

HAUTEUR DES CORRESPONDANCES DE HECKE

PAR PASCAL AUTISSIER

RÉSUMÉ. — L'objectif de cet article est de mesurer la complexité arithmétique de la courbe modulaire $X_0(N)$ en fonction du niveau N . Pour ce faire, on utilise un morphisme fini (de degré 1 sur son image) de $X_0(N)$ vers une variété fixe $X(1) \times X(1)$ et on calcule la hauteur au sens d'Arakelov de l'image T_N de ce morphisme. La hauteur employée est directement reliée à la hauteur de Faltings des courbes elliptiques.

On a besoin pour cela de considérer une théorie d'Arakelov pour les faisceaux inversibles hermitiens L_1^2 -singuliers (au lieu de C^∞ classiquement).

On en déduit des résultats sur la hauteur (de Faltings) de courbes elliptiques isogènes, ainsi que sur des moyennes de hauteurs de courbes elliptiques à multiplication complexe (*i.e.* une formule de Kronecker arithmétique).

ABSTRACT (*The height of the Hecke correspondences*). — The goal of this paper is the measure of the arithmetic complexity of the modular curve $X_0(N)$, as a function of the level N . For this, we use a finite morphism (of degree 1 over its image) from $X_0(N)$ to a fixed variety $X(1) \times X(1)$, and we calculate the (Arakelov) height of the image T_N of this morphism. This height is related to the Faltings height of elliptic curves.

For this, we need to consider an Arakelov theory for L_1^2 -singular hermitian line bundles (instead of C^∞ ones classically).

As an application, we find results on the (Faltings) height of isogenous elliptic curves, and on averages of heights of CM elliptic curves (*i.e.* an arithmetic Kronecker formula).

Texte reçu le 24 septembre 2002, accepté le 24 janvier 2003

PASCAL AUTISSIER, Département de Mathématiques, bât. 425, Université Paris XI, 91405 Orsay Cedex (France) • *E-mail* : pascal.autissier@math.u-psud.fr

Classification mathématique par sujets (2000). — 11F32, 14G40, 11G50.

Mots clefs. — Hauteur, correspondance, théorie d'Arakelov, courbe modulaire, courbe elliptique.

1. Théorie des hauteurs

1.1. Généralités

DÉFINITIONS 1.1. — Une *variété arithmétique* est un schéma X intègre, projectif et plat sur \mathbb{Z} , tel que la fibre générique $X_{\mathbb{Q}}$ soit lisse sur \mathbb{Q} .

Soient K un corps de nombres, et O_K son anneau des entiers. Une variété arithmétique *sur* O_K est un O_K -schéma X tel que X soit une variété arithmétique et que la fibre générique X_K soit géométriquement irréductible sur K .

Remarquons que si X_1 et X_2 sont des variétés arithmétiques sur O_K , alors le produit $X_1 \times_{O_K} X_2$ est aussi une variété arithmétique sur O_K .

DÉFINITIONS 1.2. — Soient X une variété arithmétique, et W une partie fermée de $X(\mathbb{C})$ stable par conjugaison complexe. Un *faisceau inversible hermitien* sur X *singulier* le long de W est un couple $\widehat{\mathcal{L}} = (\mathcal{L}; \|\cdot\|)$, formé d'un faisceau inversible \mathcal{L} sur X , et d'une famille $\|\cdot\|$ de normes hermitiennes sur $\mathcal{L}_{\mathbb{C}}$ variant de manière continue sur $X(\mathbb{C}) - W$ et invariante par conjugaison complexe.

On note $\omega_{\widehat{\mathcal{L}}}$ le $(1; 1)$ -courant de courbure de $\widehat{\mathcal{L}}_{\mathbb{C}}$ sur $X(\mathbb{C}) - W$.

Lorsque W est vide et la famille $\|\cdot\|$ est C^∞ sur $X(\mathbb{C})$, le faisceau inversible hermitien $\widehat{\mathcal{L}}$ est dit C^∞ . Les classes d'isométrie de faisceaux inversibles hermitiens C^∞ sur X forment un groupe $\widehat{\text{Pic}}(X)$ pour le produit tensoriel.

Soit X une variété arithmétique. On désigne par $Z_1(X)$ le groupe des 1-cycles (*i.e.* combinaisons \mathbb{Z} -linéaires de sous-schémas fermés intègres de dimension 1) sur X .

Un *point entier* de X est un fermé intègre de X qui est horizontal (*i.e.* plat sur \mathbb{Z}) et de dimension 1.

Soit $\widehat{\mathcal{L}}$ un faisceau inversible hermitien singulier le long d'un W . Nous notons $Z_1(X; W)$ le groupe des $D \in Z_1(X)$ tels que le support de $D_{\mathbb{C}}$ ne rencontre pas W .

DÉFINITIONS 1.3. — Soit Y un fermé intègre de X tel que $Y \in Z_1(X; W)$ en tant que cycle. La *hauteur* de Y relativement à $\widehat{\mathcal{L}}$ est le réel $h_{\widehat{\mathcal{L}}}(Y)$ défini par :

- si Y est horizontal, alors $h_{\widehat{\mathcal{L}}}(Y) = \widehat{\text{deg}}(\widehat{\mathcal{L}}|_Y)$ où $\widehat{\text{deg}}$ est le degré arithmétique;
- si Y est vertical au-dessus d'un nombre premier p , alors $h_{\widehat{\mathcal{L}}}(Y) = \text{deg}_{\mathbb{F}_p}(\mathcal{L}|_Y) \ln p$.

