Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron–Tate sur les courbes elliptiques sur $\overline{\mathbf{Q}}$

Peter Bruin

Résumé. Nous donnons un algorithme qui, étant donnée une courbe elliptique E sur $\overline{\mathbf{Q}}$ sous la forme de Weierstraß, calcule l'infimum et le supremum de la différence entre la hauteur naïve et la hauteur canonique sur $E(\overline{\mathbf{Q}})$.

Abstract. We give an algorithm that, given an elliptic curve E over $\overline{\mathbf{Q}}$ in Weierstraß form, computes the infimum and supremum of the difference between the naïve and canonical height functions on $E(\overline{\mathbf{Q}})$.

1. Introduction

Soit E une courbe elliptique sur $\overline{\mathbf{Q}}$ donnée par une équation de Weierstraß :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

On supposera toujours que *les a_i soient des entiers algébriques*.

On s'intéresse à la hauteur de Weil (ou hauteur naïve) et la hauteur de Néron–Tate (ou hauteur canonique)

$$h, \hat{h} : E(\overline{\mathbf{Q}}) \to \mathbf{R}$$

(voir ci-dessous pour les normalisations). La différence $h-\hat{h}$ est bornée sur $E(\overline{\mathbf{Q}})$. Il est donc naturel de se demander si, étant donnée une équation (1.1), on peut calculer le supremum et l'infimum de cette différence.

Des résultats dans cette direction ont été obtenus par Dem′janenko [3] et Zimmer [11], Silverman [6], Siksek [5], Cremona, Prickett et Siksek [2], et Uchida [10]. Le lecteur est renvoyé à l'introduction de [2] pour plus de détails.

1.1. Notations

Dans cet article, étant donné un corps de nombres K, on fixe les notations suivantes :

Ω_K, Ω_K^{fin}, Ω_K^{inf}	l'ensemble des places de K, resp. des places finies, resp. des places infinies
$\mathbf{Z}_K$	l'anneau des entiers de K

Pour chaque place v :

$\vert\ \vert_v$	la valeur absolue normalisée sur K correspondant à v
K_v	le complété v-adique de K
ϵ_v	le degré local $[K_v : \mathbf{Q}_p]$, où p est la place de $\mathbf{Q}$ au-dessous de v

Pour chaque place finie v :

$\mathfrak{p}_v$	l'idéal maximal $\{x \in \mathbf{Z}_K \mid \vert x\vert_v < 1\}$ de $\mathbf{Z}_K$
k_v	le corps résiduel $\mathbf{Z}_K/\mathfrak{p}_v$

Soit E est une courbe elliptique sur $\overline{\mathbf{Q}}$ donnée par une équation (1.1). On définit les coefficients b_2, b_4, b_6, c_4, c_6, le discriminant Δ_E et l'invariant j_E par les formules usuelles ; voir par example Tate [9, § 2].

1.2. Hauteurs

La hauteur (logarithmique normalisée) d'un point $x = (x_0 : \ldots : x_n) \in \mathbf{P}^n(\overline{\mathbf{Q}})$ est définie comme suit : soit $K \subset \overline{\mathbf{Q}}$ un corps de nombres contenant les x_i, alors

$$h_{\mathbf{P}^n}(x) = \frac{1}{[K : \mathbf{Q}]} \sum_{v\in\Omega_K} \log\max\{|x_0|_v, \ldots, |x_n|_v\}.$$

Mathematics Subject Classification (2010) : 11G05, 11G50, 11Y35

L'auteur a bénéficié du soutien financier du Fonds national suisse (subsides nos. 124737 et 137920) et de l'hospitalité du Max-Planck-Institut für Mathematik, Bonn.

On sait que le membre de droite est invariant par extension du corps K, de sorte que $h_{\mathbf{P}^n}$ est une fonction bien définie sur $\mathbf{P}^n(\overline{\mathbf{Q}})$.

Soit E une courbe elliptique sur $\overline{\mathbf{Q}}$ donnée par une équation de Weierstraß (1.1), et soit $P \in E(\overline{\mathbf{Q}})$. La *hauteur de Weil* (ou *hauteur naïve*) de P est définie par

$$h(P) = h_{\mathbf{P}^1}(x(P)).$$

La *hauteur de Néron–Tate* (ou *hauteur canonique*) de P est définie par

$$\hat{h}(P) = \lim_{n\to\infty} n^{-2} h(nP).$$

Notre fonction $\hat{h}$ coïncide avec celle utilisée dans l'article de Cremona, Prickett et Siksek [2] ; elle est double de celle utilisée dans l'article [6] et le livre [7] de Silverman.

2. La différence $h - \hat{h}$

Soit E une courbe elliptique sur $\overline{\mathbf{Q}}$ donnée par une équation de Weierstraß (1.1), et soit $P \in E(\overline{\mathbf{Q}})$.

2.1. Hauteurs locales

Soit $K \subset \overline{\mathbf{Q}}$ un corps de nombres tel que E soit définie sur K. Alors on a des hauteurs locales

$$\lambda_v : E(K_v) \to \mathbf{R} \quad \text{pour tout } v \in \Omega_K$$

et une décomposition de $\hat{h}$ en termes locaux

$$[K : \mathbf{Q}]\hat{h}(P) = 2 \sum_{v\in\Omega_K} \epsilon_v \lambda_v(P) \quad \text{pour tout } P \in E(K).$$

La normalisation des λ_v que nous utiliserons est celle du livre de Silverman [7, Chapter VI].

