Astérisque

D. BERTRAND

Hauteurs et isogénies

Astérisque, tome 183 (1990), p. 107-125

<http://www.numdam.org/item?id=AST_1990__183__107_0>

Société Mathématique de France
Astérisque 183 (1990)

HAUTEURS ET ISOGÉNIES

par D. BERTRAND

Théorème (Masser-Wüstholz) : *soit* d *un entier* ≥ 1 . *Il existe un nombre réel* c(d) *effectivement calculable en fonction de* d *et une constante universelle effective* C *vérifiant la propriété suivante . Soient* E *une courbe elliptique définie sur un corps de nombres* k *de degré* d *sur* $\mathbf{Q}$, *et* γ *un majorant* ≥ 1 *des hauteurs logarithmiques des coefficients d'une équation de Weierstrass de* E *sur* k . *Pour toute courbe elliptique* E' *définie sur* k *et* k-*isogène à* E , *il existe une* k-*isogénie de* E' *vers* E *de degré majoré par* $c(d)\,\gamma^{C}$.

On trouvera une démonstration de cet énoncé dans [M-W2]. L'esquisse qu'en donne [Ma4] fournit 4 pour valeur de la constante C .

Nous donnons ici la preuve d'une version affaiblie de ce théorème: l'expression c(d) est remplacée par une fonction c(k) du corps k , effectivement calculable en termes de d et de la valeur absolue δ du *discriminant* de k sur $\mathbf{Q}$. Notre démarche suit celle de [Ma4], mais paraît, par certains aspects, mieux adaptée à d'éventuelles généralisations. Et on verra en fait (appendice A) qu'au prix d'une perte significative sur C , le théorème ci-dessus découle de la démonstration de sa version affaiblie : en d'autres termes, les données δ et γ sont intimement liées.

La démonstration comporte trois parties : la première, de nature essentiellement algébrique, consiste à décrire l'isogénie ϕ qui lie *a priori* E' à E dans un modèle de Weierstrass de E' dépendant de façon logarithmique de son degré N ; la dernière met en jeu la méthode de Baker qui, sous la forme rénovée que lui donnent les lemmes de zéros, fournit alors (modulo une réduction standard expliquée dans la deuxième partie) une isogénie de E' vers E de degré majoré par un monôme en Log N . Si on a pris soin de choisir ϕ de degré minimal , N

est alors bien borné !

Le théorème fournit une version effective d'un classique théorème d'irréductibilité dû à Serre ([Se], IV, 2.1). Nous renvoyons à [Ma4] pour ses applications les plus marquantes, et à l'appendice C du présent texte pour son lien avec [Ra].

§1 Préparatifs

On reprend les hypothèses du théorème, et on considère une k-isogénie ϕ d'une courbe elliptique E'/k vers E , dont on note N le degré. On désigne par C_1, C_2, ... des nombres réels > O effectivement calculables en fonction de d et de δ . Enfin, toutes les hauteurs sont logarithmiques.

Proposition 1: *il existe deux* k-*formes différentielles de 1ère espèce* ω (resp. ω')*sur* E (resp. E') *vérifiant les propriétés suivantes:*
i) $g_2(E,\omega)$ *et* $g_3(E,\omega)$ *sont des éléments de* k *de hauteurs majorées par* $C_1\gamma$;
ii) $\phi^*\omega = \beta\omega'$, *où* β *est un élément de* k *de hauteur* $\leq C_2$ LogN ;
iii) $g_2(E',\omega')$ *et* $g_3(E',\omega')$ *sont des éléments de* k *de hauteurs majorées par* $\gamma' = C_3(\gamma + \text{LogN})$.

Corollaire : *même énoncé avec* $\beta = 1$ (remplacer ω' par $\beta\omega'$).

Démonstration : Soient **E** , **E'** les modèles de Néron de E , E' sur l'anneau *O* des entiers de k . Pour clarifier les idées, je décris tout d'abord la démonstration dans le cas où *O* est principal. Les *O*- modules ω_E (image réciproque de $\Omega^1_{E/O}$ par la section nulle) et $\omega'_{E'}$ sont alors libres. J'en fixe des générateurs ω , ω' : ils ne sont définis qu'aux unités de k près, et c'est sur elles qu'on va jouer.

i) Sans perte de généralité, on peut supposer que l'équation de Weierstrass de E donnée par l'énoncé du théorème a des coefficients entiers (chasser les dénominateurs, qui sont majorés par $\exp(C_4\,\gamma)$).

Son discriminant est alors un élément de O de norme $\leq \exp(C_5\,\gamma)$, et il en est de même de $\Delta(E,\omega)$, qui le divise, et est bien entier en vertu des propriétés d'intégralité de la forme modulaire Δ (cf. [Ka], §1, dont je rappelle d'ailleurs le principe plus loin). Il existe donc (Dirichlet) une unité ε de k telle que $\Delta(E, \omega/\varepsilon) = \varepsilon^{12}\,\Delta(E, \omega)$ soit de hauteur $\leq C_6\gamma$. La forme différentielle ω/ε (que nous convenons de rebaptiser ω) répond alors à la question.

ii) Les isogénies s'étendant aux modèles de Néron (voir [Ra]), $\phi^*\omega$ est une section de $\omega_{E'}$, et il existe un élément β de O tel que $\phi^*\omega = \beta\omega'$. Le même raisonnement, appliqué à l'isogénie duale ϕ' de ϕ, fournit un élément β' de O tel que $\phi'^*\omega = \beta'\omega$. Mais alors, $\beta'\beta\omega = (\phi\phi')^*\omega = N\omega$, et l'entier rationnel $\mathrm{Norm}_{k/\mathbb{Q}}\beta$ divise N^d. Il existe donc une unité ε' de k telle que $\beta\varepsilon'$ soit de hauteur majorée par $C_7 \mathrm{Log} N$, et la forme différentielle ω'/ε' (que nous rebaptiserons ω') vérifie ii).

iii) Montrons tout d'abord que $g_2(E', \omega')$ et $g_3(E', \omega')$ sont essentiellement des entiers de k. Il suffira alors, pour borner leurs hauteurs, de majorer leurs différentes valeurs absolues archimédiennes.