Dans le cas Y horizontal (*i.e.* Y est un point entier), on définit la *hauteur normalisée* $h'_{\widehat{\mathcal{L}}}(Y)$ de Y relativement à $\widehat{\mathcal{L}}$ par

$$h'_{\widehat{\mathcal{L}}}(Y) = \frac{h_{\widehat{\mathcal{L}}}(Y)}{[k(Y) : \mathbb{Q}]}.$$

En outre, par \mathbb{Z} -linéarité, on définit la hauteur $h_{\widehat{\mathcal{L}}}(D)$ pour tout $D \in Z_1(X; W)$.

1.2. Correspondances. — Commençons ce paragraphe par quelques rappels de la théorie d'Arakelov généralisée de Bost [2] dans le cas des surfaces arithmétiques (*i.e.* variétés arithmétiques de dimension 2).

Soient X une surface arithmétique, W une partie finie de $X(\mathbb{C})$ stable par conjugaison complexe, et $\widehat{\mathcal{L}} = (\mathcal{L}; \|\cdot\|)$ un faisceau inversible hermitien singulier le long de W . On dit que $\widehat{\mathcal{L}}$ est L_1^2 -singulier le long de W lorsque pour une (donc pour toute) famille $\|\cdot\|'$ telle que $(\mathcal{L}; \|\cdot\|')$ soit C^∞ , la fonction $\ln \|\cdot\|/\|\cdot\|'$ est L_1^2 (*cf.* [2, p. 254]) sur $X(\mathbb{C})$.

La courbure $\omega_{\widehat{\mathcal{L}}}$ se prolonge alors en un courant sur $X(\mathbb{C})$.

Les classes d'isométrie de faisceaux inversibles hermitiens L_1^2 -singuliers (le long d'un certain W) forment un groupe $\widehat{\text{Pic}}(X; L_1^2)$.

La théorie de Bost [2] (*cf.* p. 274) définit une forme bilinéaire symétrique que l'on notera $\langle \cdot, \cdot \rangle : \widehat{\text{Pic}}(X; L_1^2) \times \widehat{\text{Pic}}(X; L_1^2) \rightarrow \mathbb{R}$.

Pour $\widehat{\mathcal{L}} \in \widehat{\text{Pic}}(X; L_1^2)$, la hauteur de X relativement à $\widehat{\mathcal{L}}$ est le réel noté $h_{\widehat{\mathcal{L}}}(X)$ que l'on définit par $h_{\widehat{\mathcal{L}}}(X) = \langle \widehat{\mathcal{L}}, \widehat{\mathcal{L}} \rangle$. On a la propriété suivante :

PROPOSITION 1.4. — *Soit $\widehat{\mathcal{L}}$ un faisceau inversible hermitien L_1^2 -singulier le long d'un W tel que $\omega_{\widehat{\mathcal{L}}}$ soit localement L^t sur $X(\mathbb{C}) - W$ pour un certain réel $t > 1$. Soient $n \geq 1$ et s une section rationnelle globale non nulle de $\mathcal{L}^{\otimes n}$ sur X tel que le support de $\text{div}(s_{\mathbb{C}})$ ne rencontre pas W . Alors on a*

$$h_{\widehat{\mathcal{L}}}(X)n = h_{\widehat{\mathcal{L}}}(\text{div}(s)) - \int_{X(\mathbb{C})} \ln \|s_{\mathbb{C}}\| \omega_{\widehat{\mathcal{L}}}.$$

Démonstration. — C'est la proposition 5.3 de [2], où l'on a remplacé l'hypothèse L^∞ par l'hypothèse L^t grâce au lemme 5.2 de [2]. □

On a également une formule de projection :

Soit $f : X_1 \rightarrow X_2$ un morphisme surjectif de surfaces arithmétiques. Il est alors génériquement fini ; soit e son degré (générique).

Si $\widehat{\mathcal{L}}$ est un faisceau inversible hermitien sur X_2 L_1^2 -singulier le long d'un W , alors $f^*\widehat{\mathcal{L}}$ est un faisceau inversible hermitien sur X_1 L_1^2 -singulier le long de $f_{\mathbb{C}}^{-1}(W)$. Cela induit un homomorphisme $f^* : \widehat{\text{Pic}}(X_2; L_1^2) \rightarrow \widehat{\text{Pic}}(X_1; L_1^2)$.

On a alors $\langle f^*\widehat{\mathcal{L}} \cdot f^*\widehat{\mathcal{M}} \rangle = \langle \widehat{\mathcal{L}} \cdot \widehat{\mathcal{M}} \rangle e$ pour tout $(\widehat{\mathcal{L}}, \widehat{\mathcal{M}}) \in \widehat{\text{Pic}}(X_2; L_1^2)^2$. En particulier, on a $h_{f^*\widehat{\mathcal{L}}}(X_1) = h_{\widehat{\mathcal{L}}}(X_2)e$ pour tout $\widehat{\mathcal{L}} \in \widehat{\text{Pic}}(X_2; L_1^2)$.

On s'intéresse maintenant au cas particulier suivant : soient K un corps de nombres, X une surface arithmétique sur O_K et $\widehat{\mathcal{M}} \in \widehat{\text{Pic}}(X; L_1^2)$. On pose $P = X \times_{O_K} X$, et $\widehat{\mathcal{L}} = \text{pr}_1^* \widehat{\mathcal{M}} \otimes \text{pr}_2^* \widehat{\mathcal{M}}$, où les pr_i sont les projections $P \rightarrow X$.

Une correspondance T de X est un diviseur de Weil intègre sur P tel que les projections restreintes $\text{pr}_i : T \rightarrow X$ soient surjectives. On définit la hauteur $h_{\widehat{\mathcal{L}}}(T)$ de T relativement à $\widehat{\mathcal{L}}$ de la manière suivante :

Soit $f : T' \rightarrow T$ un morphisme surjectif de degré 1 (*i.e.* birationnel), avec T' surface arithmétique. On pose $\pi_i = \text{pr}_i \circ f$. On remarque que l'on a $f^* \widehat{\mathcal{L}} = \pi_1^* \widehat{\mathcal{M}} \otimes \pi_2^* \widehat{\mathcal{M}}$ dans $\widehat{\text{Pic}}(T'; L_1^2)$. On pose alors $h_{\widehat{\mathcal{L}}}(T) = h_{f^* \widehat{\mathcal{L}}}(T')$. La formule de projection assure que ce réel ne dépend pas du choix de T' et de f (et il existe toujours un tel couple $(T'; f)$: par exemple, la normalisation de T).