Pour $v \in \Omega_K$ et $P \in E(K_v)$, notons

$$\phi_v(P) = \epsilon_v^{-1} \log \max\bigl\{1, |x(P)|_v\bigr\} - 2\lambda_v(P).$$

Alors on a

$$\begin{aligned} [K : \mathbf{Q}]\bigl(h(P) - \hat{h}(P)\bigr) &= \sum_{v\in\Omega_K} \bigl(\log \max\bigl\{1, |x(P)|_v\bigr\} - 2\epsilon_v\lambda_v(P)\bigr) \\ &= \sum_{v\in\Omega_K} \epsilon_v \phi_v(P). \end{aligned}$$

2.2. Le discriminant stable

Quitte à élargir K, on peut supposer que E ait réduction semi-stable. Pour toute place finie v de K, on note n_v le nombre de composantes géométriques irréductibles de la réduction de E modulo v ; cette réduction est donc un n_v-gone. On note $\Delta^{\min}_{E/K}$ le discriminant minimal de E sur K, c'est-à-dire l'idéal de $\mathbf{Z}_K$ défini par

$$\Delta^{\min}_{E/K} = \prod_{v\in\Omega_K^{\mathrm{fin}}} \mathfrak{p}_v^{n_v}.$$

La norme $\operatorname{Nm} \Delta^{\min}_{E/K}$ de cet idéal satisfait à

$$\log \operatorname{Nm} \Delta^{\min}_{E/K} = \sum_{v\in\Omega_K^{\mathrm{fin}}} n_v \log \#k_v.$$

On définit

$$\Delta^{\mathrm{stable}}_E = (\operatorname{Nm} \Delta^{\min}_{E/K})^{1/[K:\mathbf{Q}]}.$$

On note que $\Delta^{\mathrm{stable}}_E$ ne dépend pas du choix de K et peut être calculé à partir de la factorisation (ou l'idéal dénominateur) de j_E dans n'importe quel corps de nombres contenant j_E ; il n'est pas nécessaire de connaître un corps K sur lequel E a réduction semi-stable.

2.3. Le théorème principal

Théorème 2.1 (cf. Cremona, Prickett et Siksek [2, Theorem 1]). *Soit E une courbe elliptique sur $\overline{\mathbf{Q}}$ donnée par une équation de Weierstraß à coefficients algébriquement entiers. Alors pour tout corps de nombres $K \subset \overline{\mathbf{Q}}$ tel que E soit définie sur K, on a*

$$[K:\mathbf{Q}] \inf_{P\in E(\overline{\mathbf{Q}})} (h(P) - \hat{h}(P)) = \sum_{v\in\Omega_K^{\inf}} \epsilon_v \inf_{E(\bar{K}_v)} \phi_v - \frac{1}{6}\log|\mathrm{N}_{K/\mathbf{Q}}\Delta_E|,$$

$$[K:\mathbf{Q}] \sup_{P\in E(\overline{\mathbf{Q}})} (h(P) - \hat{h}(P)) = \sum_{v\in\Omega_K^{\inf}} \epsilon_v \sup_{E(\bar{K}_v)} \phi_v + \frac{[K:\mathbf{Q}]}{12}\log \Delta_E^{\mathrm{stable}}.$$

Preuve. Quitte à élargir K, on peut supposer que K soit totalement complexe, que E ait réduction semi-stable scindée sur K et que tous les n_v soient pairs. Pour chaque place finie v de K, l'hypothèse que le modèle de Weierstraß soit entier par rapport à v implique

$$\begin{aligned} \inf_{E(K_v)} \phi_v &= \frac{1}{6\epsilon_v}\log|\Delta_E|_v, \\ \sup_{E(K_v)} \phi_v &= -\frac{1}{12\epsilon_v}\log|\Delta_{E/K}^{\min}|_v; \end{aligned} \tag{2.1}$$

voir [2, Proposition 8]. (Dans loc. cit. les résultats sont donnés en termes de la fonction $\Psi_v(P) = \epsilon_v\phi_v(P) + \frac{1}{6}\log|\Delta_E|_v$.) On en déduit que

$$\begin{aligned} [K:\mathbf{Q}](h(P)-\hat{h}(P)) &\geq \sum_{v\in\Omega_K^{\inf}} \epsilon_v \inf_{E(K_v)} \phi_v - \frac{1}{6}\log|\mathrm{N}_{K/\mathbf{Q}}\Delta_E|, \\ [K:\mathbf{Q}](h(P)-\hat{h}(P)) &\leq \sum_{v\in\Omega_K^{\inf}} \epsilon_v \sup_{E(K_v)} \phi_v + \frac{1}{12}\log \mathrm{Nm}\,\Delta_{E/K}^{\min} \\ &= \sum_{v\in\Omega_K^{\inf}} \epsilon_v \sup_{E(K_v)} \phi_v + \frac{[K:\mathbf{Q}]}{12}\log \Delta_E^{\mathrm{stable}}. \end{aligned}$$

