ACTA ARITHMETICA
160.4 (2013)

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

par

Peter Bruin (Zürich)

1. Introduction. Soit E une courbe elliptique sur $\overline{\mathbb{Q}}$ donnée par une équation de Weierstraß généralisée :

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

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)

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

voir ci-dessous pour les normalisations. La différence $h - \hat{h}$ est une fonction bornée sur $E(\overline{\mathbb{Q}})$.

Des majorations explicites de $h - \hat{h}$ sont utiles pour calculer des groupes de Mordell–Weil de courbes elliptiques sur les corps de nombres ; voir Silverman [6, Chapter X]. Des méthodes pour borner $h - \hat{h}$ ont été développées par Dem′yanenko [3], Zimmer [12], Silverman [7], Siksek [5], Cremona, Prickett et Siksek [2], et Uchida [11]. Le lecteur est renvoyé à l'introduction de [2] pour plus de détails.

Dans cet article, on décrit un algorithme pour *calculer* le supremum et l'infimum de la fonction $h - \hat{h}$ sur $E(\overline{\mathbb{Q}})$ avec une précision préscrite. On obtient donc des bornes optimales pour $h - \hat{h}$ sur l'ensemble des $\overline{\mathbb{Q}}$-points. Si K est un corps de définition de E, ces bornes ne sont pas en général optimales pour les K-points. Pour certaines courbes, elles améliorent néanmoins les bornes pour les K-points produites par les méthodes existantes.

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

2010 *Mathematics Subject Classification*: 11G05, 11G50, 11Y35.
Key words and phrases: elliptic curves, heights.

DOI: 10.4064/aa160-4-5

Ω_K, Ω_K^{fin}, Ω_K^{inf} l'ensemble de toutes les places de K, resp. des places finies, resp. des places infinies,

$\mathbb{Z}_K$ l'anneau des entiers de K.

Pour chaque place v :

$|\ |_v$ la valeur absolue normalisée sur K correspondant à v,

K_v le complété v-adique de K,

ϵ_v le degré local $[K_v : \mathbb{Q}_p]$, où p est la caractéristique résiduelle de v,

$\mathfrak{p}_v$ l'idéal maximal $\{x \in \mathbb{Z}_K \mid |x|_v < 1\}$ de $\mathbb{Z}_K$ si v est finie.

Soit E une courbe elliptique sur $\overline{\mathbb{Q}}$ donnée par une équation (1.1). On définit les coefficients b_2, b_4, b_6, le discriminant Δ_E et l'invariant j_E par les formules usuelles ; voir par exemple Tate [10, §2].

1.2. Hauteurs. La hauteur (logarithmique) d'un point $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$ est définie comme suit : soit $x = (x_0 : x_1)$ avec x_0 et x_1 dans un corps de nombres $K \subset \overline{\mathbb{Q}}$; alors

$$h_{\mathbb{P}^1}(x) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \Omega_K} \log \max\{|x_0|_v, |x_1|_v\}.$$

Le membre de droite est invariant par extension du corps K et par multiplication des x_i par une constante, de sorte que $h_{\mathbb{P}^1}$ est une fonction bien définie sur $\mathbb{P}^1(\overline{\mathbb{Q}})$.

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

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

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 de l'article de Cremona, Prickett et Siksek [2] ; elle est double de celle utilisée dans l'article [7] et le livre [8] de Silverman.

2. La différence $h - \hat{h}$

2.1. Hauteurs locales. Soit E une courbe elliptique sur $\overline{\mathbb{Q}}$ donnée par une équation de Weierstraß (1.1), et soit $K \subset \overline{\mathbb{Q}}$ un corps de nombres tel que E soit définie sur K. Alors on a des hauteurs locales

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

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

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

La normalisation des λ_v que nous utiliserons est celle du livre de Silverman [8, Chapter VI].

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

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

Alors on a

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

2.2. Le discriminant stable. Soient E et K comme ci-dessus. 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 $\Delta_{E/K}^{\min}$ le discriminant minimal de E sur K, c'est-à-dire l'idéal de $\mathbb{Z}_K$ défini par

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

La norme $\mathrm{Nm}\,\Delta_{E/K}^{\min}$ de cet idéal est donc

$$\mathrm{Nm}\,\Delta_{E/K}^{\min} = \prod_{v\in\Omega_K^{\mathrm{fin}}} (\mathbb{Z}_K : \mathfrak{p}_v)^{n_v}.$$

