ACTA ARITHMETICA
C.1 (2001)

À propos de la conjecture de Lang sur la minoration de la hauteur de Néron–Tate pour les courbes elliptiques sur $\mathbb{Q}$

par

Mohamed Krir (Versailles)

Introduction. Soit E une courbe elliptique sur $\mathbb{Q}$. La hauteur de Néron–Tate, relative au diviseur (0), sur E est une forme quadratique $\widehat{h}$: $E(\mathbb{Q}) \to [0, +\infty[$ définie positive sur $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Elle est donc minorée. Serge Lang a formulé la conjecture suivante à propos de ce minorant :

Conjecture ([La], p. 92). *Il existe une constante $C > 0$ telle que pour toute courbe elliptique E sur $\mathbb{Q}$ de discriminant minimal Δ_E et pour tout point d'ordre infini de $E(\mathbb{Q})$ on a*

$$\widehat{h}(P) > C \log |\Delta_E|.$$

Des minorations de $\widehat{h}$ ont été étudiées par J. H. Silverman [Si1] et par M. Hindry et J. H. Silverman [H-S]. On se propose dans cet article de préciser la constante C dans la conjecture de Lang pour certaines familles de courbes elliptiques sur $\mathbb{Q}$. On utilisera pour cela les méthodes de Silverman [Si1] en explicitant toutes les constantes. Je pense que les méthodes utilisées dans [H-S] ne fournissent pas de meilleures minorants, tout au moins dans le cas général. D'autres résultats à propos de cette conjecture sont obtenus par D. Sinou ([Sin1]–[Sin3]). On montre en particulier (voir proposition 2.3 ci-dessous) que l'on peut prendre

$$C = \begin{cases} 10^{-3} & \text{si } \Delta_E \text{ est sans facteurs carrés,} \\ 10^{-5} & \text{si le conducteur de } E \text{ est un nombre premier,} \\ 10^{-6} & \text{si l'invariant modulaire } j \text{ de } E \text{ est un nombre} \\ & \text{entier} \neq 0, 1728. \end{cases}$$

Le cas particulier des courbes elliptiques E sur $\mathbb{Q}$, d'invariant modulaire $j = 0$ ou 1728 sera traité à part. Dans le cas où $j = 0$, la courbe elliptique E admet une équation de Weierstrass de la forme $y^2 = x^3 + d$ où d est un

2000 *Mathematics Subject Classification*: 11G05, 11G07, 11G50.

entier non nul sans facteurs sixièmes. Son discriminant est $\Delta = -2^4 \cdot 3^3 \cdot d^2$ et on montre (voir proposition 3.1) que pour tout point d'ordre infini de $E(\mathbb{Q})$ on a

$$\widehat{h}(P) > 10^{-3} \log |d| + 10^{-3}.$$

Si $j = 1728$, la courbe E admet une équation de Weierstrass de la forme $y^2 = x^3 + dx$ où d est un entier non nul sans facteurs quatrièmes. Son discriminant est $\Delta = -2^6 \cdot d^3$ et on montre (voir proposition 4.1) que pour tout point d'ordre infini de $E(\mathbb{Q})$ on a

$$\widehat{h}(P) > \frac{1}{64} \log |d|.$$

Je tiens ici à remercier vivement le referee pour ses remarques et en particulier celle concernant la minoration donnée dans la proposition 2.1 de [B-S-T] qui est meilleure que celle qu'on obtient ici dans la proposition 4.1 dans le cas où la valeur de d est $-n^2$.

Pour tout nombre premier p, il existe une hauteur locale $h_p : E(\mathbb{Q}) \to \mathbb{R}$ et pour la place à l'infini de $\mathbb{Q}$, il existe une hauteur locale $h_\infty : E(\mathbb{Q}) \to \mathbb{R}$ de sorte que pour tout point $P \in E(\mathbb{Q}), P \neq 0$, on ait

$$\widehat{h}(P) = h_\infty(P) + \sum_p h_p(P).$$

On dispose de formules explicites ([Si2], th. 3.4, p. 468 et th. 4.2, p. 472) pour chacune des hauteurs locales. On se propose de donner ici un minorant de $\widehat{h}$ en minorant chacune de ses composantes locales. L'essentiel de ce travail est consacré à la minoration de la hauteur locale archimédienne h_∞, ce qui fait l'objet du §1. On montre (voir théorème 1) que pour toute courbe elliptique E sur $\mathbb{R}$ et pour tout point $P \in E(\mathbb{R}) - \{0\}$ on a $\sup_{1 \leq k \leq 9} h_\infty(kP) > 0$. Dans le §2, on utilise les minorations ainsi trouvées pour minorer la hauteur de Néron–Tate sur une courbe elliptique d'invariant modulaire $j \neq 0, 1728$ et déduire des cas particuliers de la conjecture de Lang. Enfin les deux derniers paragraphes sont consacrés à l'étude des deux cas particuliers où $j = 0$ ou 1728.

1. La hauteur locale archimédienne. Rappelons que pour toute courbe elliptique E sur $\mathbb{C}$, il existe un réseau (de périodes d'une forme différentielle non nulle invariante sur E) $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ où $\tau = s + it$ avec $s, t \in \mathbb{R}$, $|s| \leq 1/2$ et $t \geq \sqrt{3}/2$ et on a un $\mathbb{C}$-isomorphisme analytique

$$E(\mathbb{C}) \to \mathbb{C}/\Lambda, \quad P \mapsto z(P) = a(P) + b(P)\tau, \tag{1}$$

et a, b définissent deux homomorphismes

$$a, b : E(\mathbb{C}) \to \mathbb{R}/\mathbb{Z}. \tag{2}$$

Soit $P \in E(\mathbb{C}) - \{0\}$. Posons $z = z(P) = a(P) + b(P)\tau$ avec $a(P), b(P) \in \mathbb{R}/\mathbb{Z}$ et posons $q_\tau = e^{2i\pi\tau}$ et $q_z = e^{2i\pi z}$. Alors la hauteur locale archimédienne du point P est donnée par (*cf.* [Si2], th. 3.4, p. 468)

$$h_\infty(P) = -\frac{1}{2} B_2(b(P)) \log|q_\tau| - \log|1 - q_z| - \sum_{n \geq 1} \log|(1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1})| \tag{3}$$

où $B_2(T) = T^2 - T + 1/6$ est le second polynôme de Bernoulli.

