

# Variation de la hauteur de Faltings dans une classe de $\overline{\mathbb{Q}}$ -isogénie de courbes elliptiques.

Lucien Szpiro, Emmanuel Ullmo

## 1 Introduction

Soit  $E$  une courbe elliptique sur un corps de nombres  $K$  de discriminant minimal  $\Delta_E$ . Pour chaque place à l'infini  $\sigma$  de  $K$ , on choisit  $\tau_\sigma$  dans le demi-plan de Poincaré tel que  $E \otimes_\sigma \mathbb{C} \simeq \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau_\sigma$ . La hauteur de Faltings  $h(E)$  est donné explicitement par la formule

$$h(E) = \frac{1}{12} \frac{\log N_{K/\mathbb{Q}} \Delta_E}{[K : \mathbb{Q}]} - \sum_{\sigma} \frac{1}{12} \frac{\log |\Delta(\tau_\sigma) \text{Im}(\tau_\sigma)^6|}{[K : \mathbb{Q}]} \quad (1)$$

où  $\Delta$  est la fonction discriminant et  $N_{K/\mathbb{Q}}$  désigne la norme de  $K$  à  $\mathbb{Q}$ . Pour tout corps de nombres  $K$ , on note  $\overline{K}$  sa clôture algébrique et  $G_K = \text{Gal}(\overline{K}/K)$  le groupe de Galois absolu. On étudie dans ce papier la variation de la hauteur de Faltings dans une classe de  $\overline{K}$ -isogénie. On obtient le résultat suivant:

**Théorème 1.1** *Soit  $E$  une courbe elliptique semi-stable sur un corps de nombres  $K$  et sans multiplication complexe. Soit  $n$  un entier et  $n = \prod_{i=1}^r p_i^{\alpha_i}$  sa décomposition en facteurs premiers. Soit  $P$  un point de torsion de  $E$  d'ordre exactement  $n$  défini sur le corps  $K(P)$ . Soit  $\pi : E \rightarrow E'$  la  $K(P)$ -isogénie dont le noyau est le sous-groupe engendré par  $P$ . Si le groupe  $G_K$  agit transitivement sur les points d'ordre exactement  $n$ , on a :*

$$h(E') = h(E) + \frac{\log n}{2} - \sum_{i=1}^r \frac{p_i^{\alpha_i} - 1}{(p_i^2 - 1)p_i^{\alpha_i - 1}} \log p_i. \quad (2)$$

De manière générale on a :

$$h(E') = h(E) + \frac{\log n}{2} - \sum_{i=1}^r \frac{p_i^{\alpha_i} - 1}{(p_i^2 - 1)p_i^{\alpha_i - 1}} \log p_i + O(1) \quad (3)$$

où  $O(1)$  ne dépend que de la courbe elliptique  $E$ .

On peut remarquer [7] que les propriétés élémentaires de la hauteur de Faltings nous assurent qu'avec les hypothèses précédentes, on a toujours des inégalités de la forme:

$$h(E) - \frac{\log n}{2} \leq h(E') \leq h(E) + \frac{\log n}{2}.$$

Remarquons aussi que le théorème de l'image ouverte de Serre nous assure que  $G_K$  agit transitivement sur les points d'ordre exactement  $n$  dans de nombreux cas. Par exemple pour toute courbe elliptique semi-stable sur  $\mathbb{Q}$  et pour tout nombre premier  $p$  supérieur ou égal à 11, il résulte des travaux de Serre [8] et Mazur [6] que  $G_K$  agit transitivement sur les points d'ordre exactement  $p^n$ , pour un entier arbitraire  $n$ . En fait les deux outils principaux de la démonstration du théorème 1.1 sont la théorie d'Arakelov des courbes elliptiques et le théorème de l'image ouverte de Serre. Ce sera l'objet des parties 2 et 3.

Dans la partie 4, on étudie la répartition des points de torsion dans les fibres de mauvaise réduction de  $E$ . Soit  $X$  le modèle minimal non singulier de  $E$  qui sera supposé semi-stable et  $O$  la section unité. Soit  $P$  un point de  $E$  à valeurs dans  $\overline{K}$ . On note  $L = K(P)$  le corps de définition de  $P$  et  $E_P$  la section correspondante. On note  $\Phi_P$  un diviseur vertical à coefficients rationnels tel que pour tout diviseur vertical  $F$ , on ait sur  $O_L$

$$(E_P - O + \Phi_P, F) = 0,$$

où  $(, )$  désigne l'intersection d'Arakelov. Les diviseurs  $\Phi_P$  ne sont définis qu'à des multiples près des fibres de mauvaise réduction. Cependant leur auto-intersection  $\frac{-\Phi_P^2}{[L : \mathbb{Q}]}$  est indépendante du choix de  $\Phi_P$  et du choix d'un corps de rationalité  $L$  du point  $P$  et mesure en un sens la distance du point avec la composante neutre du modèle de Néron. En particulier on montre facilement ([13] proposition 4-3) que pour tout point  $P$  dans  $E(\overline{K})$  on a

$$0 \leq \frac{-\Phi_P^2}{[L : \mathbb{Q}]} \leq \frac{1}{4} \frac{\log N_{K/\mathbb{Q}} \Delta_E}{[K : \mathbb{Q}]}$$

et que  $\frac{1}{[L:\mathbb{Q}]} \phi_P^2 = 0$  si et seulement si le point  $P$  est partout dans la composante neutre du modèle de Néron de  $E$ . Le résultat principal de cette partie est le théorème suivant:

**Théorème 1.2** *Soit  $E$  une courbe elliptique semi-stable et sans multiplication complexe définie sur un corps de nombres  $K$ . Pour tout point de torsion  $P$  de  $E$ , à valeurs dans la clôture algébrique  $\overline{K}$  de  $K$ , d'ordre exactement  $n$  on a:*

$$-\frac{\Phi_P^2}{[K(P):\mathbb{Q}]} = \frac{1}{6} \frac{\log N_{K/\mathbb{Q}} \Delta_E}{[K:\mathbb{Q}]} + O\left(\frac{d(n)}{n^2}\right) \quad (4)$$

où  $d(n)$  désigne le nombre de diviseurs de  $n$ . De plus si  $G_K = \text{Gal}(\overline{K}/K)$  agit transitivement sur les points d'ordre exactement  $n$ , alors

$$-\frac{\Phi_P^2}{[K(P):\mathbb{Q}]} = \frac{1}{6} \frac{\log N_{K/\mathbb{Q}} \Delta_E}{[K:\mathbb{Q}]} \quad (5)$$

Dans la partie 5, on utilise ce dernier résultat pour étudier la variation du discriminant dans la classe de  $\overline{K}$ -isogénie d'une courbe elliptique semi-stable sur un corps de nombres  $K$ . On obtient le résultat suivant :

**Théorème 1.3** *Soit  $K$  un corps de nombres,  $E$  une courbe elliptique semi-stable sur  $K$ . Soit  $P$  un point de torsion de  $E$ , d'ordre exactement  $n$ , définie sur le corps  $L = K(P)$ . Soit  $E'$  la courbe elliptique définie sur  $L$  obtenue en quotientant  $E$  par le groupe cyclique engendré par  $P$ . Si  $G = \text{Gal}(\overline{K}/K)$  agit transitivement sur les points d'ordre exactement  $n$ , alors*

$$\frac{\log N_{K(P)/\mathbb{Q}} \Delta_{E'}}{[K(P):\mathbb{Q}]} = \frac{\log N_{K/\mathbb{Q}} \Delta_E}{[K:\mathbb{Q}]}.$$

De manière générale,  $\frac{\log N_{K(P)/\mathbb{Q}} \Delta_{E'}}{[K(P):\mathbb{Q}]}$  est uniformément borné quand  $P$  décrit l'ensemble des points de torsion de  $E$ .

Dans la partie 6, après quelques préliminaires sur les fonctions de Green canoniques sur les courbes elliptiques, on borne la variation du terme à l'infini de la hauteur de Faltings dans une classe de  $\overline{K}$ -isogénie de courbe elliptique définie sur  $K$ . Le théorème 1.1 s'obtient en combinant les résultats de ces deux parties et en utilisant des propriétés géométriques élémentaires des points de torsion d'une courbe elliptique.

Dans la partie 7, on donne l'interprétation modulaire du théorème 1.1 et on fait le lien avec les travaux de Silverman sur les points de Hecke [10].

Nous remercions Ahmed Abbes et Etienne Fouvry pour leur aide lors de la préparation de ce travail.

## 2 Théorie d'Arakelov des courbes elliptiques

Soit  $K$  un corps de nombres,  $\mathcal{O}_K$  son anneau d'entiers,  $S_K$  (resp  $S_{\infty, K}$ ) l'ensemble des places finies (resp infinies) de  $K$ . On appelle surface arithmétique un modèle régulier  $X$  sur  $\mathcal{O}_K$  d'une courbe  $X_K$  de genre  $g \geq 1$  lisse et géométriquement connexe sur  $K$ . Pour toute place à l'infini  $\sigma$ , on note  $K_\sigma$  le complété de  $K$  en la place  $\sigma$  et  $X_\sigma$  la surface de Riemann obtenue à partir de  $X_K$  en faisant le changement de base défini par  $\sigma$ . On munit chaque  $X_\sigma$  de la métrique canonique d'Arakelov  $d\mu_\sigma = \frac{i}{2g} \sum_{i=1}^g \omega_{i,\sigma} \wedge \bar{\omega}_{i,\sigma}$  où  $(\omega_{i,\sigma})$  est une base

orthonormée de  $H^0(X_\sigma, \Omega_{X_\sigma}^1)$  pour le produit scalaire  $\langle \alpha, \beta \rangle = \frac{i}{2} \int_{X_\sigma} \alpha \wedge \bar{\beta}$ .