On définit

$$\Delta_E^{\mathrm{stable}} = (\mathrm{Nm}\,\Delta_{E/K}^{\min})^{1/[K:\mathbb{Q}]}.$$

On note que $\Delta_E^{\mathrm{stable}}$ 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. Formules pour l'infimum et le supremum de $h - \hat{h}$

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

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

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

Démonstration. 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

$$\inf_{E(K_v)} \phi_v = \frac{1}{6\epsilon_v} \log |\Delta_E|_v, \qquad \sup_{E(K_v)} \phi_v = -\frac{1}{12\epsilon_v} \log |\Delta^{\min}_{E/K}|_v; \tag{2.1}$$

voir [2, Proposition 8]. (Dans [2] 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

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

Il reste à démontrer que ces bornes *localement* optimales donnent des bornes *globalement* optimales. À cet effet, on utilise l'approximation sur $\mathbb{P}^1$. Pour toute 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 $\mathbb{P}^1(K_v)$, avec $U_v = \mathbb{P}^1(K_v)$ pour toutes les $v \in \Omega_K^{\mathrm{fin}}$ sauf un nombre fini. De façon analogue, pour toute place infinie (complexe) v et tout $\epsilon > 0$, la fonction ϕ_v sur $E(K_v)$ est ϵ-proche de son supremum aux points de $E(K_v)$ dont la x-coordonnée est dans un certain ouvert non vide U_v de $\mathbb{P}^1(K_v)$. Par approximation, il existe $x_\epsilon \in \mathbb{P}^1(K)$ dont l'image dans $\mathbb{P}^1(K_v)$ est dans U_v pour toute place v. Soit $P_\epsilon \in E(\overline{\mathbb{Q}})$ un point avec $x(P_\epsilon) = x_\epsilon$; on note que P_ϵ est défini sur une 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 $\mathbb{C}$. On note

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

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

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

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

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

La fonction $\wp_\Lambda$ est périodique par rapport à Λ, et la fonction ζ_Λ est quasi-périodique : il existe un homomorphisme $\eta_\Lambda : \Lambda \to \mathbb{C}$ 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

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

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

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

On définit une fonction réelle λ_Λ sur $\mathbb{C}/\Lambda\setminus\{0\}$ par

$$\lambda_\Lambda(z) = -\log|\sigma_\Lambda(z)| + \tfrac{1}{2}Q_\Lambda(z) - \tfrac{1}{12}\log|\Delta_\Lambda|.$$

Cette fonction est lisse sur $\mathbb{C}/\Lambda\setminus\{0\}$ 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

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

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

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

Il existe $C_\Lambda \in \mathbb{C}$ et $D_\Lambda \in \mathbb{R}$ 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 $\mathbb{Z}$-base de Λ avec $\Im(\omega_1/\omega_2) > 0$. Alors on a

$$\mathrm{vol}_\Lambda = \Im(\omega_1\bar\omega_2).$$

On pose

$$\eta_1 = \eta_\Lambda(\omega_1) = 2\zeta_\Lambda(\omega_1/2), \qquad \eta_2 = \eta_\Lambda(\omega_2) = 2\zeta_\Lambda(\omega_2/2).$$

En utilisant la relation de Legendre

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

on montre facilement que

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

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 $K \to \mathbb{C}$ correspondant à v, et on regarde E comme courbe elliptique sur $\mathbb{C}$ au moyen de ce plongement.

Soit $\Lambda_v \subset \mathbb{C}$ 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 $\mathbb{C}/\Lambda_v$. Pour $P \in E(\mathbb{C})$, on note z_P le point correspondant de $\mathbb{C}/\Lambda_v$. Alors on a

$$\wp_v(z_P) = x(P) + b_2/12.$$

La hauteur locale λ_v est

$$\lambda_v(z) = \lambda_{\Lambda_v}(z)\,;$$

voir Silverman [8, Theorem VI.3.2].

La fonction ϕ_v est donnée par

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

Soient $t_1, t_2 \in \mathbb{C}/\Lambda_v$ les zéros de la fonction $\wp_v(z) - b_2/12$; on a $t_1 + t_2 = 0$. Alors les deux fonctions $\log|\wp_v(z) - b_2/12|$ 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

$$\log|\wp_v(z) - b_2/12| = 2\lambda_v(z) - \lambda_v(z-t_1) - \lambda_v(z-t_2) + I_v,$$

où

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

Cela implique

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

On pose

$$S = \{z \in \mathbb{C}/\Lambda_v \mid |\wp_v(z) - b_2/12| = 1\}.$$

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

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

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

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

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

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

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

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

Démonstration. 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

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

de sorte que

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

La loi d'addition permet, par un calcul standard, d'exprimer la fonction $\wp_v(z-t_1) + \wp_v(z-t_2)$ en $\wp_v(z)$ et $\wp_v(t_1) = \wp_v(t_2) = b_2/12$ comme suit :

$$\wp_v(z-t_1) + \wp_v(z-t_2) = \frac{b_2}{6} + \frac{b_4}{\wp_v(z) - b_2/12} + \frac{b_6}{(\wp_v(z) - b_2/12)^2}.$$