Il reste à démontrer que ces bornes *localement* optimales donnent des bornes *globalement* optimales. À cet effet, on utilise l'approximation sur $\mathbf{P}^1$. Pour chaque place finie v, la fonction ϕ_v atteint son maximum aux points de $E(K_v)$ dont la x-coordonnée est dans un certain ouvert non vide U_v de $\mathbf{P}^1(K_v)$; de plus, on a $U_v = \mathbf{P}^1(K_v)$ pour toutes les $v \in \Omega_K^{\mathrm{fin}}$ sauf un nombre fini. De façon analogue, pour chaque place infinie (complexe) v et tout $\epsilon > 0$, la fonction ϕ_v sur $E(K_v)$ est ϵ-proche de son supremum sur l'ensemble des points dont la x-coordonnée est dans un certain ouvert non vide U_v de $\mathbf{P}^1(K_v)$. Par approximation, il existe $x_\epsilon \in \mathbf{P}^1(K)$ dont l'image dans $\mathbf{P}^1(K_v)$ est dans U_v pour toute place v. Soit $P_\epsilon \in E(\overline{\mathbf{Q}})$ un point avec $x(P_\epsilon) = x_\epsilon$. (On remarquera que P_ϵ est défini sur un extension quadratique de K.) En faisant $\epsilon \to 0$, on obtient une suite de points P_ϵ pour lesquels $h(P_\epsilon) - \hat{h}(P_\epsilon)$ converge vers la borne supérieure désirée. Le même argument marche pour la borne inférieure. □

Vu le théorème 2.1, il reste à étudier les fonctions ϕ_v sur $E(\bar{K}_v)$ pour v une place archimédienne.

3. Préliminaires sur les réseaux

Soit Λ un réseau dans $\mathbf{C}$. On note

$$\mathrm{vol}_\Lambda = \frac{i}{2}\int_{\mathbf{C}/\Lambda} dz \wedge \bar{d}z.$$

Soit $\mu_\Lambda^{\mathrm{can}}$ la $(1,1)$-forme canonique sur $\mathbf{C}/\Lambda$, définie par

$$\mu_\Lambda^{\mathrm{can}} = \frac{1}{\mathrm{vol}_\Lambda}\frac{i}{2} dz \wedge d\bar{z}.$$

Rappelons la définition des fonctions σ, ζ et $\wp$ de Weierstraß :

$$\sigma_\Lambda(z) = z \prod_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right),$$

$$\zeta_\Lambda(z) = \frac{\sigma'_\Lambda}{\sigma_\Lambda}(z) = \frac{1}{z} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right),$$

$$\wp_\Lambda(z) = -\zeta'_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

On rappelle que la fonction $\wp_\Lambda$ est périodique par rapport à Λ, et que la fonction ζ_Λ est quasi-périodique : il existe un homomorphisme

$$\eta_\Lambda : \Lambda \to \mathbf{C}$$

tel que

$$\zeta_\Lambda(z+\omega) = \zeta_\Lambda(z) + \eta_\Lambda(\omega) \quad \text{pour tout } \omega \in \Lambda.$$

Soient $g_2(\Lambda)$ et $g_3(\Lambda)$ les nombres complexes tels que

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda),$$

et soit

$$\Delta_\Lambda = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2.$$

Soit $Q_\Lambda : \mathbf{C} \to \mathbf{R}$ l'unique forme $\mathbf{R}$-quadratique satisfaisant à

$$Q_\Lambda(\omega) = \Re(\omega \cdot \eta_\Lambda(\omega)) \quad \text{pour tout } \omega \in \Lambda.$$

On considère la fonction

$$\begin{aligned} \lambda_\Lambda : \mathbf{C}/\Lambda \setminus \{0\} &\longrightarrow \mathbf{R} \\ z &\longmapsto -\log|\sigma_\Lambda(z)| + \frac{1}{2} Q_\Lambda(z) - \frac{1}{12}\log|\Delta_\Lambda|. \end{aligned}$$

Cette fonction est lisse sur $\mathbf{C}/\Lambda \setminus \{0\}$ et possède une singularité logarithmique en 0. Elle satisfait à l'équation différentielle

$$2i\partial\bar{\partial}\lambda_\Lambda = 2\pi(\mu_\Lambda^{\mathrm{can}} - \delta_0)$$

avec la normalisation

$$\int_{\mathbf{C}/\Lambda} \lambda_\Lambda \mu_\Lambda^{\mathrm{can}} = 0.$$

Comme λ_Λ prend des valeurs réelles, il existe une unique fonction lisse (mais non holomorphe) $Z_\Lambda : \mathbf{C}/\Lambda \setminus \{0\} \to \mathbf{C}$ telle que

$$d\lambda_\Lambda(z) = -\frac{1}{2}\big(Z_\Lambda(z)dz + \overline{Z_\Lambda(z)}d\bar{z}\big). \tag{3.1}$$

Il existe $C_\Lambda \in \mathbf{C}$ et $D_\Lambda \in \mathbf{R}$ tels que

$$Q_\Lambda(z) = \frac{C_\Lambda}{2} z^2 + \frac{\bar{C}_\Lambda}{2}\bar{z}^2 + D_\Lambda z\bar{z}$$

et donc

$$Z_\Lambda(z) = \zeta_\Lambda(z) - C_\Lambda z - D_\Lambda \bar{z}.$$

Soit (ω_1, ω_2) une $\mathbf{Z}$-base de Λ avec $\Im(\omega_1/\omega_2) > 0$. Alors on a

$$\mathrm{vol}_\Lambda = \Im(\omega_1 \bar{\omega}_2).$$

On pose

$$\begin{aligned} \eta_1 &= \eta_\Lambda(\omega_1) = 2\zeta_\Lambda(\omega_1/2), \\ \eta_2 &= \eta_\Lambda(\omega_2) = 2\zeta_\Lambda(\omega_2/2). \end{aligned}$$

En utilisant la relation de Legendre

$$\eta_2\omega_1 - \eta_1\omega_2 = 2\pi i,$$

il est facile de montrer que

$$\begin{aligned} C_\Lambda &= \frac{\eta_1\bar{\omega}_2 - \eta_2\bar{\omega}_1}{2i\,\mathrm{vol}_\Lambda}, \\ D_\Lambda &= \frac{\pi}{\mathrm{vol}_\Lambda}. \end{aligned}$$

4. Étude des fonctions ϕ_v aux places archimédiennes

Soit K un corps de nombres, et soit E une courbe elliptique sur K donnée par une équation de Weierstraß (1.1). Soit v une place archimédienne de K. On fixe un plongement $K \to \mathbf{C}$ correspondant à v, et on regarde E comme courbe elliptique sur $\mathbf{C}$ au moyen de ce plongement.