Un fibré inversible hermitien admissible sur  $X$  est la donnée d'un fibré inversible sur  $X$  dont toutes les fibres à l'infini  $L_\sigma$  sur  $X_\sigma$  sont munies d'une structure hermitienne dont la courbure  $\Theta_\sigma$  vérifie l'égalité:

$$\Theta_\sigma = -2i\pi \deg(L)d\mu_\sigma$$

Arakelov [1] a construit une théorie des intersections pour les fibrés inversibles hermitiens admissibles sur les surfaces arithmétiques. On pourra trouver les propriétés principales de cette théorie dans [1, 2, 5, 11]. Notons tout de même qu'Arakelov a introduit pour toute surface de Riemann  $\chi$  munie de sa métrique canonique  $d\mu$  une fonction de Green canonique  $g(z, w)$  qui est  $C^\infty$  sur  $\chi \times \chi - \Delta$  ( $\Delta$  désigne la diagonale) vérifiant:

$$\begin{aligned} i) \quad & \partial_z \partial_{\bar{z}} g(z, w) = i\pi(d\mu(z) - \delta_w) \\ ii) \quad & \int_\chi g(z, w) d\mu(z) = 0 \quad \forall w \in \chi \end{aligned}$$

où  $\delta_w$  est l'opérateur de Dirac en  $w$ . Pour tout point  $P$  de  $\chi$ , on note  $1_P$  la section canonique du fibré inversible  $\mathcal{O}(P)$ . On munit alors  $\mathcal{O}(P)$  de la métrique définie par  $\|1_P\|(Q) = \exp(g(P, Q))$ . En imposant que l'isomorphisme  $\mathcal{O}(D + D') = \mathcal{O}(D) \otimes \mathcal{O}(D')$  soit une isométrie pour tout diviseur  $D$  et  $D'$  sur  $\chi$ ,

on obtient une métrique dite canonique sur tout les fibrés inversibles de la forme  $\mathcal{O}(D)$ . Pour tout diviseur horizontal  $D$  sur une surface arithmétique, on munit en chaque place à l'infini  $\mathcal{O}(D)$  de cette métrique canonique. De cette manière  $\mathcal{O}(D)$  peut être vu comme un fibré inversible hermitien admissible sur  $X$ . On dispose ainsi d'une théorie des intersections pour les diviseurs compactifiés de  $X$  qui sera utilisé dans la suite. On notera dans la suite  $(L, L')_K$  l'intersection d'Arakelov de deux fibrés inversibles hermitiens et  $(L, L')$  cette même intersection quand il n'y aura pas d'ambiguïté sur le corps de base. Pour deux diviseurs compactifiés  $D$  et  $D'$ , on notera  $(D, D') = (\mathcal{O}(D), \mathcal{O}(D'))$  et  $D^2 = (D, D)$ . L'intersection de deux sections  $E_P$  et  $E_Q$  correspondant à des points  $L$ -rationnels  $P$  et  $Q$  distincts est donné par

$$(E_P.E_Q) = \sum_{v \in S_L} (E_P.E_Q)_v \log N(v) - \sum_{\sigma \in S_{\infty, L}} g_{\sigma}(P^{\sigma}, Q^{\sigma}) \quad (6)$$

où  $(E_P, E_Q)_v$  désigne l'intersection géométrique des sections  $E_P$  et  $E_Q$  en la place finie  $v$  de  $L$  et  $N(v)$  désigne la norme de  $v$ . On note aussi  $(E_P.E_Q)_{Fin}$  la partie à distance finie de l'intersection d'Arakelov des sections  $E_P$  et  $E_Q$ .

Dans la suite on notera  $f : X \rightarrow \text{Spec } \mathcal{O}_K$  la surface arithmétique, non singulière, minimale de fibre générique  $E \rightarrow \text{Spec } K$  une courbe elliptique sur  $K$ . On note  $\mathcal{O}$  la section unité. Soit  $\Delta_{E/K}$  son discriminant minimal. On suppose que  $X$  est muni des métriques canoniques d'Arakelov en toute place à l'infini. Le fibré inversible  $\omega_{X/\mathcal{O}_K}$ , dualisant relatif de  $X$  sur  $\mathcal{O}_K$ , est alors muni d'une métrique dite canonique en toute place à l'infini  $\sigma$  qui fait de  $\omega_{X/\mathcal{O}_K}$  un fibré inversible hermitien admissible sur  $X$ . Cette métrique canonique est caractérisée par le fait qu'en toute place à l'infini  $\sigma$  et pour tout point  $P$  sur  $X_{\sigma}$ , l'isomorphisme résidu :

$$\Omega_{X_{\sigma}}^1(P) = \Omega_{X_{\sigma}}^1 \otimes \mathcal{O}_{X_{\sigma}}(P) \xrightarrow{\sim} \mathbb{C}$$

est une isométrie quand  $\mathcal{O}_{X_{\sigma}}(P)$  est muni de sa métrique canonique admissible. Soit  $E$  une courbe elliptique semi-stable sur  $K$ , on désigne par  $\deg(\omega_{X/\mathcal{O}_K})$  le degré d'Arakelov de l'image directe de son dualisant relatif. Szpiro [12] prouve la relation :

$$d_E = -\frac{\mathcal{O}^2}{[K : \mathbb{Q}]} = \frac{\deg(\omega_{X/\mathcal{O}_K})}{[K : \mathbb{Q}]} = \frac{1}{12} \frac{\log N_{K/\mathbb{Q}} \Delta_E}{[K : \mathbb{Q}]} \quad (7)$$

où  $d_E$  est définie par cette égalité et  $N_{K/\mathbb{Q}}$  désigne la norme de  $K$  à  $\mathbb{Q}$ .

### 3 Orbites sous Galois et théorème de l'image ouverte de Serre

Dans cette partie on décrit les orbites sous Galois des points de torsion d'une courbe elliptique sans multiplication complexe. Nous traduisons simplement le théorème de l'image ouverte de Serre sous la forme qui nous sera utile dans la suite.