Si v est une place finie de k première à 6, g_2 et g_3, qui sont des formes modulaires entières sur O_v (cf. [Ka1, §1), prennent des valeurs dans O_v dès que ω' engendre $\omega_{E'}$ localement en v. Idem aux places divisant 6, à des dénominateurs universellement bornés près. Les dénominateurs de $g_2(E', \omega')$ et $g_3(E', \omega')$ divisent donc un entier $C_8(k)$.

Passons aux places archimédiennes de k, que nous allons traiter suivant les techniques modulaires de [Ma1], §3 et [Ma3]. Soit v l'une d'elles. Désignons, pour tout réseau Λ de $\mathbf{C}$, par $\varpi(\Lambda)$ le minimum des valeurs absolues de ses éléments non nuls. Comme toute forme modulaire pour $SL_2(\mathbf{Z})$, soit f, de poids $w(f)$, est par définition bornée sur le domaine fondamental usuel, la fonction de réseaux $|f(\Lambda)|\,\varpi(\Lambda)^{w(f)}$

est bornée supérieurement. Les réseaux de périodes Λ_v , Λ'_v de ω et de ω' qui correspondent à v vérifiant $\beta^{-1}\Lambda'_v \subseteq \Lambda_v$, donc en particulier $\varpi(\Lambda'_v) \geq |\beta|_v \varpi(\Lambda_v)$, on en déduit :

$$\sup\{|g_2(\Lambda'_v)|_v^{1/2} , |g_3(\Lambda'_v)|_v^{1/3}\} \leq c\ |\beta|_v^{-2}\ \varpi(\Lambda_v)^{-2} ,$$

où c est une constante universelle, d'où, grâce à la majoration de la hauteur de β fournie par i) :

$$\text{Log}\ \sup\{|g_2(E',\omega')|_v^{1/2} , |g_3(E',\omega')|_v^{1/3}\} \leq C_9(\text{LogN} - \text{Log}\ \varpi(\Lambda_v)) .$$

Il reste à minorer $\varpi(\Lambda_v)$ en fonction de γ . Pour cela, complétons l'un des éléments ω_1 de Λ_v qui donne $\varpi(\Lambda_v)$ en une base directe $\{\omega_1, \omega_2=\tau\omega_1\}$ de ce réseau, de sorte que (Hermite) $\text{Im}\tau$ est $\geq \sqrt{3}/2$. La connaissance des zéros des fonctions $E_4(\tau)$ et $E_6(\tau)$ dans ce domaine entraîne que l'expression

$$\sup\{|g_2(\Lambda_v)|^{1/2} , |g_3(\Lambda_v)|^{1/3}\}\ \varpi(\Lambda_v)^2$$

est universellement minorée, et on déduit de l'inégalité de la taille la minoration : $\text{Log}\ \varpi(\Lambda_v) \geq - C_{10}\gamma$. Предложение доказано (pour O principal).

Pour passer au cas général, il suffit de noter que tout O-module de rang 1 sans torsion admet un sous-O- module libre d'indice majoré par la racine carrée de la valeur absolue du discriminant de k . Grâce aux relations $g_K(E, \lambda\omega) = \lambda^{-2K} g_K(E,\omega)$, les arguments précédents s'adaptent alors aisément en autorisant aux entiers de k qui y apparaissent d'avoir des dénominateurs divisant ces indices.

Remarque: **(i)** La démonstration (à la fois plus simple et plus précise !) que donne [Ma4] du corollaire à la Proposition 1 repose sur la formule suivante. Si Λ' est un sous-groupe d'indice N d'un réseau Λ , le réseau $N\Lambda$ est inclus dans Λ' , et l'on a (d'après Eisenstein) :

$$g_K(\Lambda') = g_K(N\Lambda) + \varepsilon_K \sum_x \wp^{(2K-2)}(x, N\Lambda) ,$$

où x parcourt un système de représentants de $\Lambda'/N\Lambda$, $\wp$ désigne la fonction de Weierstrass usuelle et ε_K est une expression simple. Les

propriétés arithmétiques standard des points de torsion conduisent alors aux estimations souhaitées, avec des constantes C_1, C_2, C_3 *ne dépendant maintenant plus que de* d.

Je me place désormais sous les hypothèses du corollaire à la proposition 1. Dans la démonstration qui suit, on va privilégier une place archimédienne de k (choisie arbitrairement). Cela revient à considérer une fois pour toutes k comme un sous-corps de $\mathbf{C}$, et, en particulier, E et E' comme des courbes elliptiques complexes. Nous désignerons par Λ, Λ' les réseaux de périodes de ω, ω', par Ω_1, Ω' des éléments non nuls de Λ, Λ' de valeurs absolues minimales, et par Ω_2 un élément de Λ tel que $\tau = \Omega_2/\Omega_1$ appartienne au domaine fondamental que l'on sait et représente la classe d'isomorphisme de $E/\mathbf{C}$. Dans ces conditions, on peut énoncer, avec des constantes C_{11},... ne dépendant ici que de d :

Proposition 2 : (voir [Ma3]) *On a :* $|\mathrm{Log}\ \varpi(\Lambda_v)| \leq C_{11}(d)\,\gamma$. *En particulier,*

i) *le logarithme de la valeur absolue de* Ω' *est majoré par* $C_{11}\gamma'$;

ii) *le logarithme de la valeur absolue de* Ω_1 *(et donc de* Ω_2*) est minoré par* $-C_{11}\,\gamma$;

iii) *il existe deux entiers rationnels* b_1, b_2, *de valeurs absolues majorées par* $\exp(C_{12}(d)(\gamma + \gamma'))$, *tels que* $\Omega' = b_1\,\Omega_1 + b_2\,\Omega_2$.

Par ailleurs, $|\Omega_2/\Omega_1| \leq C_{13}(d)\gamma$.

Démonstration: la première assertion vient d'être démontrée (la minoration explicitement; reprendre l'argument sur $|f(\Lambda)|\,\varpi(\Lambda)^{w(f)}$ et y adjoindre l'inégalité de la taille pour la majoration). L'existence d'entiers b_1, b_2 vérifiant la relation de iii) étant claire ($\phi^*\omega = \omega'$!), leur majoration résulte alors de i), de ii), et de la quasi-orthogonalité de la base $\{\Omega_1, \Omega_2\}$. Quant à la dernière assertion, on la lit directement sur le développement de Fourier de la fonction $j(\tau)$. (Noter, à ce propos, le changement d'échelle: le premier minimum de la norme sur Λ peut atteindre e^{γ}, mais le second ne dépassera pas γe^{γ}.)