Soit $\Lambda_v \subset \mathbf{C}$ le réseau des périodes de E par rapport à la 1-forme standard $dx/(2y + a_1x + a_3)$ du modèle de Weierstraß donné. On note $\wp_v$ la fonction de Weierstraß relative au réseau Λ_v, vue comme fonction méromorphe sur $\mathbf{C}/\Lambda_v$. Pour $P \in E(\mathbf{C})$, on note z_P le point correspondant de $\mathbf{C}/\Lambda_v$. Alors on a

$$\wp_v(z_P) = x(P) + \frac{b_2}{12}.$$

De plus, on a

$$g_2(\Lambda_v) = \frac{c_4}{12}, \quad g_3(\Lambda_v) = \frac{c_6}{216}.$$

On note

$$\lambda_v(z) = \lambda_{\Lambda_v}(z).$$

La fonction λ_v est la hauteur locale à la place v ; voir Silverman [7, Theorem VI.3.2].

La fonction ϕ_v est donnée par

$$\phi_v(z) = \log\max\left\{1, \left|\wp_v(z) - \frac{b_2}{12}\right|\right\} - 2\lambda_v(z) \quad \text{pour tout } z \in \mathbf{C}/\Lambda_v.$$

Soient $t_1, t_2 \in \mathbf{C}/\Lambda_v$ les zéros de la fonction $\wp_v(z) - \frac{b_2}{12}$; on a $t_1 + t_2 = 0$. Alors les deux fonctions $\log\left|\wp_v(z) - \frac{b_2}{12}\right|$ et $2\lambda_v(z) - \lambda_v(z - t_1) - \lambda_v(z - t_2)$ ont même image sous l'opérateur laplacien, à savoir $2\pi(\delta_{t_1} + \delta_{t_2} - 2\delta_0)$. Il s'ensuit que

$$\log\left|\wp_v(z) - \frac{b_2}{12}\right| = 2\lambda_v(z) - \lambda_v(z - t_1) - \lambda_v(z - t_2) + I_v,$$

où

$$I_v = \int_{\mathbf{C}/\Lambda_v} \log\left|\wp_v(z) - \frac{b_2}{12}\right|\mu^{\mathrm{can}}_{\Lambda_v}.$$

Cela implique

$$\phi_v(z) = \begin{cases} -\lambda_v(z - t_1) - \lambda_v(z - t_2) + I_v & \text{si } \left|\wp_v(z) - \frac{b_2}{12}\right| \geq 1, \\ -2\lambda_v(z) & \text{si } \left|\wp_v(z) - \frac{b_2}{12}\right| \leq 1. \end{cases} \tag{4.1}$$

On pose

$$S = \left\{ z \in \mathbf{C}/\Lambda_v \;\middle|\; \left|\wp_v(z) - \frac{b_2}{12}\right| = 1 \right\}.$$

On peut utiliser (4.1) pour calculer $\phi_v(z)$. La constante I_v peut être déterminée en comparant les deux expressions pour $\phi_v(z)$ pour n'importe quel $z \in S$.

En utilisant les formules (4.1) et (3.1), on voit que la dérivée de ϕ_v est donnée par

$$d\phi_v(z) = W_v(z)dz + \overline{W_v(z)}d\bar{z} \quad \text{pour} \quad \left|\wp_v(z) - \frac{b_2}{12}\right| \neq 1, \tag{4.2}$$

où W_v est la fonction continue sur $\mathbf{C}/\Lambda_v \setminus S$ définie par

$$W_v(z) = \begin{cases} \frac{1}{2}\big(Z_{\Lambda_v}(z-t_1) + Z_{\Lambda_v}(z-t_2)\big) & \text{si } \left|\wp_v(z) - \frac{b_2}{12}\right| > 1, \\ Z_{\Lambda_v}(z) & \text{si } \left|\wp_v(z) - \frac{b_2}{12}\right| < 1. \end{cases}$$

Lemme 4.1. *La dérivée de Z_{Λ_v} est*

$$dZ_{\Lambda_v}(z) = \big(-\wp_v(z) - C_{\Lambda_v}\big)dz - D_{\Lambda_v}d\bar{z}.$$

La dérivée de $\frac{1}{2}\big(Z_{\Lambda_v}(z-t_1) + Z_{\Lambda_v}(z-t_2)\big)$ est

$$d\left(\frac{1}{2}\big(Z_{\Lambda_v}(z-t_1) + Z_{\Lambda_v}(z-t_2)\big)\right) = \left(-C_{\Lambda_v} - \frac{b_2}{12} - \frac{1}{2}\frac{b_4}{\wp_v(z) - \frac{b_2}{12}} - \frac{1}{2}\frac{b_6}{(\wp_v(z) - \frac{b_2}{12})^2}\right)dz - D_\Lambda d\bar{z}.$$

Preuve. La première partie suit de la définition de Z_{Λ_v} et du fait que $\zeta'_{\Lambda_v}(z) = -\wp_v(z)$.