Soit  $E$  une courbe elliptique sur un corps de nombres  $K$  sans multiplication complexe. On désigne par  $E[n]$  l'ensemble des points de  $n$  torsion de  $E$  et par  $\overline{E}[n]$  l'ensemble des points qui sont d'ordre exactement  $n$ . On pose  $K_n = K(E[n])$  l'extension minimale de  $K$  contenant les coordonnées des points de  $n$ -torsion. Une famille  $(P_n, Q_n)$ ,  $n \in \mathbb{N}$  est appelé base cohérente de points de torsion de  $E$ , si pour tout  $n$ ,  $(P_n, Q_n)$  est une base de  $E[n]$  et si pour tout diviseur  $d$  de  $n$  on a  $dP_n = P_{\frac{n}{d}}$  et  $dQ_n = Q_{\frac{n}{d}}$ . On fixe dans la suite une telle base cohérente  $(P_n, Q_n)$ . Pour tout  $n$  dans  $\mathbb{N}$ , on note  $H_n$  l'image de la représentation :

$$\rho_n : G = \text{Gal}(\overline{K}/K) \longrightarrow \text{Gl}(2, \mathbb{Z}/n\mathbb{Z})$$

décrivant l'action du groupe de Galois sur les points de  $n$ -torsion dans la base cohérente  $(P_n, Q_n)$ . Quand  $n$  divise  $m$  on note  $\pi_{m,n} : \text{Gl}(2, \mathbb{Z}/m\mathbb{Z}) \rightarrow \text{GL}(2, \mathbb{Z}/n\mathbb{Z})$  le morphisme de réduction modulo  $n$ . Pour tout entier  $n$ , on appelle support de  $n$  et on note  $\text{supp}(n)$  l'ensemble des nombres premiers divisant  $n$ . Le théorème de l'image ouverte de Serre [8] affirme l'existence d'un entier  $n_0$  dépendant de  $E$  qui décompose et stabilise la représentation du groupe de Galois sur les points de torsion en le sens suivant: Pour tout entier  $n = n_1 n_2$  avec  $\text{supp}(n_1) \subset \text{supp}(n_0)$  et  $\text{supp}(n_2) \cap \text{supp}(n_0) = \emptyset$  on a  $H_n = H_{n_1} \times \text{GL}(2, \mathbb{Z}/n_2\mathbb{Z})$ . De plus l'entier  $r_0 = \text{pgcd}(n_1, n_0)$  est tel que  $H_{n_1} = \pi_{n_1, r_0}^{-1}(H_{r_0})$ .

**Proposition 3.1** *Soit  $E$  une courbe elliptique sans multiplications complexes définie sur un corps de nombres  $K$ . Soit  $n, n_0, n_1, n_2$  et  $r_0$  comme précédemment.*

- 1) *L'orbite sous  $G$  d'un point  $P$  d'ordre exactement  $n_2$  est  $\overline{E}[n_2]$ .*
- 2) *L'orbite sous  $G$  d'un point  $P$  d'ordre exactement  $n_1$  contient les points de la forme  $P + E[\frac{n_1}{r_0}]$ .*
- 3) *Soit  $\lambda$  et  $\mu$  dans  $\mathbb{Z}$  tels que  $\lambda n_1 + \mu n_2 = 1$ . L'orbite sous  $G$  d'un point  $P$  d'ordre exactement  $n$  contient les points de la forme  $(\mu n_2)P + \overline{E}[n_2] + E[\frac{n_1}{r_0}]$ .*

*Preuve.* Soit  $P$  un point d'ordre exactement  $n$ . En remplaçant  $H_n$  par un conjugué de  $H_n$ , on peut supposer que  $P = P_n$ . On pose alors  $Q = Q_n$ . Le groupe  $H_n$  contient  $\pi_{n_1, r_0}^{-1}(Id) \times \mathrm{GL}(2, \mathbb{Z}/n_2\mathbb{Z})$ .  $H_n$  contient donc:

$$H'_n = \begin{pmatrix} \lambda n_1 a + \mu n_2(1 + r_0 \alpha) & \lambda n_1 b + \mu n_2 r_0 \beta \\ \lambda n_1 c + \mu n_2 r_0 \gamma & \lambda n_1 d + \mu n_2(1 + r_0 \delta) \end{pmatrix}$$

où  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  décrit  $\mathrm{GL}(2, \mathbb{Z}/n_2\mathbb{Z})$  et  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  décrit  $M_2(\mathbb{Z}/n_1\mathbb{Z})$ . Donc l'orbite de  $P$  contient les points de la forme  $(\lambda n_1 a + \mu n_2(1 + r_0 \alpha))P + (\lambda n_1 c + \mu n_2 r_0 \gamma)Q$ . Ceci montre le point 3. Le point 2 s'obtient avec  $\lambda = 0$  et  $\mu = 1$ . Le point 1 est clair.

**Corollaire 3.2** *Soit  $E$  une courbe elliptique sur un corps de nombres  $K$  sans multiplication complexe. Le nombre d'orbites de l'action de  $G_K$  sur  $\overline{E}[n]$  est uniformément borné.*

*Preuve.* Soit  $n_0$  un entier qui décompose et stabilise la représentation du groupe de Galois  $G_K$  sur les points de torsion de  $E$ . La proposition prouve en fait que le nombre d'orbites en question est borné par  $n_0^2$ .