Si la courbe elliptique E est définie sur $\mathbb{R}$, il existe (*loc. cit.*, p. 417) un unique τ appartenant à l'ensemble

$$\mathcal{C} = \{it : t \geq 1\} \cup \{1/2 + it : t > 1/2\}$$

tel que l'isomorphisme (1) restreint à $E(\mathbb{R})$ soit défini sur $\mathbb{C}$ et il existe un unique τ appartenant à l'ensemble

$$\mathcal{F} = \{it : t > 0\} \cup \{1/2 + it : t > 0\}$$

tel que l'isomorphisme (1) restreint à $E(\mathbb{R})$ soit défini sur $\mathbb{R}$ et en composant cet isomorphisme avec l'application $z \mapsto e^{2i\pi z}$ on a un isomorphisme analytique $E(\mathbb{R}) \to \mathbb{R}^*/q_\tau^{\mathbb{Z}}$, défini sur $\mathbb{R}$.

De plus si on note Δ le discriminant d'un modèle de Weierstrass de E alors $\tau = it$ (resp. $\tau = 1/2 + it$) si $\Delta > 0$ (resp. $\Delta < 0$). Plus précisément, l'étude des variations des invariants j, c_4, c_6 associés à E permet de montrer que

$$\tau = \begin{cases} it & \text{avec } t \geq 1 \text{ si } \Delta > 0,\ c_6 \geq 0, \\ it & \text{avec } t \leq 1 \text{ si } \Delta > 0,\ c_6 \leq 0, \\ 1/2 + it & \text{avec } t \leq \sqrt{3}/6 \text{ si } \Delta < 0,\ c_4 > 0,\ c_6 \leq 0, \\ 1/2 + it & \text{avec } t \geq \sqrt{3}/6 \text{ si } (\Delta < 0,\ c_4 > 0,\ c_6 \geq 0) \\ & \text{ou } (\Delta < 0,\ c_4 \leq 0). \end{cases}$$

D'autre part, l'homomorphisme b de (2) vérifie (*cf. loc. cit.*, cor. 2.3.1, p. 420)

$$b(E(\mathbb{R})) = \begin{cases} \{0, 1/2\} & \text{si } \Delta > 0, \\ \{0\} & \text{si } \Delta < 0. \end{cases}$$

Soit alors $P \in E(\mathbb{R}) - \{0\}$. Posons $z = z(P) = a + b\tau$ avec $a, b \in \mathbb{R}/\mathbb{Z}$. La formule (3) s'écrit alors sous l'une ou l'autre des deux formes (4) ou (5) suivantes selon que $b = 0$ ou $b = 1/2$:

$$h_\infty(P) = -\frac{1}{12} \log|q_\tau| - \log|1 - e^{2i\pi a}| - \sum_{n \geq 1} \log|(1 - q_\tau^n e^{2i\pi a})(1 - q_\tau^n e^{-2i\pi a})|, \tag{4}$$

$$h_\infty(P) = \frac{1}{24}\log|q_\tau| - \log|1 - q_\tau^{1/2}e^{2i\pi a}| - \sum_{n\geq 1}\log|(1-q_\tau^{n+1/2}e^{2i\pi a})(1-q_\tau^{n-1/2}e^{-2i\pi a})|. \tag{5}$$

THÉORÈME 1. *Soit E une courbe elliptique sur $\mathbb{R}$. On suppose que son invariant modulaire j est $\neq 0, 1728$. On note Δ le discriminant d'un modèle de Weierstrass de E et c_4, c_6 les invariants $c_4(E), c_6(E)$. Pour tout point P de $E(\mathbb{R}) - \{0\}$ on a*

$$\sup_{1\leq k\leq n} h_\infty(kP) > 0 \quad où \quad n = \begin{cases} 6 & si\ \Delta > 0,\ c_6 > 0, \\ 8 & si\ \Delta > 0,\ c_6 < 0, \\ 9 & si\ \Delta < 0,\ c_4 > 0,\ c_6 < 0, \\ 5 & si\ (\Delta < 0,\ c_4 > 0,\ c_6 > 0) \\ & ou\ (\Delta < 0, c_4 < 0). \end{cases}$$

Selon le signe de Δ, c_4 et c_6, les résultats énoncés dans ce théorème seront démontrés séparément dans les propositions 1.4–1.7 ci-dessous. Pour la proposition 1.4 on aura besoin des lemmes suivants :

LEMME 1.1. *La fonction θ définie sur $]0, e^{-\pi/\sqrt{3}}[$ par*

$$\theta(x) = \frac{1}{24} - \sum_{n\geq 1}\frac{(2n-1)x^{2n-2}}{1+x^{2n-1}}$$

est strictement décroissante et s'annule pour $x = e^{-\pi}$.

Démonstration. Il est clair que θ est strictement décroissante. Montrons que $\theta(e^{-\pi}) = 0$. Pour tout nombre complexe τ de partie imaginaire > 0, la série d'Eisenstein E_2 est définie par

$$E_2(\tau) = 1 - 24\sum_{n\geq 1}\frac{nq^n}{1-q^n}$$

où $q = e^{2i\pi\tau}$ et elle vérifie l'équation fonctionnelle ([Se], p. 96)

$$E_2(\tau) = \frac{1}{\tau^2}\left(E_2\left(\frac{-1}{\tau}\right) + \frac{6i\tau}{\pi}\right),$$

ce qui permet de déduire que $E_2(i) = 3/\pi$ et pour $\tau_0 = 1/2 + i/2$ on a $E_2(-1/\tau_0) = E_2(-1+i) = E_2(i)$ et par suite

$$E_2(\tau_0) = \frac{2}{i}\left(\frac{3}{\pi} + \frac{6i}{\pi}\cdot\frac{1+i}{2}\right) = \frac{6}{\pi}.$$

D'autre part, en séparant les termes d'indices pairs et ceux d'indices impairs

dans E_2, on a

$$E_2(\tau) = 1 - 24\sum_{n\geq 1}\frac{(2n-1)q^{2n-1}}{1-q^{2n-1}} - 24\sum_{n\geq 1}\frac{(2n)q^{2n}}{1-q^{2n}}$$
$$= 1 - 24\sum_{n\geq 1}\frac{(2n-1)q^{2n-1}}{1-q^{2n-1}} - 2(1-E_2(2\tau)).$$

Appliquons cette égalité à $\tau = \tau_0$. Puisque $E_2(2\tau_0) = E_2(1+i) = E_2(i) = 3/\pi$ on a

$$\frac{6}{\pi} = 1 + 24\sum_{n\geq 1}\frac{(2n-1)e^{-(2n-1)\pi}}{1-e^{-(2n-1)\pi}} - 2\left(1-\frac{3}{\pi}\right) = -24\theta(e^{-\pi}) + \frac{6}{\pi},$$

d'où $\theta(e^{-\pi}) = 0$ et le lemme.