En remplaçant z par $z - t$, on obtient

$$dZ_{\Lambda_v}(z-t) = \big(-\wp_v(z-t) - C_{\Lambda_v}\big)dz - D_{\Lambda_v}d\bar{z},$$

de sorte que

$$\frac{1}{2}d\big(Z_{\Lambda_v}(z-t_1) + Z_{\Lambda_v}(z-t_2)\big) = \left(-\frac{\wp_v(z-t_1) + \wp_v(z-t_2)}{2} - C_{\Lambda_v}\right)dz - D_{\Lambda_v}d\bar{z}.$$

La loi d'addition permet d'exprimer $\wp_v(z-t_1) + \wp_v(z-t_2)$ en $\wp_v(z)$ et $\wp_v(t_1) = \wp_v(t_2) = \frac{b_2}{12}$ comme suit :

$$\begin{aligned}
\wp_v(z-t_1) + \wp_v(z-t_2) &= \frac{4\frac{b_2}{12}\wp_v(z)(\wp_v(z) + \frac{b_2}{12}) - g_2(\Lambda_v)(\wp_v(z) + \frac{b_2}{12}) - 2g_3(\Lambda_v)}{2(\wp_v(z) - \frac{b_2}{12})^2} \\
&= \frac{b_2}{6} + \frac{12(\frac{b_2}{12})^2 - g_2(\Lambda_v)}{2(\wp_v(z) - \frac{b_2}{12})} + \frac{4(\frac{b_2}{12})^3 - g_2(\Lambda_v)\frac{b_2}{12} - g_3(\Lambda_v)}{(\wp_v(z) - \frac{b_2}{12})^2} \\
&= \frac{b_2}{6} + \frac{12(\frac{b_2}{12})^2 - \frac{c_4}{12}}{2(\wp_v(z) - \frac{b_2}{12})} + \frac{4(\frac{b_2}{12})^3 - \frac{c_4}{12}\frac{b_2}{12} - \frac{c_6}{216}}{(\wp_v(z) - \frac{b_2}{12})^2} \\
&= \frac{b_2}{6} + \frac{b_4}{\wp_v(z) - \frac{b_2}{12}} + \frac{b_6}{(\wp_v(z) - \frac{b_2}{12})^2}.
\end{aligned}$$

Ceci implique la deuxième partie. □

On note que W_v est harmonique, de sorte que pour borner W_v sur $\mathbf{C}/\Lambda_v \setminus S$, il suffit de borner les fonctions $Z_{\Lambda_v}(z)$ et $\frac{1}{2}\big(Z_{\Lambda_v}(z-t_1) + Z_{\Lambda_v}(z-t_2)\big)$ sur S. Pour chacune de ces deux fonctions, le lemme suivant donne une majoration de sa valeur absolue sur S à partir d'une seule évaluation et d'une majoration de quelques nombres réels associés à E.

Lemme 4.2. *Pour tout $p, q \in S$, on a*

$$\begin{aligned}
\big|Z_{\Lambda_v}(q)\big| &\leq \big|Z_{\Lambda_v}(p)\big| + M_1 J, \\
\left|\frac{1}{2}\big(Z_{\Lambda_v}(q-t_1) + Z_{\Lambda_v}(q-t_2)\big)\right| &\leq \left|\frac{1}{2}\big(Z_{\Lambda_v}(p-t_1) + Z_{\Lambda_v}(p-t_2)\big)\right| + M_2 J,
\end{aligned}$$

où

$$\begin{aligned}
M_1 &= \left|C_{\Lambda_v} + \frac{b_2}{12}\right| + |D_{\Lambda_v}| + 1,\\
M_2 &= \left|C_{\Lambda_v} + \frac{b_2}{12}\right| + |D_{\Lambda_v}| + \frac{|b_4|}{2} + \frac{|b_6|}{2},\\
J &= \int_0^{2\pi} \frac{d\theta}{|4\exp(3i\theta) + b_2\exp(2i\theta) + 2b_4\exp(i\theta) + b_6|^{1/2}}.
\end{aligned}$$

Preuve. Quitte à remplacer p par $-p$ (ce qui a pour effet de multiplier $Z_{\Lambda_v}(p)$ par -1), on peut supposer qu'il existe un chemin γ de p à q dans S tel que la fonction $\wp_v(z) - \frac{b_2}{12}$ identifie γ avec un segment du cercle unité dans $\mathbf{C}$. On a

$$\begin{aligned}
Z_{\Lambda_v}(q) &= Z_{\Lambda_v}(p) + \int_\gamma dZ_{\Lambda_v}\\
&= Z_{\Lambda_v}(p) - \int_\gamma \big((\wp_v(z) + C_{\Lambda_v})dz + D_{\Lambda_v} d\bar{z}\big).
\end{aligned}$$

Pour tout $z \in S$, le lemme 4.1 implique

$$\begin{aligned}
|\wp_v(z) + C_{\Lambda_v}| &\le \left|\wp_v(z) - \frac{b_2}{12}\right| + \left|C_{\Lambda_v} + \frac{b_2}{12}\right|\\
&= 1 + \left|C_{\Lambda_v} + \frac{b_2}{12}\right|.
\end{aligned}$$