## 4 Répartition des points de torsion dans les fibres de mauvaise réduction

Le but de cette section est de montrer le théorème 1.2. On en montre en fait une version plus précise par sa nature locale sur  $K$ . Soit  $E$  une courbe elliptique sur un corps de nombres  $K$ . Soit  $X$  son modèle minimal non singulier supposé semi-stable. Pour tout point  $P$  de  $E$  à valeurs dans  $\overline{K}$ , on note  $K(P)$  son corps de définition et  $E_P$  la section correspondante. Pour tout point  $P$  et  $Q$  rationnels sur un corps  $L$  on note  $\Phi_{P,Q}$  un diviseur vertical à coefficients rationnels tel que pour tout diviseur vertical  $F$ , on ait sur  $O_L$

$$(E_P - E_Q + \Phi_{P,Q}.F) = O. \quad (8)$$

Quand  $Q = O$  on pose  $\Phi_{P,O} = \Phi_P$ . Les diviseurs  $\Phi_{P,Q}$  ne sont définis qu'à des multiples près des fibres de mauvaise réduction, mais la quantité  $\frac{-\Phi_{P,Q}^2}{[L : \mathbb{Q}]}$

est indépendante du choix de  $\Phi_{P,Q}$  et du choix d'un corps de rationalité  $L$  des points  $P$  et  $Q$ . Le lien entre l'intersection d'Arakelov et la hauteur de Néron-Tate est donné par la formule de Faltings–Hriljac [2, 4]. Pour tout point  $R$  de  $E(\overline{K})$ , on note  $h_{NT}(R)$  la hauteur de Néron-Tate de  $R$ . Pour tout point  $P$  et  $Q$  de  $E$  à valeurs dans une extension  $L$  de  $K$ , on a  $h_{NT}(P - Q) = -\frac{1}{2[L : \mathbb{Q}]}(E_P - E_Q + \Phi_{P,Q})^2$ . On peut décomposer  $\Phi_{P,Q}$  comme une somme sur toutes les places  $w$  de  $L$  de mauvaise réduction de  $E$ . On écrit cette décomposition  $\Phi_{P,Q} = \sum_{w \in S_L} \Phi_{P,Q,w}$  de sorte qu'on a une égalité de la forme:

$$-\Phi_{P,Q}^2 = \sum_{w \in S_L} -\Phi_{P,Q,w}^2 \log N(w) \quad (9)$$

où  $N(w)$  désigne la norme de l'idéal  $w$ . Pour toute place  $v$  de  $K$ , on écrit aussi cette dernière décomposition sous la forme  $-\Phi_{P,Q,v}^2 \log N(v) = \sum_{w/v} \frac{-\Phi_{P,Q,w}^2 \log N(w)}{[L : K]}$  où la somme précédente porte sur toutes les places  $w$  de  $L$  divisant  $v$ . Quand  $Q = O$ , on note naturellement  $\Phi_{P,O,w} = \Phi_{P,w}$  et  $\Phi_{P,O,v}^2 = \Phi_{P,v}^2$  pour toute place  $v$  de  $K$  et  $w$  de  $L$ . La version locale du théorème 1.2 est :

**Théorème 4.1** *Soit  $E$  une courbe elliptique semi-stable sur un corps de nombres  $K$ . Pour tout point de torsion  $P$  de  $E$ , à valeurs dans la clôture algébrique  $\overline{K}$  de  $K$ , d'ordre exactement  $n$  et pour toute place  $v$  de  $K$ , on a:*

$$\frac{-\phi_{P,v}^2 \log N(v)}{[K : \mathbb{Q}]} = \sum_{w/v} \frac{-\Phi_{P,w}^2 \log N(w)}{[K(P) : \mathbb{Q}]} = \frac{v(\Delta_E) \log N(v)}{6[K : \mathbb{Q}]} + O\left(\frac{d(n)}{n^2}\right) \quad (10)$$

où  $d(n)$  désigne le nombre de diviseurs de  $n$ . Si  $G_K = \text{Gal}(\overline{K}/K)$  agit transitivement sur les points d'ordre exactement  $n$ , alors

$$\frac{-\phi_{P,v}^2 \log N(v)}{[K : \mathbb{Q}]} = \sum_{w/v} \frac{-\Phi_{P,w}^2 \log N(w)}{[K(P) : \mathbb{Q}]} = \frac{v(\Delta_E) \log N(v)}{6[K : \mathbb{Q}]} \quad (11)$$

Enfin quand  $n$  est de la forme  $p^r$  pour un nombre premier  $p$ , on a l'égalité

$$\frac{-\phi_{P,v}^2 \log N(v)}{[K : \mathbb{Q}]} = \frac{v(\Delta_E) \log N(v)}{6[K : \mathbb{Q}]} + O\left(\frac{1}{n^2}\right) \quad (12)$$

où les constantes implicites ne dépendent que de  $E$

On obtient le théorème 1.2 en sommant sur toutes les places de mauvaise réduction de  $K$  les égalités obtenues dans cet énoncé local.