§2 Passage à la transcendance

L'énoncé-fleuve qui suit sera démontré au §3. J'explique ici comment le théorème de l'introduction s'en déduit.

Proposition 3 : *Pour tout entier* $d \geq 1$, *il existe un nombre réel* $c'(d)$ *effectivement calculable en fonction de* d *et vérifiant la propriété suivante. Fixons un corps de nombres* k *de degré* d *sur* $\mathbf{Q}$, *des nombres réels* $g , g' , r , r' , B \geq 1$, *deux réseaux* Λ , Λ' *de* $\mathbf{C}$ *d'invariants dans* k *de hauteurs majorées par* g , g' *et un entier* n *égal à* 1 *ou* 2. *Supposons qu'il existe* n *éléments* $\Omega_1 ,..., \Omega_n$ *de* Λ *linéairement indépendants sur* $\mathbf{Z}$ *et de valeurs absolues* $\leq \varpi(\Lambda)\, r$, *tels qu'une combinaison linéaire non triviale* $\Omega' = b_1 \Omega_1 + ... + b_n \Omega_n$ *à coefficients entiers de valeurs absolues* $\leq B$ *appartienne à* Λ' *et soit de valeur absolue* $\leq \varpi(\Lambda')\, r'$. *Posons enfin* : $h = g + g' + r^2 + r'^2 + \mathrm{Log}\, B$. *La propriété suivante est alors satisfaite* .

Plongeons de la façon usuelle les courbes elliptiques $E = \mathbf{C}/\Lambda$ *et* $E' = \mathbf{C}/\Lambda'$ *dans des plans projectifs, puis la variété abélienne* $G_n = E' \times E^n$ *dans un espace projectif par le biais d'un plongement de Segre* . *Repérons d'autre part l'espace tangent à l'origine de* G_n ,*qui s'identifie par construction à* $\mathbf{C} \times \mathbf{C}^n$, *au moyen des variables* $\{z', z_1,..., z_n\}$, *et notons* V_n *son hyperplan d'équation :* $z' = b_1 z_1 + ... + b_n z_n$. *Il existe alors une sous-variété abélienne non triviale* H *de* G_n , *de degré projectif majoré par* $\delta_n = c'(d)\, h^{3n}$, *dont l'espace tangent à l'origine est contenu dans* V_n .

Corollaire : *sous les hypothèses de la proposition* 3 *où l'on peut toujours supposer que* n *vaut* 2 *), il existe une isogénie de* E' *vers* E *définie sur* k *et de degré majoré par* $c''(d)\, h^{24}$, *où* $c''(d)$ *est effectivement calculable en fonction de* d .

Vérifions qu'on a alors bien démontré le théorème principal, avec $C = 49$, et $c(d)$ remplacé par une constante effective $c(k) = c(d,\delta)$. Soient donc E' une courbe elliptique définie sur k et k-isogène à E ,

et N le minimum des degrés des k-isogénies liant E et E'. D'après les propositions 1 et 2, les hypothèses de la proposition 3 sont satisfaites avec $n = 2$, $g = \gamma$, $r = C_{13}\gamma$, $r' = 1$, $g' = \gamma' = C_3(\gamma + \mathrm{Log}\, N)$, et $\mathrm{Log}\, B = C_{12}(\gamma + \mathrm{Log}\, N)$, d'où : $h = C_{14}(\gamma^2 + \mathrm{Log}\, N)$. Le degré de l'isogénie que fournit son corollaire est, comme il se doit, minoré par le minimum N. Ainsi, $N \leq C_{15}(\gamma^2 + \mathrm{Log}\, N)^{24}$, donc : $N \leq c(k)\,\gamma^{49}$. (La remarque (i) permettrait bien entendu de supprimer ici la dépendence en δ.)

Remarques : **(ii)** L'unique hypothèse qualitative de la proposition 3 (à savoir que $\Lambda \cap \Lambda'$ n'est pas réduit à O) ne présuppose pas que les courbes elliptiques $\mathbf{C}/\Lambda$ et $\mathbf{C}/\Lambda'$ soient isogènes. Mais c'en est un corollaire, en vertu d'un vieux théorème de Schneider (il s'agit donc bien d'un énoncé de transcendance !).

(iii) Pour l'application qu'on a en vue, V_n n'est autre que l'espace tangent à l'origine du noyau de l'homomorphisme $\{P', P_1, ..., P_n\} \to \phi(P') - b_1P_1 - ... - b_nP_n$ de $E' \times E^n$ dans E (rappelons que $d\phi$ est représenté par la matrice 1). Le degré de la composante neutre H_n de ce sous-groupe algébrique croît polynômialement avec B, alors que le degré du sous-groupe H fourni par la conclusion de la proposition 3 est majoré par un polynôme en $\mathrm{Log}B$. Cette réduction au logarithme des estimations triviales est typique de la méthode de Baker (voir [Be2], Proposition 8).

(iv) Pour démontrer le corollaire à la proposition 3, point n'est besoin de préciser *le corps de définition de l'isogénie* ψ (de degré $\nu \leq c'' h^{24}$) qu'il fournit. En effet, dans le cas général où le corps de base k contient le corps de définition de tous les endomorphismes de E, toute isogénie de E' vers E est automatiquement définie sur k (puisque sa duale, composée avec la k-isogénie donnée par hypothèse, est un endomomorphisme de E). Sinon, E admet des multiplications complexes par un ordre R d'un corps quadratique imaginaire non contenu dans k, et il suffit de noter que, dès qu'elle est non nulle, la somme de ψ et de sa conjuguée sous $\mathrm{Gal}(k.R/k)$ est de degré $\leq 2\nu$. Si enfin ψ est de trace nulle, sa composée avec tout élément imaginaire pur α de R est une

k-isogénie de E' vers E de degré $\leq \nu\,|\alpha|^2$; or il existe un tel élément α de norme sur $\mathbf{Q}$ majorée par la valeur absolue D du discriminant de R , et D est borné par $c'''(d)$ (d'après Gross- Zagier...). Au risque d'abîmer un peu la constante C du théorème, mais de façon plus réaliste, on majorera D par $C_{18}(d)\,g^2 \leq C_{18}\,h^2$, grâce à la dernière assertion de la proposition 2 , appliquée au conjugué $j(R)$ de $j(\tau)$ (voir [F-P]).