Ceci implique la deuxième partie. ∎

On note que la fonction W_v est harmonique. Il s'ensuit que pour borner la fonction $|W_v|$ sur $\mathbb{C}/\Lambda_v \setminus S$, il suffit de borner les deux 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*

$$|Z_{\Lambda_v}(q)| \le |Z_{\Lambda_v}(p)| + M_1 J,$$
$$\left|\tfrac{1}{2}(Z_{\Lambda_v}(q-t_1) + Z_{\Lambda_v}(q-t_2))\right| \le \left|\tfrac{1}{2}(Z_{\Lambda_v}(p-t_1) + Z_{\Lambda_v}(p-t_2))\right| + M_2 J,$$

où

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

Démonstration. 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 $\wp_v(z) - b_2/12$ identifie γ avec un segment du cercle unité dans $\mathbb{C}$. On a

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

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

$$|\wp_v(z) + C_{\Lambda_v}| \le |\wp_v(z) - b_2/12| + |C_{\Lambda_v} + b_2/12| = 1 + |C_{\Lambda_v} + b_2/12|.$$

On en déduit que

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

De façon analogue, on obtient

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

En utilisant la formule

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

on montre facilement que

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

COROLLAIRE 4.3. *Soit $p \in S$. Pour tout $z \in \mathbb{C}/\Lambda_v \setminus S$, on a*

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

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 $\mathbb{C}$, et soient $z, z_0 \in R$.*

(a) *Si $|\wp_v(z') - b_2/12| < 1$ pour tout $z' \in R$, on a*

$$|W_v(z) - W_v(z_0)| \le (|C_{\Lambda_v} + b_2/12| + |D_{\Lambda_v}| + 1)|z - z_0|.$$

(b) *Si $|\wp_v(z') - b_2/12| > 1$ pour tout $z' \in R$, on a*

$$|W_v(z) - W_v(z_0)| \le \left(|C_{\Lambda_v} + b_2/12| + |D_{\Lambda_v}| + \frac{|b_4| + |b_6|}{2}\right)|z - z_0|.$$

Démonstration. 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 $|\wp_v(z) - b_2/12| \le 1$, on a

$$|\wp_v(z) + C_{\Lambda_v}| \le |\wp_v(z) - b_2/12| + |C_{\Lambda_v} + b_2/12| \le 1 + |C_{\Lambda_v} + b_2/12|.$$

Pour $|\wp_v(z) - b_2/12| \ge 1$, le lemme 4.1 implique

$$\left|\frac{\wp_v(z - t_1) + \wp_v(z - t_2)}{2} + C_{\Lambda_v}\right| \le |C_{\Lambda_v} + b_2/12| + |b_4|/2 + |b_6|/2. \ \blacksquare$$

On considère maintenant des parallélogrammes de la forme

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

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

$$d(z_1, z_2) = \sup_{z \in R(z_0, z_1, z_2)} |z - z_0| = \tfrac{1}{2} \max\{|z_1 - z_2|, |z_1 + z_2|\}.$$

COROLLAIRE 4.5. *Soit $R = R(z_0, z_1, z_2)$ comme ci-dessus, et soit $z \in R$.*

(a) *Si $|\wp_v(z') - b_2/12| < 1$ pour tout $z' \in R$, on a*

$$|W_v(z)| \le |W_v(z_0)| + (|C_{\Lambda_v} + b_2/12| + |D_{\Lambda_v}| + 1)d(z_1, z_2).$$

(b) *Si $|\wp_v(z') - b_2/12| > 1$ pour tout $z' \in R$, on a*

$$|W_v(z)| \le |W_v(z_0)| + \left(|C_{\Lambda_v} + b_2/12| + |D_{\Lambda_v}| + \frac{|b_4| + |b_6|}{2}\right)d(z_1, z_2).$$

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 prescrite 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 $\mathbb{Z}$-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 de 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)

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

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. On vérifie facilement que cet algorithme termine et produit un μ qui satisfait à