La proposition suivante due à Szpiro [12] explique comment on calcule les  $-\Phi_{P,w}^2$ :

**Proposition 4.2 (Szpiro)** *Soit  $V$  un anneau de valuation discrète,  $f : E \rightarrow V$  une courbe elliptique dont la fibre générique est lisse et la fibre spéciale est un cycle de  $\mathbf{P}^1$  de self-intersection  $-2$ . Soit  $F_0, \dots, F_{\alpha-1}$  les composantes de cette fibre spéciale. Si  $E_P$  et  $E_Q$  sont deux sections telles que  $(E_P.F_0) \neq 0$  et  $(E_Q.F_k) \neq 0$ , le diviseur à coefficients rationnels vertical  $\Phi_{P,Q}$  définie à un multiple de la fibre spéciale près par l'équation  $((E_P - E_Q + \Phi_{P,Q}).F_i) = 0$  pour tout  $i$  est donné par:*

$$-\Phi_{P,Q}^2 = \frac{k(\alpha - k)}{\alpha} = \frac{\alpha}{6} - \frac{\alpha}{\pi^2} \sum_{l=1}^{\infty} \frac{\cos 2\pi l \frac{k}{\alpha}}{l^2} \quad (13)$$

Pour tout entier  $n$ , on note  $\Theta(n)$  le nombre de points de torsion d'ordre exactement  $n$  et  $\mu(n)$  la fonction de Moebius (l'unique fonction multiplicative telle que  $\mu(1) = 1$ ,  $\mu(p) = -1$  et  $\mu(p^k) = 0$  pour tout nombre premier  $p$  et tout entier  $k \geq 2$ ).

**Lemme 4.3** *Soit  $V$  un anneau de valuation discrète,  $f : E \rightarrow V$  une courbe elliptique dont la fibre générique est lisse et la fibre spéciale est un cycle de  $\mathbf{P}^1$  de self intersection  $-2$  de longueur  $n_v$ . On suppose que les points de  $n$  torsion de  $E$  sont rationnels sur le corps des fractions  $L$  de  $V$ . Pour tout point  $P_0$  rationnel  $L$ , on a :*

$$\sum_{Q \in E[n]} -\Phi_{P_0+Q}^2 = (n^2 - 1) \frac{n_v}{6} - \Phi_{nP_0}^2 \quad (14)$$

$$\sum_{Q \in \overline{E}[n]} -\Phi_{P_0+Q}^2 = \Theta(n) \frac{n_v}{6} - \sum_{d/n} \mu\left(\frac{n}{d}\right) \Phi_{dP_0}^2 \quad (15)$$

*Preuve.* Le deuxième point découle du premier par la formule d'inversion de Moebius quand on a remarqué que

$$\Theta(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) d^2 = \sum_{d/n} \mu\left(\frac{n}{d}\right) (d^2 - 1).$$

Comme les points de  $n$  torsion sont rationnels sur  $L$ , on a  $n_v = n\alpha$  pour un entier  $\alpha$ . Si on note  $F_0, F_1, \dots, F_{n_v-1}$  les composantes irréductibles de la fibre spéciale, les points de  $n$  torsion se répartissent en  $n$  paquets de  $n$  points sur les composantes  $F_{\lambda\alpha}$  avec  $\lambda \in \{0, 1, \dots, n-1\}$ . On suppose que le point  $P_0$  passe par la composante  $F_{r_0}$ , et on note  $x_0 = \frac{r_0}{n_v}$ . D'après (13) on a :

$$\begin{aligned} \sum_{Q \in E[n]} -\Phi_{P_0+Q}^2 &= n^2 \frac{n_v}{6} - \frac{n_v}{\pi^2} \sum_{k=1}^{\infty} \frac{n}{k^2} \sum_{\lambda=0}^{n-1} \cos 2\pi k \left(x_0 + \frac{\lambda\alpha}{n_v}\right) \\ &= n^2 \frac{n_v}{6} - \frac{n_v}{\pi^2} \sum_{k=1}^{\infty} \frac{1}{k^2} \cos 2\pi n k x_0 \\ &= (n^2 - 1) \frac{n_v}{6} - \Phi_{nP_0}^2. \end{aligned}$$

**Lemme 4.4** *Soit  $V$  un anneau de valuation discrète,  $f : E \rightarrow V$  une courbe elliptique dont la fibre générique est lisse et la fibre spéciale est un cycle de  $\mathbf{P}^1$  de self intersection  $-2$  de longueur  $n_v$ . Soit  $n_1$  et  $n_2$  deux nombres premiers entre eux. On suppose que les points de  $n_1 n_2$  torsion de  $E$  sont rationnels sur le corps des fractions  $L$  de  $V$ . Pour tout point  $P_0$  rationnel  $L$ , on a :*

$$A = \sum_{P \in P_0 + E[n_1] + \bar{E}[n_2]} -\Phi_P^2 = n_1^2 \Theta(n_2) \frac{n_v}{6} - \sum_{d/n_2} \mu\left(\frac{n_2}{d}\right) \Phi_{n_1 d P_0}^2. \quad (16)$$

*Preuve.* On a  $A = - \sum_{Q \in \bar{E}[n_2]} \sum_{P \in E[n_1]} \Phi_{(P_0+Q)+P}^2$ . Par le lemme 4.3, on a

donc :

$$A = \Theta(n_2) (n_1^2 - 1) \frac{n_v}{6} + \sum_{Q \in \bar{E}[n_2]} -\Phi_{n_1 P_0 + n_1 Q}^2.$$

On montre le lemme en remarquant que comme  $n_1$  et  $n_2$  sont premiers entre eux la multiplication par  $n_1$  est une bijection de  $\bar{E}[n_2]$  sur  $\bar{E}[n_2]$  et en appliquant une nouvelle fois le lemme 4.3.