Nous montrons maintenant comment la proposition 3 entraîne son corollaire. Retenons de sa conclusion que H est un sous-groupe connexe non trivial de G_n ne contenant pas E' et distinct de E^n (puisque Lie H est inclus dans V_n et que $b_1, \ldots, b_n$ ne sont pas tous nuls).

a) Supposons tout d'abord que les hypothèses de la proposition 3 soient satisfaites avec $n = 1$. Le sous-groupe H de sa conclusion ne peut être qu'une courbe elliptique dans $E'\times E$, passant par l'origine et se projetant surjectivement sur chacun de ces deux facteurs . Ces projections sont donc des isogénies de H vers E et E' . Si d , d' désignent leurs degrés respectifs, le degré projectif $H.(3E' + 3E)$ de H vaut $3(d + d')$ et en composant l'une avec la duale de l'autre, on obtient une isogénie de degré $dd' < \delta_1^2 << h^6$ entre E et E' .

Si maintenant les hypothèses de la proposition 3 ne sont vérifiées qu'avec $n = 2$, on distingue deux cas :

b) le sous-groupe connexe H de $E'\times E^2$ se projette surjectivement sur E' : si c'est une surface, la composante neutre de son intersection avec $E'\times E\times\{0\}$ -ou, si $b_1 = 0$, avec $E'\times\{0\}\times E$ - fournit une correspondance
du même type que supra (avec δ_1 remplacé par $3\delta_2$), d'où une isogénie entre E et E' de degré $<< h^{12}$; si c'est une courbe, la composée de sa projection sur $E\times E$ avec la projection sur l'un des facteurs E est une isogénie de degré $\leq \delta_2$, et on aboutit à la même conclusion.

c) H est un sous-groupe connexe, et *propre* de $E\times E$. La considé- ration du quotient G_2/H va alors permettre de se ramener au cas $n = 1$. Pour clarifier l'argument, je repousse à la remarque (vi)

ci-dessous le cas de multiplications complexes (qu'on pouvait d'ailleurs traiter directement) et suppose que E n'en a pas. Le sous-groupe de $\mathrm{Hom}(E^2, E) \approx \mathbf{Z}^2$ formé des homomorphismes $u = (u_1, u_2)$ dont le noyau contient H est dans ce cas engendré par un élément (u_1, u_2) de $\mathbf{Z}^2$ vérifiant $|u_1|^2 + |u_2|^2 = \deg(H)/3$ (noter que u_1 et u_2 sont premiers entre eux - puisque H est connexe -, et appliquer à l'homomorphisme dual de u le lemme 3 de [Be3]; voir aussi [M-W1], III). Comme $\mathrm{Lie}(H)$ coïncide avec $V_2 \cap \mathrm{Lie}(E^2)$, ce sous-groupe contient (b_1, b_2), et il existe un entier rationnel b tel que $(b_1, b_2) = b.(u_1, u_2)$. Mézalor, $\Omega = u_1\Omega_1 + u_2\Omega_2$ est un élément de Λ de valeur absolue $|\Omega| \leqslant \varpi(\Lambda) r^{\#}$, où $r^{\#} = 2r\sqrt{\delta_2}$, tel que :

$$\Omega' = b\Omega ,$$

où $|b| \leq B$. Bref, les hypothèses de la proposition 3 sont vérifiées avec h remplacé par $h^{\#} = g + g' + 4r^2\delta_2 + r'^2 + \mathrm{Log}\, B \leq C_{19}\, h^7$, et surtout, bien sûr, $n = 1$. D'après a), il existe donc une isogénie de E' vers E de degré $\ll h^{\#3} \ll h^{21}$. QED (pour $\mathrm{End}\, E = \mathbf{Z}$).

Bien entendu, le point fondamental cette dernière réduction est qu'elle n'a guère augmenté la valeur absolue des périodes considérées : écrire $\Omega' = \Omega$, avec $\Omega = b_1\Omega_1 + b_2\Omega_2$ pour se placer dans le cas $n = 1$ transforme h en hB, ce qui serait rédhibitoire.

Remarques : (v) "v-*rang* " *d'une isogénie* : replaçons-nous dans la situation du §1. Le plus petit des entiers n vérifiant les hypothèses de la proposition 3 pour des valeurs de r' et $\mathrm{Log}\, B$ polynômiales en le *logarithme* du degré de l'isogénie ϕ est un analogue (lointain) du p-rang des isogénies, relativement à la place archimédienne v de k qu'on a privilégiée; $\mathrm{Log}\, B$ correspond alors au niveau des p-isogénies de [Ra], §4. Dans cette optique, la preuve du corollaire peut se résumer ainsi: en général (cas b), le sous-groupe H de G_2 définit une "bonne" correspondance entre E et E', et on a gagné; quand ce n'est pas le cas (cas c), ϕ est en fait de "v-rang" 1, et (cas a) le sous- groupe H de G_1 que fournit la proposition 3 est encore une "bonne" correspondance entre E et E'. De façon plus sérieuse, les Chudnovsky ont remarqué qu'on peut toujours prendre $n = 1$ si v est une place réelle. Cela leur a

donné la première démonstration transcendante du théorème de l'introduction, lorsque k admet un plongement réel ([Ch],§4). Voir [Be1] (corollaire au théorème 2) pour une autre apparition de cette notion de v-rang.

