \exp\left(\kappa_7(\operatorname{Log} h)^{8n} \sum_{p|\operatorname{den} x(Q)} p^{16n^2(2N+1)}\right),$$

soit, $P(Q)$ majorant le nombre de facteurs premiers de $\operatorname{den} x(Q)$:

$$A(x(Q)) \leq \exp(\kappa_8(\operatorname{Log}\operatorname{Log} H(Q))^{8n} P(Q)^{49Nn^2}).$$

TROISIÈME PAS (places infinies): Il nous reste à obtenir une majoration du facteur infini de la hauteur. Elle est fournie par le théorème 5 de [11] (ou, bien entendu, par l'amélioration donnée dans [6]). Nous l'énonçons sous la forme suivante:

PROPOSITION 5 (Masser): *Il existe un nombre réel* $\kappa_9 = \kappa_9(a, b, K) > 0$ *tel que, pour tout élément* Q *de* $E(K)$, *on ait*:

$$\operatorname{Log} D(Q) > \kappa_9 \operatorname{Log} H(Q).$$

DÉMONSTRATION: Nous considérons un plongement σ de K dans $\mathbf{C}$, et nous reprenons les notations utilisées au cours de la démonstration du lemme 8. Soient $u_1^{\sigma}, \ldots, u_n^{\sigma}$ des nombres complexes tels que:

$$\mathcal{P}^{\sigma}(u_i^{\sigma}) = \sigma(x(Q_i)).$$

En vertu du théorème 5 de [11], on a, pour tout élément ω de Λ^{σ}:

$$|\gamma_1 u_1^{\sigma} + \cdots + \gamma_n u_n^{\sigma} - \omega|_{\infty} > \exp(-\kappa_{10} h^{1/2}),$$

d'où:

$$|\sigma(x(Q))|_{\infty} \leq C_2 \mu^2 |\sigma(x(\mu Q))|_{\infty} \leq \exp(\kappa_{11}[\operatorname{Log} H(Q)]^{1/2}).$$

On en déduit:

$$\prod_{v \in M_{\infty}} \sup(1, \|x(Q)\|_v) \leq \exp(\kappa_{12}[\operatorname{Log} H(Q)]^{1/2}).$$

La proposition 5 résulte alors du lemme 11.

En définitive, les différentes relations établies ci-dessus entraînent:

$$H(Q) = A(x(Q)) \prod_{v \in M_\infty} \sup(1, \|x(Q)\|_v)$$
$$\leq \exp(\kappa_8 (\text{Log Log } H(Q))^{8n} P(Q)^{49Nn^2} + \kappa_{12} (\text{Log } H((Q))^{1/2}).$$

soit:

$$P(Q) \geq \kappa_{13} [\text{Log } H(Q)]^{1/(50Nn^2)} \geq \kappa_{13} [\text{Log } H(Q)]^{1/(13Nr^2)},$$

et le théorème 3 est démontré.

BIBLIOGRAPHIE

[1] Y. Amice: *Les nombres p-adiques.* P.U.F., collection SUP, Paris, (1975).

[2] A. Baker: *Transcendental number theory.* Cambridge University Press, Cambridge (1975).

[3] D. Bertrand: Lemmes de Schwarz et lemmes d'approximations dans les domaines ultramétriques. *C.R. Conf.* Luminy, Juin 1976. Groupe d'étude d'analyse ultramétrique Amice-Robba, Secr. Math. Paris (1976), n° J8.

[4] D. Bertrand: Sous groupes à un paramètre p-adique de variétés de groupes. *Inventiones Math.* 40 (1977) 171–193.

[5] J.W.S. Cassels: Diophantine equations with special reference to elliptic curves (survey article). *J. London Math. Soc. 41* (1966) 193–291.

[6] J. Coates et S. Lang: Diophantine approximations on abelian varieties with complex multiplications. *Inventiones Math. 34* (1976) 129–133.

[7] S. Kotov: Die arithmetische Struktur der rationalen Punkte auf Kurven vom Geschlecht Eins. *Acta Arith.* (à paraître).

[8] S. Lang: Diophantine approximations on toruses. *Amer. J. Math. 86* (1964) 521–533.

[9] S. Lang: *Elliptic curves; diophantine analysis.* (Livre à paraître).

[10] K. Mahler: Über die rationalen Punkte auf Kurven vom Geschlecht Eins. *J. r. ang. Math., 170* (1934) 168–178.

[11] D.W. Masser: *Elliptic functions and transcendence.* Lecture Notes in Math. 437, Springer, Berlin-Heidelberg-New York (1975).

[12] K. Ribet: Dividing rational points on abelian varieties of C.M. type. *Compositio Math., 33* (1976) 69–74.

[13] J. Tate: The arithmetic of elliptic curves. *Inventiones Math., 23* (1974) 179–206.

[14] A. Weil: Sur les fonctions elliptiques $\mathfrak{p}$-adiques, *Note aux C.R. Acad. Sc. Paris, 203* (1936) 22–24.

(Oblatum 21-XII-1976)

Centre de Mathématiques de l'Ecole Polytechnique
Plateau de Palaiseau
91128 Palaiseau Cedex (France)