Notons que lorsque $\widehat{\mathcal{M}}$ est C^∞ , cette définition coïncide celle de [3, p. 945] (hauteur de T en tant que 2-cycle sur P).

REMARQUE 1.5. — Soit T un diviseur de Weil intègre horizontal sur P qui n'est pas une correspondance. Alors T est nécessairement une surface arithmétique de la forme $T = \text{pr}_1^* Y = Y \times_{O_K} X$ ou $T = \text{pr}_2^* Y = X \times_{O_K} Y$, avec Y point entier de X .

Si de plus $Y \in Z_1(X; W)$, alors on a (par bilinéarité de la forme $\langle \cdot, \cdot \rangle$) :

$$h_{\widehat{\mathcal{L}}_T}(T) = 2 \deg_K(\mathcal{M}_K) h_{\widehat{\mathcal{M}}}(Y) + [k(Y) : K] h_{\widehat{\mathcal{M}}}(X).$$

2. Préliminaires modulaires

Soient \mathcal{H} le demi-plan supérieur, et $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. On note l'action du groupe modulaire $\Gamma(1) = \text{SL}_2(\mathbb{Z})$ sur $\overline{\mathcal{H}}$ de la manière suivante :

$$\text{si } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1) \quad \text{et} \quad \tau \in \overline{\mathcal{H}}, \quad \text{alors} \quad \gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

On pose

$$M_1 = \Gamma(1) \backslash \overline{\mathcal{H}}.$$

La fonction elliptique modulaire j induit un isomorphisme $j : M_1 \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$. Soit

$$\mu = \frac{3i d\tau \wedge d\bar{\tau}}{2\pi(\text{Im}\tau)^2} = \frac{3dx \wedge dy}{\pi y^2}$$

la (1;1)-forme de Poincaré, qui induit une mesure de probabilité sur M_1 .

Pour $\tau \in \mathcal{H}$, on pose $q = e^{2i\pi\tau}$ et $\Delta(\tau) = (2\pi)^{12} q \prod_{n \geq 1} (1 - q^n)^{24}$.

Soient ζ la fonction de Riemann, et κ_0 la constante d'Euler. Dans toute la suite, on note κ_1 la constante

$$\kappa_1 = \frac{6}{\pi^2} \zeta'(2) - \kappa_0 - \ln(2\pi^2) + \frac{1}{2} = 12\zeta'(-1) - \ln \pi - \frac{1}{2}.$$

Pour $(\tau_1; \tau_2) \in \mathcal{H}^2$ avec $\tau_1 \neq \tau_2$, on pose $y_i = \text{Im}\tau_i$, et

$$g(\tau_1; \tau_2) = -2 \ln \left(|j(\tau_1) - j(\tau_2)| \cdot |\Delta(\tau_1)\Delta(\tau_2)| y_1^6 y_2^6 \right).$$

La fonction g peut être vue comme une fonction sur $(\Gamma(1) \backslash \mathcal{H})^2$ privé de la diagonale. C'est une fonction de Green pour la mesure μ . En particulier, on a le résultat suivant :

PROPOSITION 2.1. — Pour tout $\tau_1 \in \mathcal{H}$, on a $\int_{M_1} g(\tau_1; \tau) \mu(\tau) = 24\kappa_1$.

Démonstration. — Il suffit d'appliquer la « formule de Jensen modulaire » de Rohrlich [19] à $f(\tau) = (2\pi)^{-12}(j(\tau) - j(\tau_1))\Delta(\tau)$, qui est une forme modulaire de poids 12. \square

Pour un entier $N \geq 1$, on pose

$$\mathcal{C}_N = \left\{ \gamma = \begin{bmatrix} a_\gamma & b_\gamma \\ 0 & d_\gamma \end{bmatrix} \in M_2(\mathbb{Z}); a_\gamma d_\gamma = N, \right. \\ \left. a_\gamma \geq 1, 0 \leq b_\gamma \leq d_\gamma - 1 \text{ et } a_\gamma \wedge b_\gamma \wedge d_\gamma = 1 \right\}.$$

On pose

$$e_N = \#\mathcal{C}_N = N \prod_{\substack{p|N \\ p \text{ premier}}} \left(1 + \frac{1}{p}\right).$$

Il existe un unique polynôme $\Phi_N \in \mathbb{Z}[X; Y]$ (le polynôme modulaire d'ordre N , cf. [21, p. 109–110]) tel que

$$\forall \tau \in \mathcal{H}, \quad \Phi_N(X; j(\tau)) = \prod_{\gamma \in \mathcal{C}_N} (X - j(\gamma\tau)).$$

On a $\Phi_1 = X - Y$ et $\Phi_N(X; Y) = \Phi_N(Y; X)$ pour tout $N \geq 2$.

Les résultats combinatoires suivants nous seront utiles dans la suite :

LEMME 2.2. — Pour tout $N \geq 2$ et tout $\tau \in \mathcal{H}$, on a

$$\prod_{\gamma \in \mathcal{C}_N} \Delta(\gamma\tau) = [-\Delta(\tau)]^{e_N}.$$

Démonstration. — Le quotient des deux membres est une fonction méromorphe sur M_1 sans zéro ni pôle sur $M_1 - \{\infty\}$, donc est une constante. On calcule alors cette constante en comparant le premier terme non nul (*i.e.* celui de degré e_N) du q -développement de chaque membre. \square

Soient $N \geq 1$ et $N = \prod_i p_i^{r_i}$ sa décomposition en facteurs premiers. Posons

$$\lambda_N = \sum_i \frac{p_i^{r_i} - 1}{p_i^{r_i-1}(p_i^2 - 1)} \ln p_i.$$

On remarque que l'on a $\lambda_N = O(\ln \ln N)$.