(vi) *Le cas de multiplications complexes.* Pour le traiter, le plus simple consiste à réécrire l'hypothèse de la proposition 3 sous la forme : $\Omega' = b\Omega$, où b est cette fois un élément de l'anneau R des endomorphismes de E (autrement dit, le v-rang sur R vaut toujours 1). La preuve du §3 s'étend sans difficulté, et on conclut comme en a) . On peut aussi (en remplaçant $\mathbf{Z}$ par R) reprendre l'argument précédent et ce, presque mot pour mot si R est principal (la rationnalité de b_1 et b_2 et la coprimalité de u_1 et u_2 entraînent que sans en changer les valeurs absolues, les éléments b , u_1 et u_2 de R peuvent être choisis rationnels). Si R n'est pas principal, le R -module $\mathrm{Hom}(E^2, E)$ contient un sous-R -module libre d'indice majoré, avec les notations de la remarque iv), par $\sqrt{D}$. On aboutit alors à une relation de la forme $\Omega'^* = b^*\Omega^*$, avec $|b^*| \leq \sqrt{DB}$, $r'^* \leq \sqrt{D}r'$, $r^* \leq \sqrt{D}r^{\#}$, d'où une isogénie de degré $<< h^{*3}$, où $h^* = \sqrt{D}h^7$. Les majorations de D données à la remarque (iv) permettent de conclure.

§3 La méthode de Baker

On reprend les notations de la proposition 3 , qu'on va maintenant démontrer. On désigne de plus par $\wp = \wp(z, \Lambda)$, $\wp' = \wp(z,\Lambda')$ les fonctions de Weierstrass associées aux réseaux Λ , Λ' (l'apostrophe n'est donc pas une dérivation). Les expressions $c_1, c_2, \ldots$ représentent désormais des nombres réels > 0 effectivement calculables en fonction du seul degré d de k sur $\mathbf{Q}$.

Je regroupe tout d'abord les estimations, de nature analytique ou arithmétique, auxquelles on fera appel (la seconde, qui concerne le type de croissance de certaines fonctions thêta, est cruciale). J'exprime les résultats sur le réseau Λ , mais c'est leur analogue sur Λ' qui importe le plus dans les applications.

Proposition 4 (voir [Ma3]) : i) *pout tout couple* $\{t , \ell\}$ *d'entiers* ≥ 1,

la dérivée d'ordre t *de* $\wp^{\ell}(z, \Lambda)$ *s'exprime comme un polynôme de degré* $\leq c_1(t+\ell)$ *en* $g_2(\Lambda)/2$, $\wp(z,\Lambda)$ *et sa dérivée première, à coefficients entiers de valeur absolue* $\leq c_1(t+\ell)\,\mathrm{Log}(t+\ell)$;

ii) *il existe une fonction thêta* $\theta = \theta(z,\Lambda)$ *associée au diviseur polaire de* $\wp$ *telle que, pour tout nombre complexe* z :

$$|\,\mathrm{Log}\,\max(|\theta(z)|\,,\,|\theta\wp(z)|)\,| \leq c_2(g + (|z|/\varpi(\Lambda))^2)$$

(noter les valeurs absolues au premier membre);

iii) *pour tout couple* {n,q} *d'entiers* ≥ 1 , *et tout élément* Ω *de* Λ , *le nombre* $\wp(n\Omega/q)$, *s'il est défini, est algébrique sur* k , *de degré* $< q^2$, *et de hauteur (absolue)* $\leq c_3 g$;

iv) *pour tout couple* {n,q} *d'entiers* ≥ 1 , *et tout élément* Ω *de* Λ *de valeur absolue* $\leq \varpi(\Lambda)\,t$, *le nombre* $\theta(n\Omega/q)$, *s'il est non nul, est de valeur absolue* $\geq \exp(-c_4(gq^2 + t^2(n/q)^2))$.

Démonstration: pour i), voir [Ba] , ou [Ma3] (ou encore [Da]); comme le covolume de Λ est minoré par $\varpi(\Lambda)^2/2$ (Hermite), ii) résulte immédiatement de [Co] ou de [F-P], dont on trouvera d'ailleurs des formes raffinées, et plus suggestives, dans [Ma3] et dans [Da]; iii) résulte de l'énoncé bien connu de Demjanenko-Zimmer (voir aussi [M-Z]); on en déduit que $|\wp(n\Omega/q)|$ est $\leq \exp(c_5 g q^2)$, et la minoration sous-jacente à ii) conduit à iv).

Remarque : (vii) Suivant une remarque de B. Mazur, la fonction thêta en question est un avatar archimédien de la fonction thêta p-adique canonique du cas ordinaire. En fait, le lemme 1.3.6 de [Ka 2] montre que la fonction $\theta(z)$ du lemme 3.1 de [Ma3] coïncide, à un facteur trivial près, avec le carré de la fonction $\Delta(\Lambda)^{1/12}\sigma(z,\Lambda)\exp(-s_2(\Lambda)z^2/2)$, où les notations σ et s_2 ont leur signification usuelle.

Passons à la démonstration de la proposition 3 . Je la détaille sous l'hypothèse (plus délicate, même si la conclusion en est moins précise) où n vaut 2 , et indique à la fin comment choisir les paramètres quand $n = 1$. J'omettrai l'indice 2 des notations G_2 , V_2 , δ_2 de la proposition.

1ère étape [Siegel: *construction d'un diviseur* Z *sur* $G = E' \times E^2$ *admettant*

un gros sous-schéma ponctuel supporté par l'origine] Posons

$$L = 4\,d\,h^6 , \quad T = h^9 ,$$

toujours avec $h = g + g' + r^2 + \mathrm{Log}\, N$, et notons Ω le point $(\Omega', \Omega_1, \Omega_2)$ de $\mathbf{C}^3$. Il existe un polynôme $P(X , X_1, X_2)$ non nul de degrés partiels $\leq L$, à coefficients entiers rationnels de hauteur $\eta \leq c_6 h^{10}$, tel que la fonction

$$F(z', z_1, z_2) = P(\wp'(z'), \wp(z_1), \wp(z_2))$$

s'annule au point $(1/2)\Omega$ à un ordre de multiplicité $\geq T$ selon le champ de 2-directions défini par V .