LEMME 1.2. *L'application φ qui à $\tau = 1/2 + it$ avec $t \geq \sqrt{3}/6$ associe le réel*

$$\varphi(\tau) = -\frac{1}{12}\log|q| - \log\prod_{n\geq 1}(1+q^{2n}-q^n)$$

où $q = e^{2i\pi\tau}$, atteint son minimum en $\tau_0 = 1/2 + i\sqrt{3}/6$ et ce minimum est égal à 0.

Démonstration. Posons $\Delta(\tau) = q\prod_{n\geq 1}(1-q^n)^{24}$. On a alors

$$\varphi(\tau) = -\frac{1}{12}\log|q| - \log\prod_{n\geq 1}\frac{(1-q^{6n})(1-q^n)}{(1-q^{3n})(1-q^{2n})}$$
$$= -\frac{1}{24}\log|q|^2\prod_{n\geq 1}\left(\frac{(1-q^{6n})(1-q^n)}{(1-q^{3n})(1-q^{2n})}\right)^{24}$$
$$= -\frac{1}{24}\log\left|\frac{\Delta(6\tau)\Delta(\tau)}{\Delta(3\tau)\Delta(2\tau)}\right|.$$

La dérivée par rapport à q de $\log|\Delta(\tau)|$ est égale à

$$\frac{1}{q}\left(1 - 24\sum_{n\geq 1}\frac{nq^n}{1-q^n}\right) = \frac{1}{q}E_2(\tau)$$

où E_2 est la série d'Eisenstein définie dans la preuve du lemme 1.1. La dérivée par rapport à q de $\varphi(\tau)$ est donc

$$\frac{\partial\varphi(\tau)}{\partial q} = -\frac{1}{24}(6E_2(6\tau) - 3E_2(3\tau) - 2E_2(2\tau) + E_2(\tau)).$$

Il est bien connu que la fonction qui à $\tau = 1/2 + it$ associe $E_2(\tau)$ décroît de $E_2(1/2 + i\sqrt{3}/2) = 2\pi/\sqrt{3}$ à 1 quand t varie de $\sqrt{3}/2$ à $+\infty$, et la fonction

qui à $\tau = it$ associe $E_2(\tau)$ croît de $-\infty$ à 1 quand t varie de 0 à $+\infty$. Dans notre cas $\tau = 1/2 + it$ avec $t \geq \sqrt{3}/6$. Donc

$$\begin{aligned} E_2(6\tau) &= E_2(6it) > E_2(i) = 3/\pi, \\ E_2(2\tau) &= E_2(2it) < 1, \\ E_2(3\tau) &= E_2(1/2 + it) \leq E_2(1/2 + i\sqrt{3}/2) = 2\sqrt{3}/\pi, \\ E_2(\tau) &> 0. \end{aligned}$$

La dernière inégalité découle du fait que la somme $\sum_{n\geq 1} nq^n/(1-q^n)$ est strictement négative puisque ses termes sont alternés et sont de valeur absolue strictement décroissante comme il résulte des inégalités suivantes et du fait que $|q| \leq e^{-\pi/\sqrt{3}}$:

$$\left|\frac{(n+1)|q|^{n+1}}{1-|q|^{n+1}}\right| \cdot \left|\frac{1-|q|^n}{n|q|^n}\right| = \left(1+\frac{1}{n}\right)|q|\left|\frac{1-q^n}{1-q^{n+1}}\right| \leq 2|q|\frac{1+|q|}{1-|q|} < 1.$$

Il résulte que $\partial\varphi(\tau)/\partial q > 0$ et donc que le minimum de φ est atteint en τ_0. Calculons $\varphi(\tau_0)$. La fonction Δ est une forme modulaire de poids 12. Il s'ensuit que $\Delta(2\tau_0) = (i\sqrt{3})^{12}\Delta(6\tau_0)$ et $\Delta(3\tau_0) = \tau_0^{12}\Delta(\tau_0)$ et donc que $\varphi(\tau_0) = 0$ car

$$\frac{\Delta(6\tau_0)\Delta(\tau_0)}{\Delta(3\tau_0)\Delta(2\tau_0)} = (i\sqrt{3}\,\tau_0)^{-12} = \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^{-12} = 1.$$

LEMME 1.3. *Quand le couple* (q,a) *décrit* $]-5+\sqrt{24}, 0[\times]0, 1/2]$ *on a*

$$\psi(q,a) := \frac{1}{8} + \sum_{n\geq 1} \frac{q^n \sin^2 \pi a}{1 + q^{2n} - 2q^n \cos 2\pi a} > 0.$$

Démonstration. La série

$$S(a) = \sum_{n\geq 1} \frac{q^n}{1 + q^{2n} - 2q^n \cos 2\pi a}$$

est du signe de son premier terme (donc < 0) car ses termes (u_n) sont alternés et sont de valeur absolue strictement décroissante comme il résulte des inégalités suivantes :

$$\left|\frac{u_{n+1}}{u_n}\right| \leq |q|\frac{(1+|q|^n)^2}{(1-|q|^{n+1})^2} \leq |q|\frac{(1+|q|)^2}{(1-|q|^2)^2} = \frac{|q|}{(1-|q|)^2} < 1.$$

Il s'ensuit que la fonction $a \mapsto \sin^2 \pi a \cdot S(a)$ est décroissante (comme produit d'une fonction croissante positive et d'une fonction décroissante négative), d'où

$$\psi(q,a) \geq \psi\left(q, \frac{1}{2}\right) = \frac{1}{8} + \sum_{n\geq 1} \frac{q^n}{(1+q^n)^2} > \frac{1}{8} + \frac{q}{(1+q)^2} = \frac{q^2+10q+1}{8(1+q)^2} > 0.$$