LEMME 2.3. — Avec ces notations, on a

$$\sum_{\gamma \in \mathcal{C}_N} \ln \frac{d_\gamma}{a_\gamma} = e_N(\ln N - 2\lambda_N).$$

Démonstration. — Notons S_N le membre de gauche. On vérifie aisément que pour M et N premiers entre eux, on a $S_{MN} = e_N S_M + e_M S_N$. Il reste donc à calculer S_{p^r} pour p premier et $r \geq 1$. On trouve

$$S_{p^r} = \left[p^{r-1}(p+1)r - 2 \frac{p^r - 1}{p-1} \right] \ln p.$$

On en déduit le résultat. \square

3. Hauteur de T_N

Soit $X(1)$ le schéma de modules grossier des courbes elliptiques généralisées. L'invariant modulaire j induit un isomorphisme $j : X(1) \xrightarrow{\sim} \mathbb{P}_{\mathbb{Z}}^1$. Par ailleurs, $X(1)(\mathbb{C})$ s'identifie à M_1 .

Pour un entier $N \geq 1$, soit $X_0(N)$ la compactification de Deligne-Rapoport du schéma de modules grossier des isogénies cycliques de degré N entre courbes elliptiques (cf. [9], [13]). On sait que $X_0(N)$ est une surface arithmétique normale.

On pose $P = X(1) \times_{\mathbb{Z}} X(1)$. On a un morphisme $i_N : X_0(N) \rightarrow P$ fini (de degré 1 sur son image), induit par le foncteur qui à une isogénie $\alpha : E \rightarrow E'$ associe le couple $(E; E')$. Soit T_N l'image de i_N (qui est birationnelle à $X_0(N)$). T_N est un diviseur intègre sur P , appelé la correspondance de Hecke d'ordre N .

Soit $[\infty]$ le diviseur associé à la pointe $\infty \in X(1)(\mathbb{Z})$. On pose

$$\mathcal{M} = \mathcal{O}_{X(1)}([\infty]) = j^* \mathcal{O}_{\mathbb{P}^1}(1).$$

On munit le faisceau inversible \mathcal{M} de la métrique $\| \cdot \|_m$ telle que

$$\|1\|_m(\tau) = |\Delta(\tau)|(\text{Im}\tau)^6.$$

On pose $\widehat{\mathcal{M}} = (\mathcal{M}; \| \cdot \|_m)$. Ce faisceau inversible hermitien sur $X(1)$ (L_1^2 -singulier le long de $\infty_{\mathbb{C}}$) a la propriété suivante :

Soit E une courbe elliptique sur $\overline{\mathbb{Q}}$. Elle définit un point $x \in X(1)(\overline{\mathbb{Q}})$. Soit Y l'adhérence de l'image de x . Notons $\tilde{h}(E)$ la hauteur de Faltings (stable) de E . Alors on a $\tilde{h}(E) = \frac{1}{12} h'_{\widehat{\mathcal{M}}}(Y)$.

On pose $\widehat{\mathcal{L}} = \text{pr}_1^* \widehat{\mathcal{M}} \otimes \text{pr}_2^* \widehat{\mathcal{M}}$ où les pr_i sont les projections $P \rightarrow X(1)$.

On peut relier T_N et le polynôme modulaire Φ_N de la façon suivante : soient $\tilde{\Phi}_N$ le polynôme bi-homogène associé à Φ_N , vu comme section globale de $\mathcal{O}(e_N; e_N)$ sur $\mathbb{P}^1 \times_{\mathbb{Z}} \mathbb{P}^1$, et $\phi_N = (j \times j)^* \tilde{\Phi}_N$ section globale de $\mathcal{L}^{\otimes e_N}$. On a alors la relation $T_N = \text{div}(\phi_N)$ (cf. [9, p. 283]).

PROPOSITION 3.1. — On a $h_{\widehat{\mathcal{M}}}(X(1)) = 12\kappa_1$.

Démonstration. — C'est le théorème 6.1 de [14, p. 229]. Cela peut aussi se démontrer à partir de la proposition 2.1. \square

Soient Y un diviseur de Weil intègre sur $X(1)$, et $n = [k(Y) : \mathbb{Q}]$. Il existe une section globale s de $\mathcal{M}^{\otimes n}$ sur $X(1)$ telle que $\text{div}(s) = Y$. Posons

$$\pi_i = \text{pr}_i \circ i_N : X_0(N) \longrightarrow X(1).$$

Le morphisme π_2 induit (cf. [11]) un homomorphisme

$$\pi_{2*} : Z_1(X_0(N)) \longrightarrow Z_1(X(1)).$$

On pose alors $T_{N*}Y = \pi_{2*}(\text{div}(\pi_1^*s))$; c'est un 1-cycle sur $X(1)$.

On peut décrire $T_{N*}Y$ d'une autre manière : notons Y' le diviseur de Weil intègre $Y' = \text{pr}_1^*Y = Y \times_{\mathbb{Z}} X(1)$. Le diviseur T_N étant en fait un diviseur de Cartier, on peut considérer le 1-cycle intersection $T_N \cdot Y' = \text{div}(\phi_{N|Y'})$. Alors $T_{N*}Y = \text{pr}_{2*}(T_N \cdot Y')$.