Voici pourquoi : considérons la base

$$\{\partial_1 = b_1 \partial/\partial z' + \partial/\partial z_1 , \partial_2 = b_2 \partial/\partial z' + \partial/\partial z_2\}$$

de V . Par définition, on demande à F que toutes ses dérivées partielles d'ordre $< T$ en ∂_1 et ∂_2 s'annulent en $\Omega/2$. Il s'agit donc de résoudre un système linéaire d'ordre $< T^2$ en plus de L^3 variables, à coefficients dans un corps de nombres de degré $\leq 9\,d$. D'après les assertions i) et iii) de la proposition 4 , le maximum de l'exponentielle des hauteurs (et d'un dénominateur commun) de ces coefficients est majoré par

$$B^T e^{c_7 (g + g')(L+T)} e^{c_8 (T+L)\mathrm{Log}(T+L)} ,$$

et le lemme de Siegel permet de conclure. Le diviseur effectif Z sur G correspondant au diviseur de la fonction analytique en $\mathbf{z} = (z', z_1 , z_2)$:

$$\Theta(z) = (\theta'(z'+\Omega'/2)\theta(z_1+\Omega_1/2)\theta(z_2\Omega_2/2))^L F(z + \Omega/2) ,$$

passe alors par l'origine avec une multiplicité $\geq T$ le long de V .

2ème étape [extrapolation: *le diviseur Z passe en fait par un sous-groupe cyclique Γ pas trop petit de G , toujours avec forte multiplicité le long de V* (c'est, avec la définition même des coefficients de V , le seul passage analytique de la preuve)] . Soit q le plus petit entier impair tel que

$$q \geq h^{1/13} .$$

On va montrer que la fonction Θ s'annule en tous les multiples entiers de $(1/q)\Omega$ avec un multiplicité $\geq T/2$ le long de V . Soit donc $s\Omega/q$ un tel point, avec, sans perte de généralité, $|s| < q$.

Par périodicité, la fonction Θ s'annule en tous les multiples entiers de Ω avec une multiplicité $\geq T$ le long de V. Considérons alors la fonction d'une variable $f(z) = D\Theta(z\Omega)$, où D est un monôme différentiel d'ordre $\tau < T/2$ en les dérivations ∂_1, ∂_2 de V, tel que $D'\Theta(s\Omega/q)$ soit nul pour tout opérateur D' de ce type et d'ordre $< \tau$. La fonction f s'annule en tous les entiers à un ordre $\geq T - \tau \geq T/2$, et d'après les inégalités de Cauchy, la proposition 5, ii) et la majoration donnée des valeurs absolues des coefficients de Ω, son maximum sur un disque de rayon $R \geq 1$ vérifie :

$$|f|_R \leq (L+1)^3 e^{\eta(BT)^T} e^{c_2(2g+g'+4R^2(2r^2+r'^2))L}.$$

Le lemme de Schwarz, appliqué sur les disques de rayon $R = h^{3/2}$ et $3R$, entraîne alors que :

$$\text{Log } |D\Theta(s\Omega/q)| \leq \text{Log } |f|_1 \leq \text{Log}|f|_R \leq -TR + \text{Log}|f|_{3R} \leq -c_9 h^{10,5},$$

et on déduit de la formule de Leibniz, jointe à la définition de D et à la proposition 4, iv), que le nombre $\xi = DF(s\Omega/q + \Omega/2)$ vérifie :

$$\text{Log } |\xi| \leq c_{10}((g+g')q^2 + r^2 + r'^2) L - c_9 h^{10,5} \leq -c_{11} h^{10,5}.$$

Mais d'après la proposition 4, iii), ce nombre est algébrique sur k, de degré $\leq 36\, q^6$, et de hauteur (absolue) majorée, à un facteur constant près, par

$$T \text{ Log } B + \text{Log } H + \text{Log } L + (T + L)(g + g' + \text{Log}(L + T)) \leq c_{12} h^{10}.$$

Comme $dq^6 h^{10}$ est beaucoup plus petit que $h^{10,5}$ (pour $h > c_{13}$), la formule du produit impose à ξ d'être nul, et Θ s'annule bien en $s\Omega/q$ à un ordre $\geq T/2$ le long de V. En d'autres termes, le diviseur Z de G passe par le sous-groupe cyclique Γ engendré par $\exp_G(\Omega/q)$ avec une multiplicité $\geq T/2$ le long de V.

3ème étape [Le paradis des lemmes de zéros] On va faire appel au lemme de multiplicité de [Ph], dont je transcris maintenant l'énoncé dans notre contexte. La constante (effective) c qui y apparaît ne dépend que du plongement projectif de G.

Proposition 5 (Philippon) : *Soient* G *une variété abélienne plongée*

dans un espace projectif , λ *et* τ *deux entiers* ≥ 1 , Γ *un sous-groupe fini de* G , V *une sous espace de* Lie G *et* Z *un diviseur effectif sur* G , *de degré projectif* λ . *On suppose que* Z *passe par* Γ *avec un ordre de multiplicité* $\geq$ (dimG) τ *le long de* V . *Il existe alors une sous-variété abélienne* H *de* G , *distincte de* G , *telle que*

$$\tau^{\dim\pi_*(V)} \operatorname{card}(\pi(\Gamma)) \deg(H) \leq c\, \lambda^{\dim\pi(G)} ,$$

où π *désigne la projection de* G *sur* G/H .

D'après le 2ème pas, le diviseur Z construit au 1er pas vérifie les hypothèses de la proposition 5 avec $\tau = T/6$, $\lambda = c_{14} L$ et un sous-groupe Γ de cardinal q (on peut en effet supposer sans perte de généralité que Ω est une période primitive du réseau $\Lambda' \times \Lambda^2$ de $\mathbf{C}^3$). Que peut-on alors dire de la sous-variété abélienne H de sa conclusion?

- elle ne peut être réduite à O , puisque $T^{\dim(V)} q = T^2 q$ est bien plus grand que $L^{\dim(G)} = L^3$;

- les sous-variétés abéliennes H dont l'algèbre de Lie n'est pas contenue dans V vérifient V + Lie H = Lie G , d'où dim $\pi_*(V)$ = dim $\pi(G)$, et sont également exclues, en vertu de l'inégalité T >> L .