PROPOSITION 1.4. *Soit E une courbe elliptique définie sur $\mathbb{R}$. On suppose que son invariant modulaire j est $\neq 0, 1728$. Si $\Delta < 0$, $c_4 > 0$, $c_6 > 0$ ou si $\Delta < 0$, $c_4 < 0$ alors pour tout point $P \in E(\mathbb{R}) - \{0\}$ on a*

$$h_\infty(P) > -0.35, \tag{6}$$

$$\sup_{1 \le k \le 5} h_\infty(kP) > 0. \tag{7}$$

Démonstration. Ici E est isomorphe, sur $\mathbb{R}$, à $R^*/q_\tau^{\mathbb{Z}}$ où $\tau = 1/2 + it$ avec $t > \sqrt{3}/6$. On pose $q = q_\tau$ pour simplifier. On a alors $-e^{-\pi/\sqrt{3}} < q < 0$ et pour tout point $P \in E(\mathbb{R})$ on a par l'isomorphisme (1), $z(P) = a \in]0, 1]$, donc $h_\infty(P)$ est donné par (4) et est donc égale à la fonction

$$f(q,a) = -\frac{1}{12}\log|q| - \log 2 - \log\sin\pi a - \log\prod_{n\ge 1}(1 + q^{2n} - 2q^n\cos 2\pi a) \tag{8}$$

et puisque $f(q,a) = f(q, 1-a)$ on peut restreindre a à l'intervalle $]0, 1/2]$.

Pour montrer (7) il suffit de minorer $f(q,a)$ quand le couple (q,a) décrit $]-e^{-\pi/\sqrt{3}}, 0[\times]0, 1/6]$ car l'un des réels $z(kP)$ pour $1 \le k \le 5$ est dans $]0, 1/6]$. Or, on a

$$\frac{\partial}{\partial a} f(q,a) = -8\pi(\operatorname{cotg}\pi a)\psi(q,a)$$

où

$$\psi(q,a) = \frac{1}{8} + \sum_{n\ge 1} \frac{q^n \sin^2 \pi a}{1 + q^{2n} - 2q^n \cos 2\pi a}$$

est la fonction définie au lemme 1.3. Et par la preuve de ce même lemme on a

$$\psi(q,a) \ge \psi\left(q, \frac{1}{6}\right) > \psi\left(q, \frac{1}{4}\right) > \frac{1}{8} + \frac{q}{2(1+q^2)} = \frac{q^2 + 4q + 1}{8(1+q^2)} > 0.$$

Il s'ensuit que $\frac{\partial}{\partial a} f(q,a) < 0$ et que pour q fixé on a

$$\min_{0 < a \le 1/6} f(q,a) = f\left(q, \frac{1}{6}\right) = -\frac{1}{12}\log|q| - \log\prod_{n\ge 1}(1 + q^{2n} - q^n).$$

Par le lemme 1.2 on a $f(q, 1/6) \ge 0$, ce qui prouve (7).

Pour montrer (6) on va minorer $f(q,a)$ quand le couple (q,a) décrit $]-5 + \sqrt{24}, 0[\times]0, 1/2]$ puis quand le couple (q,a) décrit l'ensemble $]-e^{-\pi/\sqrt{3}}, -5 + \sqrt{24}[\times]0, 1/2]$. Prenons le premier cas. On a encore

$$\begin{aligned}\min_{0 < a \le 1/2} f(q,a) = f\left(q, \frac{1}{2}\right) &= -\frac{1}{12}\log|q| - \log 2 - \log\prod_{n\ge 1}(1 + q^n)^2 \\ &= -\frac{1}{12}\log|q| - \log 2 + 2\log\prod_{n\ge 1}(1 + |q|^{2n-1})\end{aligned}$$

et

$$\frac{\partial}{\partial q} f\left(q, \frac{1}{2}\right) = -\frac{1}{12q} - 2\sum_{n\geq 1} \frac{(2n-1)q^{2n-2}}{1-q^{2n-1}}$$
$$= -\frac{2}{q}\left(\frac{1}{24} - \sum_{n\geq 1} \frac{(2n-1)|q|^{2n-1}}{1+|q|^{2n-1}}\right) = -\frac{2}{q}\theta(|q|)$$

où θ est la fonction définie au lemme 1.1. Et par ce même lemme on a alors

$$\min_{-5+\sqrt{24}<q<0} f(q,1/2) = f(-e^{-\pi}, 1/2)$$
$$= \frac{\pi}{12} - \log 2 + 2\log \prod_{n\geq 1}(1+e^{-(2n-1)\pi}) > -0.35.$$

Reste à montrer que $f(q,a) > -0.35$ quand $(q,a) \in]-e^{-\pi/\sqrt{3}}, -5+\sqrt{24}[\times]0, 1/2]$. Pour cela on commence par minorer $f(q,a)$ par la fonction $g(q,a)$ obtenue en isolant le premier terme du produit intervenant dans (8) et en minorant le reste du produit par sa valeur en $a = 1/2$. On a alors $f(q,a) > g(q,a)$ où

$$g(q,a) = -\frac{1}{12}\log|q| - \log 2 - \log((\sin \pi a)(1+q^2-2q\cos 2\pi a))$$
$$- \log \prod_{n\geq 2}(1+q^n)^2$$

et donc

$$\frac{\partial}{\partial a} g(q,a) = 0 \;\Leftrightarrow\; \sin^2 \pi a = \frac{(1-q)^2}{-12q},$$
$$\frac{(1-q)^2}{-12q} < 1 \;\Leftrightarrow\; q^2 + 10q + 1 < 0,$$
$$-e^{-\pi/\sqrt{3}} < q < -5+\sqrt{24} \;\Rightarrow\; q^2 + 10q + 1 < 0.$$

Il existe alors un unique $a_0 \in]0, 1/2[$ tel que $\frac{\partial}{\partial a} g(q, a_0) = 0$ et on a

$$\min_{0<a<1/2} g(q,a) = g(q,a_0)$$
$$= -\frac{1}{12}\log|q| - \log 2 - \log\frac{(1-q)^3}{3\sqrt{-3q}} - \log\prod_{n\geq 2}(1+q^n)^2.$$

On sait que la fonction

$$\alpha(q) := -\frac{1}{12}\log|q| - \log 2 - \log\prod_{n\geq 2}(1+q^n)^2$$

est décroissante en q et un calcul simple montre que la fonction

$$\beta(q) := -\log\frac{(1-q)^3}{3\sqrt{-3q}}$$

est croissante en q. Sachant que $-e^{-\pi/\sqrt{3}} \simeq -0.163$ et $-5+\sqrt{24} \simeq -1.101$ on a

$$\min_{-e^{-\pi/\sqrt{3}}<q\le -0.13} g(q,a_0) = \alpha(-0.13)+\beta(-e^{-\pi/\sqrt{3}}) > -0.35,$$

$$\min_{-0.13<q\le -5+\sqrt{24}} g(q,a_0) = \alpha(-5+\sqrt{24})+\beta(-0.13) > -0.35.$$

Ceci achève la preuve de la proposition 1.4.