Remarquons que $\text{deg}_{\mathbb{Q}}((T_{N*}Y)_{\mathbb{Q}}) = e_N n$. On remarque également que si Y est vertical au-dessus d'un premier p , alors $Y = X(1)_{\mathbb{F}_p}$ et $T_{N*}Y = e_N Y$.

On se propose de calculer la hauteur de T_N relativement à $\widehat{\mathcal{L}}$, ainsi que la hauteur de $T_{N*}Y$ relativement à $\widehat{\mathcal{M}}$ lorsque Y est horizontal.

THÉOREME 3.2. — Soient $N \geq 1$, et Y un point entier de $X(1)$ tel que $Y_{\mathbb{C}}$ ne rencontre pas $\infty_{\mathbb{C}}$. Posons $n = [k(Y) : \mathbb{Q}]$. On a alors

$$h_{\widehat{\mathcal{L}}}(T_N) = 12e_N(\ln N - 2\lambda_N + 4\kappa_1), \quad \frac{1}{e_N n} h_{\widehat{\mathcal{M}}}(T_{N*}Y) = h'_{\widehat{\mathcal{M}}}(Y) + 6 \ln N - 12\lambda_N.$$

Démonstration. — Posons $Y' = \text{pr}_1^*Y$. D'après la proposition 1.4, on a la formule

$$(*) \quad h_{\widehat{\mathcal{L}}_{|Y'}}(\text{div}(\phi_{N|Y'})) = h_{\widehat{\mathcal{L}}_{|Y'}}(Y')e_N + \int_{Y'(\mathbb{C})} \ln \|\phi_{N\mathbb{C}}\| \omega_{\widehat{\mathcal{L}}_{|Y'}}.$$

D'autre part, on a

$$\|\phi_{N\mathbb{C}}\|(\tau; \tau') = |\Phi_N(j(\tau); j(\tau'))| \cdot |\Delta(\tau)\Delta(\tau')|^{e_N} ((\text{Im}\tau)(\text{Im}\tau'))^{6e_N}.$$

En utilisant le lemme 2.2 et le fait que $\text{Im}(\gamma\tau') = a_{\gamma}/d_{\gamma}\text{Im}\tau'$ pour $\gamma \in \mathcal{C}_N$, on obtient

$$2 \ln \|\phi_{N\mathbb{C}}\|(\tau; \tau') = 12S_N - \sum_{\gamma \in \mathcal{C}_N} g(\gamma\tau; \tau')$$

où l'on a posé $S_N = \sum_{\gamma \in \mathcal{C}_N} \ln d_{\gamma}/a_{\gamma}$.

L'ensemble $Y(\mathbb{C})$, vu comme partie de M_1 , peut s'écrire $Y(\mathbb{C}) = \{\tau_1; \dots; \tau_n\}$ pour des $\tau_i \in \Gamma(1) \setminus \mathcal{H}$. La formule (*) donne alors

$$h_{\widehat{\mathcal{L}}_{|Y'}}(T_N \cdot Y') = h_{\widehat{\mathcal{L}}_{|Y'}}(Y')e_N + \sum_{i=1}^n \int_{M_1} \left(6S_N - \frac{1}{2} \sum_{\gamma \in \mathcal{C}_N} g(\gamma\tau; \tau') \right) \mu(\tau').$$

Grâce à la proposition 2.1 et au lemme 2.3, on en déduit l'égalité suivante :

$$h_{\widehat{\mathcal{L}}_{|Y'}}(T_N \cdot Y') = h_{\widehat{\mathcal{L}}_{|Y'}}(Y')e_N + 6e_N n(\ln N - 2\lambda_N - 2\kappa_1).$$

Or, d'après la remarque 1.5 et la proposition 3.1, on a d'une part $h_{\widehat{\mathcal{L}}|_{Y'}}(Y') = 2h_{\widehat{\mathcal{M}}}(Y) + 12\kappa_1 n$. D'autre part, en écrivant $\widehat{\mathcal{L}} = \text{pr}_1^* \widehat{\mathcal{M}} \otimes \text{pr}_2^* \widehat{\mathcal{M}}$ et la formule de projection pour les 1-cycles, on trouve $h_{\widehat{\mathcal{L}}|_{Y'}}(T_N \cdot Y') = e_N h_{\widehat{\mathcal{M}}}(Y) + h_{\widehat{\mathcal{M}}}(T_N * Y)$.

On en déduit le résultat : $h_{\widehat{\mathcal{M}}}(T_{N*} Y) = e_N n (h'_{\widehat{\mathcal{M}}}(Y) + 6 \ln N - 12\lambda_N)$.

Maintenant, soit s une section globale de $\mathcal{M}^{\otimes n}$ sur $X(1)$ vérifiant $\text{div}(s) = Y$. Posons $s' = (\pi_1^* s \otimes \pi_2^* s)$; c 'est une section globale de $i_N^* \mathcal{L}^{\otimes n}$ sur $X_0(N)$. D'après la proposition 1.4, on a l'égalité

$$(**) \quad h_{\widehat{\mathcal{L}}}(T_N)n = h_{i_N^* \widehat{\mathcal{L}}}(X_0(N))n = h_{i_N^* \widehat{\mathcal{L}}}(\text{div}(s')) - \int_{X_0(N)(\mathbb{C})} \ln \|s'\| \omega_{i_N^* \widehat{\mathcal{L}}}.$$

Par la symétrie de T_N , on a

$$h_{i_N^* \widehat{\mathcal{L}}}(\text{div}(s')) = 2e_N h_{\widehat{\mathcal{M}}}(Y) + 2h_{\widehat{\mathcal{M}}}(T_N * Y) = 4e_N h_{\widehat{\mathcal{M}}}(Y) + 12e_N n (\ln N - 2\lambda_N).$$