On en déduit que

$$|Z_{\Lambda_v}(q)| \le |Z_{\Lambda_v}(p)| + M_1 \int_\gamma |dz|.$$

De façon analogue, on obtient

$$\left|\frac{1}{2}\big(Z_{\Lambda_v}(q-t_1) + Z_{\Lambda_v}(q-t_2)\big)\right| \le \left|\frac{1}{2}\big(Z_{\Lambda_v}(p-t_1) + Z_{\Lambda_v}(p-t_2)\big)\right| + M_2\int_\gamma |dz|.$$

En utilisant la formule

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

on montre facilement que

$$\begin{aligned}
\int_\gamma |dz| &\le \int_{|x|=1} \frac{|dx|}{|2y + a_1x + a_3|}\\
&= \int_0^{2\pi} \frac{d\theta}{|4\exp(3i\theta) + b_2\exp(2i\theta) + 2b_4\exp(i\theta) + b_6|^{1/2}}\\
&= J.
\end{aligned}$$

Ceci complète la démonstration. □

Corollaire 4.3. *Soit p un point quelconque de S. Pour tout $z \in \mathbf{C}/\Lambda_v \setminus S$, on a*

$$|W_v(z)| \le \max\left\{\big|Z_{\Lambda_v}(p)\big| + M_1 J, \left|\frac{1}{2}\big(Z_{\Lambda_v}(p-t_1) + Z_{\Lambda_v}(p-t_2)\big)\right| + M_2 J\right\}.$$

Les résultats suivants ne sont pas strictement nécessaires, mais permettent d'obtenir un algorithme plus efficace ci-dessous.

Lemme 4.4. *Soit R un sous-ensemble convexe de $\mathbf{C}$.*
(a) Si $|\wp_v(z) - \frac{b_2}{12}| < 1$ pour tout $z \in R$, on a

$$|W_v(z) - W_v(z_0)| \leq \left(\left|C_{\Lambda_v} + \frac{b_2}{12}\right| + |D_{\Lambda_v}| + 1\right)|z - z_0| \quad \textit{pour tout } z, z_0 \in R.$$

(b) Si $|\wp_v(z) - \frac{b_2}{12}| > 1$ pour tout $z \in R$, on a

$$|W_v(z) - W_v(z_0)| \leq \left(\left|C_{\Lambda_v} + \frac{b_2}{12}\right| + |D_{\Lambda_v}| + \frac{|b_4| + |b_6|}{2}\right)|z - z_0| \quad \textit{pour tout } z, z_0 \in R.$$

Preuve. Dans chacun des deux cas, la fonction W_v est différentiable sur R, et il suffit de borner sa dérivée. Le lemme 4.1 implique que pour $|\wp_v(z) - \frac{b_2}{12}| \leq 1$, on a

$$\begin{aligned}|\wp_v(z) + C_{\Lambda_v}| &\leq \left|\wp_v(z) - \frac{b_2}{12}\right| + \left|C_{\Lambda_v} + \frac{b_2}{12}\right| \\ &\leq 1 + \left|C_{\Lambda_v} + \frac{b_2}{12}\right|.\end{aligned}$$

Pour $|\wp_v(z) - \frac{b_2}{12}| \geq 1$, le lemme 4.1 implique

$$\left|\frac{\wp_v(z - t_1) + \wp_v(z - t_2)}{2} + C_{\Lambda_v}\right| \leq \left|C_{\Lambda_v} + \frac{b_2}{12}\right| + \frac{|b_4|}{2} + \frac{|b_6|}{2},$$

ce qui complète la démonstration. □

On considère maintenant des parallélogrammes de la forme

$$R(z_0, z_1, z_2) = \left\{z_0 + s_1 z_1 + s_2 z_2 \mid s_1, s_2 \in \left[-\tfrac{1}{2}, \tfrac{1}{2}\right]\right\}$$

pour $z_0, z_1, z_2 \in \mathbf{C}$ tels que z_1 et z_2 sont $\mathbf{R}$-linéairement indépendants. On note

$$\begin{aligned}d(z_1, z_2) &= \sup_{z \in R(z_0, z_1, z_2)} |z - z_0| \\ &= \frac{1}{2}\max\{|z_1 - z_2|, |z_1 + z_2|\}.\end{aligned}$$

Corollaire 4.5. *Soit $R = R(z_0, z_1, z_2)$ comme ci-dessus.*
(a) Si $|\wp_v(z) - \frac{b_2}{12}| < 1$ pour tout $z \in R$, on a

$$|W_v(z)| \leq |W_v(z_0)| + \left(\left|C_{\Lambda_v} + \frac{b_2}{12}\right| + |D_{\Lambda_v}| + 1\right) d(z_1, z_2) \quad \textit{pour tout } z \in R.$$

(b) Si $|\wp_v(z) - \frac{b_2}{12}| > 1$ pour tout $z \in R$, on a

$$|W_v(z)| \leq |W_v(z_0)| + \left(\left|C_{\Lambda_v} + \frac{b_2}{12}\right| + |D_{\Lambda_v}| + \frac{|b_4| + |b_6|}{2}\right) d(z_1, z_2) \quad \textit{pour tout } z \in R.$$

5. Un algorithme

L'étude de ϕ_v ci-dessus permet de construire un algorithme pour calculer le supremum de ϕ_v avec une précision préscrite ϵ. On a un algorithme complètement analogue pour calculer l'infimum.