PROPOSITION 1.5. *Soit E une courbe elliptique définie sur $\mathbb{R}$. On suppose que son invariant modulaire j est $\neq 0, 1728$. Si $\Delta > 0$, $c_6 > 0$ alors pour tout point $P \in E(\mathbb{R}) - \{0\}$ on a*

$$\sup_{1\le k\le 2} h_\infty(kP) > -0.174 \quad \textit{et} \quad \sup_{1\le k\le 6} h_\infty(kP) > 0. \tag{9}$$

Démonstration. Dans ce cas E est isomorphe, sur $\mathbb{R}$, à $\mathbb{R}^*/q_\tau^{\mathbb{Z}}$ où $\tau = it$ avec $t > 1$. On a donc $0 < q := q_\tau < e^{-2\pi}$ et par l'isomorphisme (1), $z(P) = a(P)+b(P)\tau$ avec $b(P) = 0$ ou $1/2$ et si $b(P) = 1/2$ alors $b(2P) = 0$. Donc pour montrer la première inégalité de (9), il suffit de minorer la fonction $f(q,a)$ donnée par (8) quand (q,a) décrit $]0, e^{-2\pi}[\times]0, 1/2[$, et pour montrer la deuxième inégalité, il suffit de minorer $f(q,a)$ quand (q,a) décrit $]0, e^{-2\pi}[\times]0, 1/4[$ car si $z(P) = a \in]0, 1/2[$ alors l'un des trois points $P, 2P, 3P$ est tel que $z(kP) \in]0, 1/4[$. La proposition découle alors de la décroissance de $f(q,a)$ en a et en q et du fait que $f(e^{-2\pi}, 1/2) > -0.174$ et $f(e^{-2\pi}, 1/4) > 0.177$.

PROPOSITION 1.6. *Soit E une courbe elliptique définie sur $\mathbb{R}$. On suppose que son invariant modulaire j est $\neq 0, 1728$. Si $\Delta < 0$, $c_4 > 0$, $c_6 < 0$ alors pour tout point $P \in E(\mathbb{R}) - \{0\}$ on a*

$$\sup_{1\le k\le 9} h_\infty(kP) > 0.$$

Démonstration. Dans ce cas E est isomorphe sur $\mathbb{R}$, à $\mathbb{R}^*/q_\tau^{\mathbb{Z}}$ où $\tau = 1/2 + it$ avec $t < \sqrt{3}/6$. L'application $z \mapsto z/(2\tau - 1)$ définit un isomorphisme φ de $E(\mathbb{C})$ sur $\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau'$ où $\tau' = (\tau-1)/(2\tau-1)$. On a $\tau' = 1/2+it'$ avec $t' > \sqrt{3}/2$. Soit $P \in E(\mathbb{R})$. On peut supposer que $\varphi(P)$ est égal à la classe d'un nombre complexe de la forme ibt' avec $-1 < b \le 1$. Et comme h_∞ est paire on peut restreindre b à l'intervalle $]0, 1]$. Posons $q = q_{\tau'} = e^{2i\pi\tau'}$. On a $-e^{-\pi\sqrt{3}} < q < 0$, $q_z = e^{2i\pi z} = |q|^b$ et $h_\infty(P)$ est égale à la fonction

$$f(q,b) = -\frac{1}{2}B_2(b)\log|q| - \log(1-|q|^b) - \log\prod_{n\ge 1}(1-q^n|q|^b)(1-q^n|q|^{-b}).$$

Il suffit de minorer $f(q,b)$ pour $(q,b) \in]-e^{-\pi\sqrt{3}}, 0[\times]0, 1/5]$ puisque l'un des neuf points $\varphi(kP)$ pour $1 \le k \le 9$ est égal à la classe d'un nombre complexe de la forme ibt' avec $b \in]0, 1/5]$.

La dérivée par rapport à b de $f(q,b)$ est

$$\frac{\partial}{\partial b}f(q,b) = -\frac{1}{2}(2b-1)\log|q| + \frac{|q|^b}{1-|q|^b}\log|q| + (|q|^b - |q|^{-b})\log|q|\sum_{n\geq 1}u_n(q,b)$$

où

$$u_n(q,b) = \frac{q^n}{(1-q^n|q|^b)(1-q^n|q|^{-b})}.$$

La série alternée $\sum_{n\geq 1}u_n(q,b)$ est négative (comme son premier terme) car la suite $|u_n(q,b)|$ tend vers 0 en décroissant comme le montre les inégalités suivantes :

$$\frac{|u_{n+1}(q,b)|}{|u_n(q,b)|} \leq |q|\frac{(1+|q|^{n+b})(1+|q|^{n-b})}{(1-|q|^{n+1+b})(1-|q|^{n+1-b})} \leq |q|\frac{2(1+|q|)}{(1-|q|)^2} < 1.$$

Il s'ensuit que

$$\begin{aligned}\min_{0<b\leq 1/5} f(q,b) &= f(q,1/5)\\ &= -\frac{1}{300}\log|q| - \log(1-|q|^{1/5})\\ &\quad - \log\prod_{n\geq 1}(1-q^n|q|^{1/5})(1-q^n|q|^{-1/5})\\ &\geq \frac{\pi\sqrt{3}}{300} + \sum_{n\geq 1}\frac{|q|^{n/5}}{n} - \sum_{n\geq 1}\log(1+|q|^{n+1/5})(1+|q|^{n-1/5})\\ &\geq \sum_{n\geq 1}\frac{|q|^{n/5} - 2n|q|^{n-1/5}}{n} > 0.\end{aligned}$$