Par ailleurs, on a $\|s'_\mathbb{C}\| = \|\pi_1^* s_\mathbb{C}\| \cdot \|\pi_2^* s_\mathbb{C}\|$. On vérifie également que l'on a $\omega_{i_N^* \widehat{\mathcal{L}}} = 2\pi_1^* \mu = 2\pi_2^* \mu$ sur $M_N = X_0(N)(\mathbb{C}) = \Gamma_0(N) \backslash \overline{\mathcal{H}}$. On en déduit que

$$\begin{aligned} \int_{M_N} \ln \|s'_\mathbb{C}\| \omega_{i_N^* \widehat{\mathcal{L}}} &= 2 \int_{M_N} \ln \|\pi_1^* s_\mathbb{C}\| \pi_1^* \mu + 2 \int_{M_N} \ln \|\pi_2^* s_\mathbb{C}\| \pi_2^* \mu \\ &= 4e_N \int_{M_1} \ln \|s_\mathbb{C}\| \mu. \end{aligned}$$

En utilisant de nouveau la proposition 1.4, la formule (**) donne alors

$$h_{\widehat{\mathcal{L}}}(T_N)n = 4h_{\widehat{\mathcal{M}}}(X(1))e_N n + 12e_N n (\ln N - 2\lambda_N).$$

D'où la formule pour $h_{\widehat{\mathcal{L}}}(T_N)$. □

On en déduit le résultat suivant sur la hauteur de Faltings de courbes elliptiques isogènes :

COROLLAIRE 3.3. — Soient E une courbe elliptique sur $\overline{\mathbb{Q}}$, G_1, \dots, G_{e_N} les sous-groupes cycliques d'ordre N de E (il y a e_N tels sous-groupes) et $E_i = E/G_i$. Alors on a

$$\frac{1}{e_N} \sum_{i=1}^{e_N} \tilde{h}(E_i) = \tilde{h}(E) + \frac{1}{2} \ln N - \lambda_N.$$

Démonstration. — Soient $x \in X(1)(\overline{\mathbb{Q}})$ le point défini par E et Y l'adhérence de l'image de x . On a alors

$$\tilde{h}(E) = \frac{1}{12} h'_{\widehat{\mathcal{M}}}(Y) \quad \text{et} \quad \sum_{i=1}^{e_N} \tilde{h}(E_i) = \frac{1}{12n} h_{\widehat{\mathcal{M}}}(T_N * Y).$$

Il suffit donc d'appliquer le théorème 3.2. □

REMARQUE 3.4. — Lorsque E est sans multiplication complexe, le théorème de l'image ouverte de Serre [20] implique qu'il existe un entier $n_0 \geq 1$ (ne dépendant que de E) tel que :

$$N \wedge n_0 = 1 \implies \tilde{h}(E_i) \text{ est indépendant de } i.$$

Alors pour toute isogénie $\alpha : E \rightarrow E'$ cyclique de degré N premier à n_0 , on a

$$\tilde{h}(E') = \tilde{h}(E) + \frac{1}{2} \ln N - \lambda_N.$$

REMARQUE 3.5. — La première formule du théorème 3.2 précise un résultat asymptotique de Cohen [5] sur la hauteur de Weil (au lieu d'Arakelov) du polynôme Φ_N , résultat qui peut se traduire de la manière suivante :

Soit $\|\cdot\|_1$ une métrique telle que $\widehat{\mathcal{L}}_1 = (\mathcal{L}; \|\cdot\|_1)$ soit C^∞ et à courbure définie positive; alors on a $(1/e_N)h_{\widehat{\mathcal{L}}_1}(T_N) = 12 \ln N - 24\lambda_N + O(1)$.

Par ailleurs, le corollaire 3.3 était connu de Szpiro et Ullmo [23] pour N sans facteur carré (cf. aussi Silverman [22] pour une formule asymptotique en termes de hauteurs de Weil).

4. Formule de Kronecker arithmétique

On commence ce paragraphe par quelques rappels de la théorie de la multiplication complexe des courbes elliptiques (cf. par exemple [8] et [15]).

On désigne par QuIm l'ensemble des classes d'isomorphie d'ordres quadratiques imaginaires.

Soit $A \in \text{QuIm}$ un tel ordre, de nombre de classe $H_A = \#\text{Pic}(A)$. Les classes de $\overline{\mathbb{Q}}$ -isomorphie de courbes elliptiques E sur $\overline{\mathbb{Q}}$ telles que $\text{End}_{\overline{\mathbb{Q}}}(E) \simeq A$ forment un ensemble $\text{Ell}(A)$ de cardinal H_A . Le polynôme

$$Q_A(X) = \prod_{E \in \text{Ell}(A)} (X - j(E))$$

est alors à coefficients entiers et irréductible sur \mathbb{Q} .

Pour $N \geq 1$, on note $R_{A;N}$ l'ensemble (fini) des $x \in A$ tels que A/xA soit un groupe cyclique d'ordre N , et $r_{A;N} = \#(R_{A;N}/A^*)$; on pose également

$$f_N = \sum_{\gamma \in \mathcal{C}_N} \max\left(\frac{a_\gamma}{d_\gamma}; 1\right) \quad \text{et} \quad f'_N = \sum_{\gamma \in \mathcal{C}_N} \min\left(\frac{a_\gamma}{d_\gamma}; 1\right).$$

On a $f_N = 2e_N - f'_N$ et on peut montrer que l'on a $f'_N = O_\varepsilon(N^{1/2+\varepsilon})$ pour tout $\varepsilon > 0$.