Notre algorithme, dont l'idée fondamentale est inspirée de l'algorithme de Cremona, Prickett et Siksek [2, § 9], fonctionne par dichotomie récursive. On commence avec un domaine fondamental $R(0, \omega_1, \omega_2)$, où (ω_1, ω_2) est une $\mathbf{Z}$-base de Λ_v, et on pose $\mu = \phi_v(0)$. À chaque étape, on considère un parallélogramme $R(z_0, z_1, z_2)$. On remplace μ par $\max\{\mu, \phi_v(z_0)\}$, de sorte que μ est toujours la plus grande valeur de ϕ_v qu'on a rencontré jusque-là. De plus, on calcule un majorant M pour la fonction $|W_v|$ sur $R(z_0, z_1, z_2)$ par le corollaire 4.3 ou le corollaire 4.5. Pour tout $z \in R(z_0, z_1, z_2)$, on a par (4.2)

$$\begin{aligned} |\phi_v(z) - \phi_v(z_0)| &\leq 2d(z_1, z_2) \sup_{R(z_0,z_1,z_2)} |W_v| \\ &\leq 2d(z_1, z_2)M. \end{aligned} \tag{5.1}$$

Dans le cas où

$$\phi_v(z_0) + 2d(z_1, z_2)M < \mu + \epsilon,$$

on conclut grâce à (5.1) que ϕ_v est inférieur à $\mu + \epsilon$ sur tout le parallélogramme $R(z_0, z_1, z_2)$. Dans le cas opposé, on coupe $R(z_0, z_1, z_2)$ en deux nouveaux parallélogrammes le long de la droite qui passe par le centre z_0 et qui est parallèle à un côté de longueur minimale de $R(z_0, z_1, z_2)$, et on applique le processus de façon récursive à ces nouveaux parallélogrammes. Il est facile de voir que cet algorithme termine et produit un μ qui satisfait à

$$\sup_{\mathbf{C}/\Lambda_v} \phi_v - \epsilon < \mu \leq \sup_{\mathbf{C}/\Lambda_v} \phi_v.$$

6. Exemples

Voici quelques exemples. Nous avons utilisé PARI/GP [4] pour la plupart des calculs, et Sage [8] pour calculer la hauteur canonique de points définis sur des corps de nombres.

6.1. La courbe 11A3

Cette courbe a un modèle globalement minimal donné par l'équation

$$E : y^2 + y = x^3 - x^2.$$

On a

$$-\Delta_E = \Delta_E^{\text{stable}} = 11.$$

Notre algorithme donne

$$\sup_{E(\mathbf{C})} \phi_v = 0.597\ldots,$$

$$\inf_{E(\mathbf{C})} \phi_v = -0.156\ldots$$

En utilisant le théorème 2.1, on obtient

$$-0.556 < h(P) - \hat{h}(P) < 0.798 \quad \text{pour tout } P \in E(\overline{\mathbf{Q}}).$$

Pour comparaison, la majoration trouvée par l'algorithme de Silverman [6] est

$$h(P) - \hat{h}(P) < 4.695,$$

et celle trouvée par l'algorithme de Cremona, Prickett et Siksek [2] pour les $\mathbf{Q}$-points est

$$h(P) - \hat{h}(P) < 0.300.$$

Par approximation dans $\mathbf{P}^1$ comme dans la preuve du théorème 2.1, on peut trouver des points $P, Q \in E(\overline{\mathbf{Q}})$ tels que $h(P) - \hat{h}(P)$ est très proche de -0.556 et $h(Q) - \hat{h}(Q)$ est très proche de 0.798. On prend

$$\begin{aligned} P &= (-1, \alpha) \quad \text{avec } \alpha^2 + \alpha + 2 = 0, \\ Q &= (37/61, \beta) \quad \text{avec } \beta^2 + \beta + \frac{2^3 \cdot 3 \cdot 37^2}{61^3} = 0. \end{aligned}$$

Le point P est défini sur $\mathbf{Q}(\sqrt{-7})$; le point Q est défini sur $\mathbf{Q}(\sqrt{7 \cdot 11 \cdot 17 \cdot 61 \cdot 73})$. On a

$$\begin{aligned} h(P) &= 0, & \hat{h}(P) &= 0.5556807\ldots, & h(P) - \hat{h}(P) &= -0.5556807\ldots, \\ h(Q) &= \log 61, & \hat{h}(Q) &= 3.3130740\ldots, & h(Q) - \hat{h}(Q) &= 0.7977997\ldots \end{aligned}$$

6.2. La courbe 15A4

Voici un example pour montrer que notre méthode donne parfois une meilleure majoration de $h - \hat{h}$ pour les $\overline{\mathbf{Q}}$-points que celle de Cremona, Prickett et Siksek [2] pour les $\mathbf{Q}$-points.