Proposition 1.7. *Soit E une courbe elliptique définie sur $\mathbb{R}$. On suppose que son invariant modulaire j est $\neq 0, 1728$. Si $\Delta > 0$, $c_6 < 0$ alors pour tout point $P \in E(\mathbb{R}) - \{0\}$ on a*

$$\sup_{1\leq k\leq 8} h_\infty(kP) > 0.$$

Démonstration. Dans ce cas E est isomorphe, sur $\mathbb{R}$, à $\mathbb{R}^*/q_\tau^{\mathbb{Z}}$ où $\tau = it$ avec $t < 1$. L'application $z \mapsto z/\tau$ définit un isomorphisme φ défini sur $\mathbb{C}$, de $E(\mathbb{C})$ sur $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau'$ où $\tau' = -1/\tau$. On $\tau' = it'$ avec $t' > 1$. Soit $P \in E(\mathbb{R})$ et soit z un nombre complexe dont la classe est $\varphi(P)$. On peut choisir $z = a + b\tau'$ avec $a = 0$ ou $1/2$ et $0 < b \leq 1$. Posons $q = q_{\tau'} = e^{2i\pi\tau'}$. On a $0 < q < e^{-2\pi}$. Si $a = 0$ alors $q_z = e^{2i\pi z} = q^b$ et $h_\infty(P)$ est égale à la fonction

$$f(q,b) = -\frac{1}{2}B_2(b)\log q - \log(1-q^b) - \log\prod_{n\geq 1}(1-q^{n-b})(1-q^{n+b}).$$

Si $a = 1/2$ alors en considérant $2P$ on se ramène au cas $a = 0$. D'autre part, puisque $f(q,b) = f(q,1-b)$, on peut restreindre b à l'intervalle $]0,1/2]$. Enfin, pour montrer la proposition il suffit de minorer $f(q,b)$ pour $(q,b) \in]0,e^{-2\pi}[\times]0,1/5]$ puisque l'un des quatres points $\varphi(kP)$ pour $1 \leq k \leq 4$ est égal à la classe d'un nombre complexe de la forme $b\tau'$ avec $b \in [-1/5,1/5]$ et on utilise le fait que h_∞ est paire. Pour $(q,b) \in]0,e^{-2\pi}[\times]0,1/5]$ on a

$$f(q,b) > -\frac{1}{2}B_2(1/5)\log e^{-2\pi} = \frac{\pi}{150} > 0.$$

2. La hauteur de Néron–Tate. Soit E une courbe elliptique définie sur $\mathbb{Q}$ dont un modèle de Weierstrass minimal à coefficients entiers est

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{10}$$

Notons Δ_E son discriminant. Soit p un nombre premier. On note E_p la cubique (éventuellement singulière) dont une équation est obtenue en réduisant (10) modulo p et on note $E_0(\mathbb{Q}_p)$ le sous-groupe de $E(\mathbb{Q}_p)$ formé des points qui se réduisent modulo p en un point non singulier de E_p. La hauteur locale en la place p est une fonction $h_p : E(\mathbb{Q}_p) - \{0\} \to \mathbb{R}$. Sa valeur en un point $P = (x,y) \in E_0(\mathbb{Q}_p) - \{0\}$ est donnée par (*cf.* [Si2], th. 4.1, p. 470)

$$h_p(P) = \sup\left(-\frac{1}{2}v_p(x), 0\right) + \frac{1}{12}v_p(\Delta_E)\log p \tag{11}$$

où v_p est la valuation p-adique de $\mathbb{Q}_p$, normalisée par $v_p(p) = 1$.

La hauteur de Néron–Tate associée au diviseur (0) sur E est une forme quadratique $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}$, définie positive sur $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Sa valeur en un point P non nul est

$$\widehat{h}(P) = h_\infty(P) + \sum_p h_p(P). \tag{12}$$

Proposition 2.1. *Soit E une courbe elliptique sur $\mathbb{Q}$, d'invariant modulaire $j \neq 0, 1728$ et de discriminant minimal Δ_E. Soit P un point d'ordre infini de $E(\mathbb{Q})$. Si P appartient à $E_0(\mathbb{Q}_p)$ pour tout nombre premier p, on a*

$$\widehat{h}(P) > \frac{1}{12n^2}\log|\Delta_E| \tag{13}$$

où n est l'entier défini au théorème 1. *En particulier, on a*

$$\widehat{h}(P) > \frac{1}{972}\log|\Delta_E|. \tag{14}$$

Démonstration. Par (11) on a $h_p(P) \geq \frac{1}{12}v_p(\Delta_E)\log p$ pour tout nombre premier p et par le théorème 1, on a $\sup_{1\leq k\leq n} h_\infty(kP) > 0$. Il s'ensuit en

utilisant (12) que

$$n^2\widehat{h}(P) = \sup_{1\le k\le n} \widehat{h}(kP) > \frac{1}{12}\sum_p v_p(\Delta_E)\log p = \frac{1}{12}\log|\Delta_E|$$

et puisque $n \le 9$ on a l'inégalité (14).

Pour tout nombre premier p divisant Δ_E (*i.e.* E a mauvaise réduction en p) notons c_p le plus petit entier > 0 qui annule $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. L'entier c_p est déterminé par l'algorithme de Tate ([Ta] ou [Si2], p. 364). On a

$$c_p = \begin{cases} 1,2 & \text{si } E \text{ a en } p \text{ mauvaise réduction} \\ & \text{multiplicative non décomposée,} \\ v_p(\Delta_E) & \text{si } E \text{ a en } p \text{ mauvaise réduction} \\ & \text{multiplicative décomposée,} \\ 1,2,3,4 & \text{si } E \text{ a en } p \text{ mauvaise réduction} \\ & \text{de type additive,} \end{cases} \tag{15}$$

et posons

$$C_E = \mathrm{ppcm}(c_p). \tag{16}$$

Pour tout point P d'ordre infini de $E(\mathbb{Q})$, le point $C_E P$ appartient à $E_0(\mathbb{Q}_p)$ pour tout nombre premier p. Le corollaire suivant est une conséquence immédiate de la proposition 2.1.

Corollaire 2.2. *Pour toute courbe elliptique E sur $\mathbb{Q}$, d'invariant modulaire $j \neq 0, 1728$ et pour tout point P d'ordre infini de $E(\mathbb{Q})$ on a*

$$\widehat{h}(P) > \frac{1}{972C_E^2}\log|\Delta_E|. \tag{17}$$

La proposition qui suit précise la constante C dans la conjecture de Lang pour certaines familles de courbes elliptiques sur $\mathbb{Q}$: ce sont les courbes pour lesquelles on a des informations sur la constante C_E définie ci-dessus.