Fixons maintenant $N \geq 2$. Le polynôme $\Phi_N(X; X)$ est de degré f_N . On a la relation de Kronecker (cf. [15, p. 144], [8, p. 287]) :

Il existe un entier c_N tel que

$$\Phi_N(X; X) = c_N \prod_{A \in \text{QuIm}} Q_A(X)^{r_{A;N}}.$$

En particulier, en considérant le degré des deux membres, on obtient

$$f_N = \sum_{A \in \text{QuIm}} r_{A;N} H_A.$$

Par ailleurs, on a

$$|c_N| = \begin{cases} p & \text{si } N = p^{2r} \text{ avec } p \text{ premier et } r \geq 1; \\ 1 & \text{sinon.} \end{cases}$$

On peut traduire géométriquement la relation de Kronecker : pour $A \in \text{QuIm}$, soit Y_A le point entier de $X(1) \simeq \mathbb{P}^1$ défini par le polynôme homogène associé à Q_A . Par l'interprétation modulaire de $X(1)$, on a $Y_A(\overline{\mathbb{Q}}) \simeq \text{Ell}(A)$.

Posons $\psi = \text{pr}_1^* 1 \otimes \text{pr}_2^* 1$, où 1 est vue comme section globale de $\mathcal{O}_{X(1)}([\infty])$ sur $X(1)$; ψ est une section globale de \mathcal{L} sur P . On pose $s_N = \phi_N^{\otimes 2} / \psi^{\otimes f'_N}$ section rationnelle globale de $\mathcal{L}^{\otimes f_N}$ sur P , de diviseur $2T_N - f'_N \text{pr}_1^*[\infty] - f'_N \text{pr}_2^*[\infty]$. Soit $\delta = i_1 : X(1) \rightarrow P$ le plongement diagonal.

On pose

$$V_N = \begin{cases} X(1)_{\mathbb{F}_p} & \text{si } N = p^{2r} \text{ avec } p \text{ premier et } r \geq 1; \\ 0 & \text{sinon.} \end{cases}$$

On a alors $\text{div}(\delta^* s_N) = 2V_N + 2 \sum_{A \in \text{QuIm}} r_{A;N} Y_A$ dans $Z_1(X(1))$.

Cette formulation géométrique permet de démontrer le résultat suivant sur des sommes de hauteurs de Faltings de courbes elliptiques à multiplication complexe :

PROPOSITION 4.1. — *Pour tout $A \in \text{QuIm}$, choisissons $E_A \in \text{Ell}(A)$. Alors pour tout $N \geq 2$, on a*

$$12 \sum_{A \in \text{QuIm}} r_{A;N} H_A \tilde{h}(E_A) = 6e_N (\ln N - 2\lambda_N) + 12f_N \kappa_1 - \ln |c_N| - \int_{M_1} \left[f'_N \ln |\Delta(\tau)(\text{Im}\tau)^6| + \frac{1}{2} \sum_{\gamma \in \mathcal{C}_N} g(\tau; \gamma\tau) \right] \mu(\tau).$$

Démonstration. — On a, par la relation de Kronecker :

$$24 \sum_{A \in \text{QuIm}} r_{A;N} H_A \tilde{h}(E_A) = h_{\widehat{\mathcal{M}}}(\text{div}(\delta^* s_N)) - 2 \ln |c_N|.$$

Or $\delta^* s_N$ est une section rationnelle globale de $\delta^* \mathcal{L}^{\otimes f_N} = \mathcal{M}^{\otimes 2f_N}$ sur $X(1)$. Donc, d'après la proposition 1.4, on a

$$h_{\widehat{\mathcal{M}}}(\text{div}(\delta^* s_N)) = 2f_N h_{\widehat{\mathcal{M}}}(X(1)) + \int_{M_1} \ln \|s_{N\mathbb{C}}\|(\tau; \tau) \mu(\tau).$$

Posons $y_i = \text{Im}\tau_i$. Alors on a

$$\|s_{NC}\|(\tau_1; \tau_2) = |\Phi_N(j(\tau_1); j(\tau_2))|^2 \cdot |\Delta(\tau_1)\Delta(\tau_2)y_1^6 y_2^6|^{f_N}.$$

Par les lemmes 2.2 et 2.3, on trouve

$$\ln \|s_{NC}\|(\tau_1; \tau_2) = 12e_N(\ln N - 2\lambda_N) - f'_N \ln |\Delta(\tau_1)\Delta(\tau_2)y_1^6 y_2^6| - \sum_{\gamma \in \mathcal{C}_N} g(\tau_1; \gamma\tau_2).$$

On en déduit la formule énoncée. □

PROPOSITION 4.2. — *Il existe une constante $\theta \in \mathbb{R}$ telle que pour tout $N \geq 2$, on ait*

$$\frac{1}{f_N} \sum_{A \in \text{QuIm}} r_{A;N} H_A \tilde{h}(E_A) \leq \frac{1}{4} \ln N - \frac{\lambda_N}{2} + \theta.$$

Démonstration. — Soit $\|\cdot\|'$ une métrique telle que $\widehat{\mathcal{M}}' = (\mathcal{M}; \|\cdot\|')$ soit C^∞ et que la courbure $\omega_{\widehat{\mathcal{M}}'}$ soit définie positive sur M_1 . On pose $\widehat{\mathcal{L}}' = \text{pr}_1^* \widehat{\mathcal{M}}' \otimes \text{pr}_2^* \widehat{\mathcal{M}}'$.

La fonction $\ln \|\cdot\|'/\|\cdot\|_m$ est uniformément majorée sur M_1 , disons par une constante θ_0 . Alors pour tout point entier Y de $X(1)$ autre que $[\infty]$, on obtient $h'_{\widehat{\mathcal{M}}'}(Y) \leq h_{\widehat{\mathcal{M}}'}(Y) + \theta_0$.