*Preuve du théorème 4.1.*

Comme les  $-\Phi_{P,v}^2$  sont invariants par l'action de  $G$ , on peut les calculer comme une moyenne sur des conjugués de  $P$  par l'action du groupe de Galois  $G_K$ . Soit donc  $P$  un point d'ordre exactement  $n$ . Soit  $L$  un corps de rationalité des points de  $E$  d'ordre  $n$ .

Quand  $G_K$  agit transitivement sur les points d'ordre exactement  $n$ , on a:

$$\frac{-\Phi_{P,v}^2}{[K:\mathbb{Q}]} = \frac{1}{\Theta(n)} \sum_{Q \in E[n]} \frac{-\Phi_{Q,v}^2}{[K:\mathbb{Q}]} = \frac{1}{\Theta(n)} \sum_{w/v} \sum_{Q \in E[n]} \frac{-\Phi_{Q,w}^2}{[L:\mathbb{Q}]} \quad (17)$$

En utilisant l'équation (15) avec  $P_0 = 0$  on obtient le théorème dans ce cas.

Quand  $n = p^r$ , d'après le théorème de Serre et l'énoncé précédent il n'y a qu'un nombre fini de nombre premier  $p$  à considérer. D'après la proposition 3.1, il existe  $r_0$  tel que pour tout  $r \geq r_0$ , l'orbite sous Galois de  $P$  contient  $P + E[\frac{p^r}{p^{r_0}}]$ . On applique la méthode précédente en utilisant l'équation (14) pour obtenir le théorème dans ce cas.

Dans le cas général, on fixe un entier  $n_0$  qui décompose et stabilise la représentation de  $G = \text{Gal}(\bar{K}/K)$ , comme dans la section 3. On écrit  $n$  sous la forme  $n = n_1 n_2$  avec  $\text{supp}(n_1) \subset \text{supp}(n_0)$  et  $\text{supp}(n_2) \cap \text{supp}(n_0) = \emptyset$ . On pose  $r_1 = \text{pgcd}(n_0, n_1)$  de sorte que

$$H_n = \pi_{n_1, r_1}^{-1}(H_{r_1}) \times \text{GL}(2, \mathbb{Z}/n_2 \mathbb{Z}).$$

Soit  $\lambda$  et  $\mu$  tels que  $\lambda n_1 + \mu n_2 = 1$  et  $P_1 = \mu n_2 P$  Soit  $v$  une place de  $K$  de mauvaise réduction. En utilisant la proposition 3.1, on trouve:

$$\frac{-\Phi_{P,v}^2 \log N(v)}{[K:\mathbb{Q}]} = \frac{r_1^2}{n_1^2 \Theta(n_2)} \sum_{w/v} \sum_{P \in P_1 + E[\frac{n_1}{r_1}] + \bar{E}[n_2]} \frac{-\Phi_{P,w}^2 \log N(w)}{[L:\mathbb{Q}]}$$

Soit  $P_2 = \frac{n_1}{r_1} P_1$ . On calcule cette dernière somme à l'aide du lemme 4.3 en remarquant qu'en toute place  $w$  de  $L$  le nombre de composantes du modèle de Néron de  $E$  en  $w$  est  $w(\Delta_E)$  :

$$\frac{-\Phi_{P,v}^2 \log N(v)}{[K:\mathbb{Q}]} = \sum_{w/v} \frac{w(\Delta_E) \log N(w)}{6[L:\mathbb{Q}]} + \frac{r_1^2}{n_1^2 \Theta(n_2)} \sum_{d/n_2} \sum_{w/v} \frac{-\mu(\frac{n_2}{d}) \Phi_{dP_2,w}^2}{[L:\mathbb{Q}]}$$

On obtient alors le théorème 4.1 en remarquant que la fonction  $\Theta(x)$  est uniformément minorée par  $\frac{6x^2}{\pi^2}$  et que

$$\sum_{w/v} \frac{-\Phi_{dP_2,w}^2}{[L:\mathbb{Q}]}$$

est borné indépendamment de  $n$  et de  $d$ .

**Remarque** On perd en fait beaucoup d'information en faisant la majoration grossière qui conduit à un terme d'erreur en  $\frac{d(n)}{n^2}$ . Pour comprendre sa nature, on est amené à considérer des fonctions de la forme  $\psi(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right)g(\bar{n})$ , où  $\bar{n}$  désigne la classe de  $n$  modulo un entier  $n_0$  fixé à l'avance et  $g$  une fonction qui dans notre cas est complètement explicite. Il est facile de voir qu'en moyenne ces fonctions sont beaucoup plus petites que  $d(n)$ . Elles sont par exemple nulles dès que  $n$  est multiple d'un nombre premier congrue à 1 modulo  $n_0$ .