Proposition 2.3. *Soit E une courbe elliptique sur $\mathbb{Q}$ d'invariant modulaire $j \neq 0, 1728$ et de discriminant minimal Δ_E. Pour tout point P d'ordre infini de $E(\mathbb{Q})$ on a*

$$\widehat{h}(P) > C\log|\Delta_E|$$

où

$$C = \begin{cases} 10^{-3} & \textit{si } \Delta_E \textit{ est sans facteurs carrés,} \\ 10^{-5} & \textit{si le conducteur de } E \textit{ est un nombre premier,} \\ 10^{-6} & \textit{si l'invariant modulaire } j \textit{ de } E \textit{ est un nombre entier.} \end{cases}$$

Démonstration. Dans ces trois cas on sait calculer la constante C_E et on utilise (17).

1) Si Δ_E est sans facteurs carrés alors toute mauvaise réduction de E est de type multiplicatif et on a donc $C_E = 1$.

2) Si le conducteur de E est un nombre premier p alors $\Delta_E = \pm p^m$ où m est un entier ≥ 1. Et d'après Mestre et Oesterlé [M-O], on a $m \leq 5$ car E est semi-stable sur $\mathbb{Q}$. Aussi la (seule) mauvaise réduction de E est en p et elle est de type multiplicatif. Donc $C_E = m \leq 5$.

3) Si j est un nombre entier alors E n'a de réduction de type multiplicatif en aucun nombre premier p et donc C_E est un diviseur de 12 d'après (15).

On passe maintenant à l'étude des cas particuliers où $j = 0$ ou 1728.

3. Le cas $j = 0$: la courbe d'équation $y^2 = x^3 + d$. Soit E une courbe elliptique sur $\mathbb{Q}$ d'invariant $j = 0$. Il existe un entier non nul d tel qu'une équation de Weierstrass de E soit de la forme

$$y^2 = x^3 + d.$$

Le discriminant de E est $\Delta = -2^4 \cdot 3^3 \cdot d^2$. Les invariants c_4 et c_6 attachés à E sont $c_4 = 0$ et $c_6 = -2^5 \cdot 3^3 \cdot d$. La courbe E est isomorphe sur $\mathbb{R}$ à $\mathbb{R}^*/q^{\mathbb{Z}}$ où $q = e^{2i\pi\tau}$ avec $\tau = 1/2 + i\sqrt{3}/6$ (resp. $\tau = 1/2 + i\sqrt{3}/2$) si $d > 0$ (resp. $d < 0$).

PROPOSITION 3.1. *Soit d un entier non nul sans facteurs sixièmes. Soit E la courbe elliptique sur $\mathbb{Q}$ d'équation $y^2 = x^3 + d$ et soit P un point d'ordre infini de $E(\mathbb{Q})$. On a*

$$\widehat{h}(P) > 10^{-3} \log |d| + 10^{-3}.$$

Démonstration. 1) On commence par minorer $h_\infty(P)$. Pour tout point $P \in E(\mathbb{R}) - \{0\}$ on a

$$h_\infty(P) > c \quad \text{où} \quad c = \begin{cases} -0.35 & \text{si } d > 0, \\ -0.25 & \text{si } d < 0. \end{cases}$$

En effet, l'expression de $h_\infty(P)$ est donné par l'égalité (8) dans laquelle on peut restreindre le réel a à l'intervalle $]0, 1/2]$ et où $q = -e^{-\pi/\sqrt{3}}$ si $d > 0$ et $q = -e^{-\pi\sqrt{3}}$ si $d < 0$. L'inégalité (6) est encore valable dans le cas présent aussi bien dans le cas $d > 0$ que dans le cas $d < 0$ (voir la preuve de (6)) et on a donc $h_\infty(P) > -0.35$, pour tout point $P \in E(\mathbb{R}) - \{0\}$. Remarquons aussi que dans le cas où $d < 0$ on peut obtenir un minorant meilleur que celui dans (6). En effet, on a

$$\begin{aligned} h_\infty(P) &= \frac{\pi\sqrt{3}}{12} - \log 2 - \log \sin \pi a - \log \prod_{n \geq 1} (1 + q^{2n} - 2q^n \cos 2\pi a) \\ &\geq \frac{\pi\sqrt{3}}{12} - \log 2 - 2 \log \prod_{n \geq 1} (1 + e^{-\pi n\sqrt{3}}) > -\frac{1}{4}. \end{aligned}$$

2) Si P appartient à $E_0(\mathbb{Q}_p)$ pour tout nombre premier p alors

$$\widehat{h}(P) = h_\infty(P) + \sum_p h_p(P) > c + \frac{1}{12}\sum_p v_p(\Delta)\log p$$
$$= c + \frac{4}{12}\log 2 + \frac{3}{12}\log 3 + \frac{2}{12}\log|d| > \frac{1}{6}\log|d| + c'$$

où

$$c' = \begin{cases} 0.15 & \text{si } d > 0, \\ 0.25 & \text{si } d < 0. \end{cases}$$

3) Enfin, par l'algorithme de Tate ([Ta]) l'ordre c_p de $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ vaut $1, 2, 3$ ou 4 si $p \neq 2, 3$. Pour $p = 2$, si 2 ne divise pas d ou si 2 divise exactement d alors la réduction de E en 2 est du type II et donc $c_2 = 1$. Enfin si 2^2 divise d alors $c_2 = 2, 3$ ou 4. Pour $p = 3$, si 3 ne divise pas d ou si 3 divise exactement d alors $c_3 = 1$. Si 3^2 divise d et 3^4 ne divise pas d alors $c_3 = 1$ ou 3. Enfin, si 3^4 divise d alors $c_3 = 1, 2, 3$ ou 4. Il s'ensuit que le point $12P$ appartient à $E_0(\mathbb{Q}_p)$ pour tout nombre premier p. Et puisque $144\widehat{h}(P) = \widehat{h}(12P)$ on a

$$\widehat{h}(P) > \frac{1}{864}\log|d| + \frac{c'}{144} > 10^{-3}\log|d| + 10^{-3}.$$

Remarque 3.2. Si d est sans facteurs carrés alors pour tout nombre premier p, l'entier c_p défini en (15) est égal à 1, donc la constante C_E définie en (16) vaut aussi 1 et par suite pour tout point d'ordre infini de $E(\mathbb{Q})$ on a

$$\widehat{h}(P) > \frac{1}{6}\log|d| + c'.$$

4. Le cas $j = 1728$: la courbe d'équation $y^2 = x^3 + dx$. Soit E une courbe elliptique sur $\mathbb{Q}$ d'invariant $j = 1728$. Il existe un entier non nul d tel qu'une équation de Weierstrass de E soit de la forme

$$y^2 = x^3 + dx.$$

Le discriminant de E est $\Delta = -2^6 \cdot d^3$. Les invariants c_4 et c_6 attachés à E sont $c_4 = -2^4 \cdot 3 \cdot d$ et $c_6 = 0$. La courbe E est isomorphe sur $\mathbb{R}$ à $\mathbb{R}^*/q^{\mathbb{Z}}$ où $q = e^{2i\pi\tau}$ avec $\tau = 1/2 + i/2$ (resp. $\tau = i$) si $d > 0$ (resp. $d < 0$).