Ainsi, H est un sous-groupe algébrique connexe non trivial de G , d'algèbre de Lie contenue dans V , et de degré projectif

$$\deg H \leq c_{14} L\, (L/T)^{\dim(V/\text{Lie } H)} \leq c'(d)\, h^6 \quad \text{(pour } n = 2) .$$

Enfin, la démonstration précédente s'adapte facilement au cas n = 1 , où on pourra choisir comme paramètres :

$$L = 4d\, h^3 \ , \ T = h^6 \ , \ \eta \approx h^7 \ , \text{ et R , q comme plus haut.}$$

Remarques : (viii) Si les paramètres L et T de la construction du 1er pas expriment des conditions géométriques évidentes sur Z , c'est en *théorie d'Arakelov* que le paramètre η prend une signification naturelle : on peut en effet définir grâce à lui des métriques sur les fibrés $O_G(L) \otimes k_V$ telles que le polynôme auxiliaire P s'interprète comme une section du fibré d'Arakelov correspondant. La référence au lemme de Siegel (c'est à dire au principe des tiroirs), plutôt qu'au théorème de

Minkowski, pour justifier l'existence d'une telle section, est standard en transcendence.

(ix) Dans le 2ème pas, le fait que ξ puisse être de degré élevé sur k joue contre nous. C'est pourtant bien ce qui se produit (d'après les théorèmes d'irréductibité de Serre). Il est cocasse que l'énoncé auquel on en a permette de raffiner une partie de ces théorèmes...

(x) Il n'est pas sans intérêt de noter que des énoncés similaires à la proposition 5 du 3ème pas (mais moins généraux) apparaissent également dans la démonstration "algébrique" des théorèmes de Faltings. Voir par exemple [MB], lemme 3.2.3 (contrairement à [Ph], la preuve de ce lemme de zéros ne fait d'ailleurs pas explicitement appel à la théorie de l'intersection).

(xi) La démarche de la démonstration ci-dessus, et de la réduction par passage au quotient du §2 , cas c , est inspirée de la preuve de la proposition 8 de [Be2] (voir [Wü] pour un analogue multiplicatif). Il est probable que la présentation donnée dans [P-W] de la méthode de Baker permette d'obtenir directement (i.e. sans hypothèse sur la valeur de n) la correspondance recherchée entre E et E' , et même d'éviter le recours aux points de division par q dans le lemme de zéros.

(xii) *Des courbes aux points* : La même méthode de transcendance permet d'établir le résultat suivant : si des points P_1 , ..., P_n de E(k) , de hauteurs de Néron-Tate $\leq \eta$, sont linéairement dépendants sur **Z** (on voudrait dire "isogènes entre eux dans leur ensemble"), ils sont nécessairement liés par une relation de dépendance linéaire à coefficients entiers de valeurs absolues (on voudrait dire, avec beaucoup de guillemets,"une isogénie de degré") $\leq c(E,n,k)\ \eta^{n-1}(\mathrm{Log}\ \eta)^{c(n)}$. Mais des méthodes purement algébriques - et tout aussi effectives - y conduisent également, sans même le terme en Log (cf. [Ma2] , [Be3]) . Il serait intéressant de traduire tout ceci en termes de 1-motifs.

Appendice

A) *Une chasse aux discriminants* : dans la version affaiblie que nous venons d'établir du théorème de [M-W2] , la dépendance de la "cons-

tante" $c(k)$ en la valeur absolue δ du discriminant de k sur $\mathbf{Q}$ n'apparaît que par le biais de la constante C_3 de la proposition 3, et on vérifie aisément que $c(k)$ est, à un facteur explicite en d près, de la forme $(\mathrm{Log}\ \delta)^{C'}$, où $C' = C-1$. Quitte à augmenter la constante C , on peut alors supprimer cette dépendance en δ . A titre de curiosité (puisqu'il est bien plus simple d'appliquer la remarque (i)), nous indiquons ici pourquoi.

Notons tout d'abord k_0 le corps de définition du modèle de Weierstrass de E donné dans l'énoncé du théorème, et N le degré de la k-isogénie dont on part. D'après l'inégalité de Hadamard (voir l'addendum de [Si]), le logarithme de la valeur absolue du discriminant de k_0 sur $\mathbf{Q}$ est $<< \gamma$ (les constantes implicites de ce paragraphe ne dépendent que du degré d). Du corollaire 2.1.4 de [Ra] , joint au théorème de comparaison des hauteurs stable et modulaire de [MB], on déduit par ailleurs que la hauteur de l'invariant modulaire $j(E')$ de E' est $<< \gamma + \mathrm{Log}\ N$. Soient alors L_0 le sous-corps de k engendré sur k_0 par $j(E')$, et E'' une courbe elliptique definie sur L_0 , isomorphe à E' sur la clôture algébrique $\overline{k}$ de L_0 , et munie d'un modèle de Weierstrass de hauteur $<< h(j(E'))$. Il est clair qu'une telle courbe existe, et que l'extension L de L_0 engendrée par les points de 3-torsion de E et de E'' est de degré $\leq 81d$ sur $\mathbf{Q}$. Toujours d'après [Si], elle vérifie : $\mathrm{Log}|\mathrm{Disc}(L/\mathbf{Q})| << \gamma + \mathrm{Log}\ N$. Mais il existe par hypothèse une $\overline{k}$ -isogénie de E'' vers E de degré N , et dès que E n'admet comme automorphismes que 1 et -1 (cas auquel on peut, sans perte de généralité, se ramener), un argument classique de cohomologie galoisienne et de rigidité impose à une telle isogénie d'être définie sur L . Le discriminant de L étant maintenant contrôlé, on peut appliquer au triplet (E, E'', L) notre version affaiblie du théorème : il existe une L-isogénie de E'' vers E de degré $<< (\gamma + \mathrm{Log}\ N)^{C'} \gamma^{C}$. Idem, donc, avec une $\overline{k}$ -isogénie de E' vers E , donc encore, par l'argument de la remarque (iv), avec une k-isogénie de E' vers E . On conclut comme auparavant, en choisissant N minimal.

Noter que l'extension des scalaires obtenue par adjonction de points de torsion a rendu les courbes E et E'' semi-stables. On aurait ainsi pu également contrôler le discriminant du corps de définition de

l'isogénie en appliquant à la variété abélienne $E \times E''$ le théorème de lissité de Ribet [Ri].

B) *La constante* C : Tout d'abord, un point technique. On a ici choisi comme échelle de mesure des espaces tangents des tores complexes le minimum ϖ des valeurs absolues non nulles de leurs réseaux de périodes. Il aurait été plus rentable de prendre le covolume de ces réseaux (voir la preuve de la proposition 3, ii)). Cela permet, dans l'application du corollaire à la proposition 3 , de prendre r de l'ordre de $\sqrt{\gamma}$, d'où une division de C par 2 .