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

6. Exemples. Voici quelques exemples. Nous avons utilisé PARI/GP [4] pour la plupart des calculs, et Sage [9] 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

$$\inf_{E(\mathbb{C})} \phi_v = -0.156\ldots, \qquad \sup_{E(\mathbb{C})} \phi_v = 0.597\ldots.$$

En utilisant le théorème 2.1, on obtient

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

Pour comparaison, la majoration trouvée par l'algorithme de Silverman [7] est

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

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

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

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

de -0.556 et que $h(Q)-\hat{h}(Q)$ est très proche de 0.798. On prend

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

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

$$h(P)=0, \qquad h(Q)=\log 61,$$
$$\hat{h}(P)=0.5556807\ldots, \qquad \hat{h}(Q)=3.3130740\ldots,$$
$$h(P)-\hat{h}(P)=-0.5556807\ldots, \qquad h(Q)-\hat{h}(Q)=0.7977997\ldots.$$

6.2. La courbe 15a4. Voici un exemple pour montrer que notre méthode donne parfois une meilleure majoration de $h-\hat{h}$ pour les $\overline{\mathbb{Q}}$-points que celle de Cremona, Prickett et Siksek [2] pour les $\mathbb{Q}$-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

$$\inf_{E(\mathbb{C})}\phi_v=0.584\ldots, \qquad \sup_{E(\mathbb{C})}\phi_v=2.512\ldots.$$

En utilisant le théorème 2.1, on obtient

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

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

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

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

$$\inf_{E(\mathbb{C})}\phi_v=0.217\ldots, \qquad \sup_{E(\mathbb{C})}\phi_v=1.422\ldots.$$

En utilisant le théorème 2.1, on obtient

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

Des bornes optimales pour les $\mathbb{Q}$-points ont déjà été calculées dans [1]. En fait, on a

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

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

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

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

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

$$\begin{aligned} h(P) &= \log 5169, \\ \hat{h}(P) &= 6.4174217\ldots, \\ h(P) - \hat{h}(P) &= 2.1330128\ldots. \end{aligned}$$

6.4. Une courbe étudiée par Cremona, Prickett et Siksek. Notre dernier exemple est une courbe elliptique de rang 4 sur $\mathbb{Q}$ 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 $\mathbb{Q}$, le conducteur étant $2^2 \cdot 199 \cdot 362793983647$. On a

$$\Delta_E = 2^4 \cdot 199 \cdot 362793983647, \qquad \Delta_E^{\mathrm{stable}} = 199 \cdot 362793983647.$$

Notre algorithme donne

$$\inf_{E(\mathbb{C})} \phi_v = 0.879\ldots, \qquad \sup_{E(\mathbb{C})} \phi_v = 5.780\ldots.$$

En utilisant le théorème 2.1, on obtient

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

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

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

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

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

De l'autre côté, le point

$$Q = (-45092013952912, \alpha)$$

avec

$$\alpha^2 = -199 \cdot 1601 \cdot 22133 \cdot 362793983647 \cdot 35838855272124651419$$

satisfait à

$$\begin{aligned} h(Q) &= 31.4397262\ldots, \\ \hat{h}(Q) &= 23.0000267\ldots, \\ h(Q) - \hat{h}(Q) &= \ \ 8.4396995\ldots. \end{aligned}$$

Remerciements. 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.

Références

[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*, Math. Comp. 44 (1985), 473–481.

[2] J. E. Cremona, M. Prickett and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory 116 (2006), 42–68.

[3] V. A. Dem′janenko, *An estimate of the remainder term in Tate's formula*, Math. Notes 3 (1968), 173–177.

[4] The PARI Group, PARI/GP, version 2.6.0, Bordeaux, 2013, http://pari.math.u-bordeaux.fr/.

[5] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. 25 (1995), 1501–1538.

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986 (2nd ed., 2009).

[7] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723–743.

[8] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts Math. 151, Springer, 1994.

[9] W. A. Stein et al., *Sage Mathematics Software*, version 5.10, The Sage Development Team, 2013, http://www.sagemath.org/.

[10] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. 23 (1974), 179–206.

[11] Y. Uchida, *The difference between the ordinary height and the canonical height on elliptic curves*, J. Number Theory 128 (2008), 263–279.

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

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

Current address:
Mathematics Institute
Zeeman Building
University of Warwick
Coventry CV4 7AL
United Kingdom
E-mail: P.Bruin@warwick.ac.uk

Reçu le 5.2.2013 (7339)