Proposition 4.1. *Soit d un entier impair sans facteurs quatrièmes. Soit E la courbe elliptique d'équation $y^2 = x^3 + dx$. Soit P un point d'ordre infini de $E(\mathbb{Q})$. On a*

$$\widehat{h}(P) > \frac{1}{64}\log|d|.$$

Démonstration. 1) Pour tout point P de $E(\mathbb{R}) - \{0\}$ on a

$$\begin{cases} h_\infty(P) > -0.345 & \text{si } d > 0, \\ \sup(h_\infty(P), h_\infty(2P)) > -0.18 & \text{si } d < 0. \end{cases}$$

En effet, si $d > 0$, on a $q = -e^{-\pi}$ et pour tout point P de $E(\mathbb{R}) - \{0\}$, on a, par l'isomorphisme (1) $z(P) = a \in]0, 1]$ et $h_\infty(P)$ est donné par la fonction $f(q, a)$ en (8) et on peut encore restreindre a à l'intervalle $]0, 1/2]$. Le résultat est alors un cas particulier de l'inégalité (6) de la proposition 1.4. Cependant on doit raffiner un peu le minorant de (6) pour ne pas trouver des constantes négatives dans le minorant de $\widehat{h}(P)$ (voir ci-dessous). En fait on a (voir le début de la preuve de (6))

$$h_\infty(P) > f(-e^{-\pi}, 1/2) = \frac{\pi}{12} - \log 2 + 2 \log \prod_{n \geq 1} (1 + e^{-(2n-1)\pi}) > -0.345.$$

Si $d < 0$, alors $q = e^{-2\pi}$ et par l'isomorphisme (1), on a pour tout point P de $E(\mathbb{R}) - \{0\}$, $z(P) = a$ ou $a + i/2$ avec $a \in]0, 1/2]$.

Si $z(P) = a$ alors

$$\begin{aligned} h_\infty(P) &= \frac{\pi}{6} - \log 2 - \log \sin \pi a - \log \prod_{n \geq 1} (1 + q^{2n} - 2q^n \cos 2\pi a) \\ &\geq \frac{\pi}{6} - \log 2 - 2 \log \prod_{n \geq 1} (1 + e^{-2\pi n}) > -0.18. \end{aligned}$$

Si $z(P) = a + i/2$. En considérant $2P$ on est dans le cas précédent. Donc $h_\infty(2P) > -0.18$. On peut donc dire que dans tous les cas ($d < 0$ ou $d > 0$) on a $h_\infty(2P) > -0.345$.

2) D'après l'algorithme de Tate [Si2, p. 364], la réduction de E en un nombre premier $p \neq 2$ est de type I_0, auquel cas $c_p = 1$, si p ne divise pas d, et est de type III, I_0^* ou III^* respectivement si p, p^2 ou p^3 divise exactement d, auxquels cas c_p vaut respectivement 2, (2 ou 4), ou 4. En $p = 2$ la réduction de E est de type III, auquel cas $c_2 = 2$, si 2 ne divise pas d, et est de type III, I_n^* ou III^* respectivement si 2, 2^2 ou 2^3 divise exactement d, auxquels cas c_2 vaut respectivement 1, (2 ou 4), ou 2. Il s'ensuit que $4P$ appartient à $E_0(\mathbb{Q}_p)$ pour tout nombre premier p et donc

$$\begin{aligned} \widehat{h}(P) &> \frac{1}{16} \left(h_\infty(4P) + \frac{6}{12} \log 2 + \frac{3}{12} \log |d| \right) \\ &> \frac{1}{16} \left(-0.345 + 0.346 + \frac{1}{4} \log |d| \right) > \frac{1}{64} \log |d|. \end{aligned}$$

Remarque 4.2. Si d est sans facteurs carrés alors pour tout nombre premier p divisant d, l'entier c_p défini en (15) est égal à 2, donc la constante C_E définie en (16) vaut aussi 2 et par suite pour tout point d'ordre infini de $E(\mathbb{Q})$ on a

$$\widehat{h}(P) > \frac{1}{16} \log |d|.$$

Références

[B-S-T] A. Bremner, J. H. Silverman and N. Tzanakis, *Integral points in arithmetic progression on* $y^2 = x(x^2 - n^2)$, J. Number Theory 80 (2000), 187–208.

[H-S] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450.

[La] S. Lang, *Elliptic Curves*: *Diophantine Analysis*, Springer, 1978.

[M-O] J. F. Mestre et J. Oesterle, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. 400 (1989), 173–184.

[Se] J. P. Serre, *A Course in Arithmetic*, Springer, 1973.

[Si1] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. 48 (1981), 633–648.

[Si2] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[Sin1] D. Sinou, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory 64 (1997), 104–129.

[Sin2] —, *Minorations de hauteurs sur les variétés abéliennes*, Bull. Soc. Math. France 121 (1993), 509–544.

[Sin3] —, *Autour d'une conjecture de S. Lang*, dans : Approximations diophantiennes et nombres transcendants (Luminy, 1990), de Gruyter, Berlin, 1992, 65–98.

[Ta] J. Tate, *Algorithm for determining the type of singular fiber in an elliptic pencil*, dans: Lecture Notes in Math. 467, Springer, 1975, 33–52.

Laboratoire de Mathématiques
UMR 8100
Bâtiment Fermat
Université de Versailles
45 Avenue des Etats-Unis
F-78035 Versailles Cedex, France
E-mail: krir@math.uvsq.fr

Reçu le 17.4.1998
et révisé le 2.4.2001 (3366)