La courbe 15A4 a un modèle globalement minimal donné par l'équation

$$E : y^2 + xy + y = x^3 + x^2 + 35x - 28.$$

On a

$$-\Delta_E = \Delta_E^{\text{stable}} = 3^2 \cdot 5^8.$$

Notre algorithme donne

$$\inf_{E(\mathbf{C})} \phi_v = 0.584\ldots,$$

$$\sup_{E(\mathbf{C})} \phi_v = 2.512\ldots$$

En utilisant le théorème 2.1, on obtient

$$-1.928 < h(P) - \hat{h}(P) < 3.769 \quad \text{pour tout } P \in E(\overline{\mathbf{Q}}).$$

Pour comparaison, la majoration trouvée par l'algorithme de [2] est

$$h(P) - \hat{h}(P) < 3.915 \quad \text{pour tout } P \in E(\mathbf{Q}).$$

6.3. La courbe 5077A1

Cette courbe, déjà étudiée par Buhler, Gross et Zagier [1], a un modèle globalement minimal donné par l'équation

$$E : y^2 + y = x^3 - 7x + 6$$

On a

$$\Delta_E = \Delta_E^{\text{stable}} = 5077.$$

Notre algorithme donne

$$\inf_{E(\mathbf{C})} \phi_v = 0.217\ldots,$$

$$\sup_{E(\mathbf{C})} \phi_v = 1.422\ldots$$

En utilisant le théorème 2.1, on obtient

$$-1.206 < h(P) - \hat{h}(P) < 2.134 \quad \text{pour tout } P \in E(\overline{\mathbf{Q}}).$$

Des bornes optimales pour les $\mathbf{Q}$-points ont déjà été calculées dans loc. cit. En fait, on a

$$-1.2050811\ldots \leq h(P) - \hat{h}(P) \leq 0 \quad \text{pour tout } P \in E(\mathbf{Q}),$$

où la borne inférieure est atteinte par le point $(-1, 3)$ et la borne supérieure par le point à l'infini.

Par approximation dans $\mathbf{P}^1$, on trouve le point

$$P = (5169, \alpha) \quad \text{avec } \alpha^2 + \alpha - 138108205632 = 0,$$

défini sur $\mathbf{Q}(\sqrt{7 \cdot 5077 \cdot 15544411})$. On a

$$h(P) = \log 5169, \quad \hat{h}(P) = 6.4174217\ldots, \quad h(P) - \hat{h}(P) = 2.1330128\ldots$$

6.4. Une courbe étudiée par Cremona, Prickett et Siksek

Notre dernier exemple est une courbe elliptique de rang 4 sur $\mathbf{Q}$ étudiée par Cremona, Prickett et Siksek dans [2, § 11] :

$$E : y^2 = x^3 - 459x^2 - 3478x + 169057.$$

Cette courbe n'est pas semi-stable sur $\mathbf{Q}$, le conducteur étant $2^2 \cdot 199 \cdot 362793983647$. On a

$$\begin{aligned} \Delta_E &= 2^4 \cdot 199 \cdot 362793983647, \\ \Delta_E^{\text{stable}} &= 199 \cdot 362793983647. \end{aligned}$$

Notre algorithme donne

$$\begin{aligned} \inf_{E(\mathbf{C})} \phi_v &= 0.879\ldots, \\ \sup_{E(\mathbf{C})} \phi_v &= 5.780\ldots \end{aligned}$$

En utilisant le théorème 2.1, on obtient

$$-4.901 < h(P) - \hat{h}(P) < 8.440 \quad \text{pour tout } P \in E(\overline{\mathbf{Q}}).$$

Les bornes trouvées par Cremona, Prickett et Siksek [2] sont

$$-6.532 < h(P) - \hat{h}(P) < 0.4621 \quad \text{pour tout } P \in E(\mathbf{Q}).$$

Ils ont également trouvé un point $P \in E(\mathbf{Q})$ pour lequel

$$h(P) - \hat{h}(P) = -4.9001533\ldots$$

De l'autre côté, le point

$$Q = (-45092013952912, \alpha) \quad \text{avec } \alpha^2 = -199 \cdot 1601 \cdot 22133 \cdot 362793983647 \cdot 35838855272124651419$$

satisfait à

$$h(Q) = 31.4397262\ldots, \quad \hat{h}(Q) = 23.0000267\ldots, \quad h(Q) - \hat{h}(Q) = 8.4396995\ldots$$

Bibliographie

[1] J. P. Buhler, B. H. Gross and D. B. Zagier, On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. *Mathematics of Computation* **44** (1985), 473–481.

[2] J. E. Cremona, M. Prickett and S. Siksek, Height difference bounds for elliptic curves over number fields. *Journal of Number Theory* **116** (2006), no. 1, 42–68.

[3] В. А. Демьяненко, Оценка остаточного члена в формуле Тэйта. *Математические Заметки* **3** (1968), № 3, 271–278.
V. A. Dem′janenko, An estimate of the remainder term in Tate's formula. *Mathematical Notes* **3** (1968), no. 3, 173–177. (English translation.)

[4] The PARI Group, PARI/GP, version 2.6.0. Bordeaux, 2012, `http://pari.math.u-bordeaux.fr/`.

[5] S. Siksek, Infinite descent on elliptic curves. *Rocky Mountain Journal of Mathematics* **25** (1995), no. 4, 1501–1538.

[6] J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of Computation* **55** (1990), 723–743.

[7] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics **151**. Springer-Verlag, New York, 1994.

[8] W. A. Stein et al., Sage Mathematics Software, version 5.2. The Sage Development Team, 2012, `http://www.sagemath.org/`.

[9] J. T. Tate, The arithmetic of elliptic curves. *Inventiones mathematicae* **23** (1974), 179–206.

[10] Y. Uchida, The difference between the ordinary height and the canonical height on elliptic curves. *Journal of Number Theory* **128** (2008), no. 2, 263–279.

[11] H. G. Zimmer, On the difference between the Weil height and the Néron–Tate height. *Mathematische Zeitschrift* **147** (1976), 35–51.

Peter Bruin
Institut für Mathematik
Universität Zürich
Winterthurerstrasse 190
CH-8057 Zürich

`peter.bruin@math.uzh.ch`