Par ailleurs, d'après un théorème de Bézout arithmétique (cf. [3], [17]), il existe une constante θ_1 telle que pour tout $N \geq 2$, on ait

$$h_{\widehat{\mathcal{L}}'}(T_1 \cdot T_N) \leq e_N h_{\widehat{\mathcal{L}}'}(T_1) + h_{\widehat{\mathcal{L}}'}(T_N) + \theta_1 e_N.$$

Or on a, par la relation de Kronecker, l'égalité

$$h_{\widehat{\mathcal{L}}'}(T_1 \cdot T_N) = 2 \sum_{A \in \text{QuIm}} r_{A;N} h_{\widehat{\mathcal{M}}'}(Y_A) + 2f'_N h_{\widehat{\mathcal{M}}'}([\infty]) + 2 \ln |c_N|.$$

En posant $\theta_2 = h_{\widehat{\mathcal{L}}'}(T_1)$ et $\theta_3 = h_{\widehat{\mathcal{M}}'}([\infty])$, on trouve donc

$$24 \sum_{A \in \text{QuIm}} r_{A;N} H_A \tilde{h}(E_A) \leq h_{\widehat{\mathcal{L}}'}(T_N) + (\theta_1 + \theta_2)e_N + 2\theta_0 f_N - 2\theta_3 f'_N.$$

En utilisant le résultat de Cohen [5] rappelé dans la remarque 3.5, on en déduit la proposition. □

REMARQUE 4.3. — Pour $A \in \text{QuIm}$, notons \mathbf{d}_A l'opposé du discriminant de A . La formule de la proposition 4.2 a pour membre de gauche une moyenne de hauteurs de Faltings de courbes elliptiques à multiplication complexe par des ordres A tels que $3 \leq \mathbf{d}_A \leq 4N$ (car $r_{A;N} \neq 0$ implique $\mathbf{d}_A \leq 4N$).

Cet énoncé est à comparer avec les estimations individuelles de Colmez [6] : il existe des constantes $a > 0$ et $b \in \mathbb{R}$ telles que pour tout $A \in \text{QuIm}$, on ait $\tilde{h}(E_A) \geq a \ln \mathbf{d}_A + b$. Par ailleurs, pour tout $\varepsilon > 0$, on a $\tilde{h}(E_A) = O_\varepsilon(\mathbf{d}_A^\varepsilon)$ pour tout $A \in \text{QuIm}$.

BIBLIOGRAPHIE

- [1] ARAKELOV (S.J.) – *Intersection theory of divisors on an arithmetic surface*, Math. USSR Izvest., t. **8** (1974), pp. 1167–1180.
- [2] BOST (J.-B.) – *Potential theory and Lefschetz theorems for arithmetic surfaces*, Ann. Sci. École Norm. Sup., t. **32** (1999), pp. 241–312.
- [3] BOST (J.-B.), GILLET (H.) & SOULÉ (C.) – *Heights of projective varieties and positive Green forms*, J. Amer. Math. Soc., t. **7** (1994), pp. 903–1027.
- [4] BURGOS (J.I.) – *Arithmetic Chow rings and Deligne-Beilinson cohomology*, J. Alg. Geom., t. **6** (1997), pp. 335–377.
- [5] COHEN (P.) – *On the coefficients of the transformation polynomials for the elliptic modular function*, Proc. Cambridge Phil. Society, t. **95** (1984), pp. 389–402.
- [6] COLMEZ (P.) – *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe*, Compositio Math., t. **111** (1998), pp. 359–368.
- [7] CORNELL (G.) & SILVERMAN (J.H.) – *Arithmetic Geometry*, Springer-Verlag, 1986.
- [8] COX (D.A.) – *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*, Wiley-Interscience Publication, 1989.
- [9] DELIGNE (P.) & RAPOPORT (M.) – *Les schémas de modules de courbes elliptiques*, in *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., vol. 349, Springer, 1973, pp. 143–316.
- [10] FALTINGS (G.) – *Calculus on arithmetic surfaces*, Ann. of Math., t. **119** (1984), pp. 387–424.
- [11] FULTON (W.) – *Intersection theory*, seconde éd., Springer-Verlag, 1998.
- [12] HIRZEBRUCH (F.) & VAN DER GEER (G.) – *Lectures on Hilbert modular surfaces*, Sémin. Math. Sup., vol. 77, Presses de l'Université de Montréal, Montréal, Qué., 1981.
- [13] KATZ (N.) & MAZUR (B.) – *Arithmetic moduli of elliptic curves*, Princeton University Press, 1985.
- [14] KÜHN (U.) – *Generalized arithmetic intersection numbers*, J. reine angew. Math., t. **534** (2001), pp. 209–236.
- [15] LANG (S.) – *Elliptic functions*, Graduate Texts in Math., vol. 112, Springer, 1987.
- [16] MAILLOT (V.) & ROESSLER (D.) – *Conjectures sur les dérivées logarithmiques des fonctions L d'Artin aux entiers négatifs*, À paraître, 2002.
- [17] MCKINNON (D.) – *An arithmetic analogue of Bezout's theorem*, Compositio Math., t. **126** (2001), pp. 147–155.
- [18] MUMFORD (D.) – *Hirzebruch's proportionality theorem in the non-compact case*, Invent. Math., t. **42** (1977), pp. 239–272.

- [19] ROHRLICH (D.E.) – *A modular version of Jensen's formula*, Proc. Cambridge Phil. Soc., t. **95** (1984), pp. 15–20.
- [20] SERRE (J.-P.) – *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., t. **15** (1972), pp. 259–331.
- [21] SHIMURA (G.) – *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.
- [22] SILVERMAN (J.H.) – *Hecke points on modular curves*, Duke Math. J., t. **60** (1990), pp. 401–423.
- [23] SZPIRO (L.) & ULLMO (E.) – *Variation de la hauteur de Faltings dans une classe de $\overline{\mathbb{Q}}$ -isogénie de courbe elliptique*, Duke Math. J., t. **97** (1999), pp. 81–97.