De façon plus fondamentale, on n'a fait appel, dans la formulation de la proposition 3 , qu'à "la moitié" de l'information fournie par l'isogénie ϕ , alors que l'assertion iii) de la proposition 2 s'étend sans modification notoire au second minimum de Λ' . Pour en tirer parti, il convient d'étendre la proposition 3 en un énoncé de type "formes linéaires simultanées de logarithmes de points algébriques" (au sens de [P-W]).

En fait, tout porte à croire (voir [Ch], et [La], théorème 6, joint à la proposition 1 du présent texte) que du point de vue transcendant, la valeur optimale de C est 2 . La tradition folklorique veut sans doute que C vaille 0 (au moins dans la version affaiblie du théorème), mais cela paraît sans espoir du côté transcendant

C) *Hauteurs* : Dans ce dernier paragraphe, les "constantes" dépendent de d et de δ , et nous nous restreignons pour simplifier aux courbes elliptiques E'/k munies d'une k-isogénie vers E et semi-stables (d'après le théorème de monodromie et le théorème d'Hermite, cette hypothèse est satisfaite sur une extension de k de degré et de discriminant effectivement contrôlés). Une fois le degré minimal N des k-isogénies entre E et E' borné, le corollaire 2.1.4 de [Ra] permet de majorer la valeur absolue m de la différence entre les hauteurs de Faltings $h(E) = h(E/k)$ et $h(E')$ de E et E' . On obtient : $m \ll \text{Log } h(E)$. Au théorème 4.4.9 de [Ra], Raynaud donne une majoration de m *indépendante* du calcul de N , qui entraîne $m \ll (\text{Log } B(E))^2$, où $B(E)$ désigne le maximum des normes des places de mauvaise réduction de E/k , mais est en fait beaucoup plus fine. Il serait intéressant de comparer ces majorations (à l'aide de l'inégalité de Stark, ou, comme dans [La], de la conjecture de Szpiro). De façon plus fondamentale, peut-on *déduire* des résultats de [Ra] une majoration du degré minimal N ?

Bibliographie

[Ba] A. BAKER : On the periods of the Weierstrass $\wp$-function; Symp. Math., 68-69, INDAM, IV, 155-174.

[Be1] D. BERTRAND : Galois orbits on abelian varieties; London M.S. L.N. 109, 1986, 21-35.

[Be2] D. BERTRAND : Lemmes de zéros et nombres transcendants; in Astérisque 145 -146 ,1987, 21-44. (Voir aussi: La théorie de Baker revisitée; Probl. Dioph. 84-85, n°2.)

[Be3] D. BERTRAND : Minimal heights and polarizations on abelian varieties; Prep. MSRI, Berkeley, Juin 1987 .

[Co] P. COHEN : Explicit calculation of some effective constants in transcendence theory; in Ph. D. Nottingham, 1985.

[Ch] D. & G. CHUDNOVSKY : Padé approximations and diophantine geometry; Proc. Nat.Ac. Sc. USA, 82, 1985, 2212-2216.

[Da] S. DAVID : Fonctions thêta et points de torsion des variétés abéliennes; CRAS Paris, 305, 1987, 211-214. (Voir aussi : Formes modulaires et dérivées de fonctions thêta; "Problèmes diophantiens" 86-87, n°4.)

[F-P] A. FAISANT- G. PHILIBERT: Approximations simultanées de τ et de $j(\tau)$; "Problèmes diophantiens" 83-84, t. 2, n°2.

[Ka1] N. KATZ : p-adic properties of modular forms and modular schemes ; in Modular Functions III, SLN 350, 1973, 69-190.

[Ka2] N. KATZ : p-adic interpolation of real analytic Eisenstein series; Ann. Math., 104, 1976, 459-571.

[La] M. LAURENT : Une nouvelle démonstration du théorème d'isogénie, d'après [Ch]; Birkhäuser Prog .Math., 71, 1987, 119-131.

[M-Z] Y. MANIN-Y. ZARHIN: Heights on families of abelian varieties; USSR Mat. Sb., 18, 1972, 169-179.

[Ma1] D. MASSER : Small values of heights on families of abelian varieties; SLN 1290, 1988, 109-148.

[Ma2] D. MASSER : Linear relations on algebraic groups; in "New advances in transcendence theory", ed. A. Baker, Cambridge U.P.,1988, 248-262.

[Ma3] D. MASSER : Counting points of small heights on elliptic curves; Bull. SMF, à paraître.

[Ma4] D. MASSER : Exposés en Bavière, été 1988.

[M-W1] D. MASSER-G. WUSTHOLZ : Fields of large transcendence degree generated by values of elliptic functions; Inv. mat. 72, 1983, 407-464.

[M-W2] D. MASSER-G. WUSTHOLZ : Estimating isogenies on elliptic curves ; Invent. math., à paraître.

[MB] L. MORET-BAILLY : Compactifications, hauteurs et finitude; in Astérisque 127, 1985, 113-129.

[Ph] P. PHILIPPON: Lemmes de zéros sur les groupes algébriques commutatifs; Bull. SMF, 114, 1986, 355-383, et 115, 1987, 397-399.

[P-W] P. PHILIPPON - M. WALDSCHMIDT : Formes linéaires de logarithmes simultanées sur les groupes algébriques; à paraître.

[Ra] M. RAYNAUD : Hauteurs et isogénies; Astérisque127, 1985, 199-234.

[Ri] K. RIBET : Endomorphisms of semi-stable abelian varieties over number fields; Ann. Maths 101, 1975, 555-562.

[Se] J-P. SERRE : Abelian ℓ -adic representations and elliptic curves; Benjamin, 1968.

[Si] J. SILVERMAN : The Thue equation and height functions; Birkhäuser Prog. Math., 31, 1983, 259-270.

[Wü] G. WUSTHOLZ: A new approach to Baker's theorem on linear forms in logarihms II; SLN 1290, 1988.

Daniel BERTRAND
Université de Paris VI
Mathématiques, T.46
75 251 Paris Cédex O5.