## 5 Variation du discriminant dans une classe de $\overline{K}$ -isogénie

Le but de cette partie est de démontrer le théorème 1.3. On commence par le lemme suivant :

**Lemme 5.1** *Soit  $E$  une courbe elliptique semi-stable sur un corps de nombres  $K$ . Soit  $P$  un point de torsion de  $E$ , d'ordre exactement  $n$ , définie sur le corps  $L = K(P)$  et soit  $E_P$  la section correspondante sur  $\mathcal{O}_L$ . Si  $G = \text{Gal}(\overline{K}/K)$  agit transitivement sur les points d'ordre  $n$  alors  $\frac{(E_P.O)}{[K(P) : \mathbb{Q}]} = 0$ . Dans tous les cas  $\frac{(E_P.O)}{[K(P) : \mathbb{Q}]} = O\left(\frac{d(n)}{n^2}\right)$  et si  $n = p^r$  est la puissance d'un nombre premier  $p$ , on a  $\frac{(E_P.O)}{[K(P) : \mathbb{Q}]} = O\left(\frac{1}{n^2}\right)$  pour une constante implicite ne dépendant que de  $E$ .*

*Preuve.* C'est une conséquence du théorème 1.2 et de l'équation (7) quand on a remarqué que par la formule de Faltings-Hriljac [2, 4], on a :

$$\frac{(E_P.O)}{[K(P) : \mathbb{Q}]} = -d_E - \frac{\Phi_P^2}{2[K(P) : \mathbb{Q}]}.$$

**Lemme 5.2** *Soit  $E$  une courbe elliptique semi-stable sur un corps de nombres  $L$ . Soit  $P$  et  $Q$  deux points rationnels sur  $L$  et  $E_P$  et  $E_Q$  les sections correspondantes sur  $\mathcal{O}_L$ . On a  $(E_P.E_Q) = (E_{P-Q}.O)$ , où  $E_{P-Q}$  désigne la section associée au point  $P - Q$ .*

*Preuve.* C'est à nouveau une conséquence du théorème de Faltings-Hriljac [2, 4]. Par cette formule on peut calculer la hauteur de Néron-Tate de deux manières différentes et on obtient:

$$(E_{P-Q} - O + \Phi_{P-Q})^2 = (E_P - E_Q - \Phi_{P,Q})^2.$$

Le lemme se démontre alors en remarquant que  $-\Phi_{P,Q}^2 = -\Phi_{P-Q}^2$ .

**Proposition 5.3 (Szpiro)** *Soit  $\pi : E \rightarrow E'$  une isogénie entre des courbes semi-stables définies sur un corps de nombres  $L$ . Supposons que son noyau  $H$  soit fini et déployé sur  $\mathcal{O}_L$ . Soit  $E_1, \dots, E_h$  les  $\mathcal{O}_L$ -points de  $H$ . On a :*

$$\sum_{i \neq j} \frac{(E_i, E_j)}{[L : \mathbb{Q}]} = h(d_E - d_{E'}). \quad (18)$$

La démonstration de cette proposition est donnée dans [12]. Pour tout point de torsion  $P$ , on note  $E / \langle P \rangle$  la courbe elliptique (sur  $K(P)$ ) obtenue en quotientant  $E$  par le sous-groupe cyclique engendré par  $P$ . Soit  $n$  un entier, on note  $r(n)$  le nombre de sous-groupes cycliques d'ordre  $n$  de  $E$ .

**Lemme 5.4** *Soit  $n$  un entier et  $(P_1, \dots, P_{r(n)})$  des générateurs des sous-groupes cycliques d'ordre  $n$  de  $E$ . Pour tout  $i \in [1, \dots, r(n)]$ , on a :*

$$d_E - d_{E/\langle P_i \rangle} = \sum_{j=1}^{n-1} (E_{jP_i}, O). \quad (19)$$

De plus on a en moyenne l'égalité :

$$\frac{1}{r(n)} \sum_{i=1}^{r(n)} d_{E/\langle P_i \rangle} = d_E. \quad (20)$$

*Preuve.* La première égalité résulte du lemme 5.2 et de la proposition 5.3 appliquée à l'isogénie cyclique engendrée par  $P_j$ . La deuxième s'obtient en sommant les égalités précédentes et en appliquant de nouveau la proposition 5.3 à la multiplication par  $n$ .

*Preuve du Théorème 1.3.* Quand le groupe de Galois  $G_K$  agit transitivement sur les points d'ordre exactement  $n$ , il agit aussi transitivement

sur les points d'ordre un diviseur de  $n$ . Le lemme 5.1 et l'équation (19) prouvent l'invariance du discriminant dans ce cas. Dans le cas général, soit  $P$  un point d'ordre exactement  $n$ . L'équation (19) et l'invariance par Galois de l'intersection d'Arakelov prouvent que pour tout  $\sigma \in G_K$  on a  $d_{E/\langle P^\sigma \rangle} = d_{E/\langle P \rangle}$ . D'après le corollaire 3.2,  $\{d_{E/\langle Q \rangle} \mid Q \in \overline{E}[n]\}$  a un cardinal uniformément borné quand  $n$  varie. Comme les  $d_{E/\langle P \rangle}$  sont minorés (par 0), prennent pour chaque  $n$  un nombre borné de valeurs et sont en moyenne égaux à  $d_E$  (20); ils sont uniformément bornés.

## 6 Estimation à l'infini

Dans cette partie on borne la variation du terme à l'infini de la hauteur de Faltings dans la classe de  $\overline{K}$ -isogénie d'une courbe elliptique  $E$  définie sur un corps de nombres.

Soit  $E$  une courbe elliptique sur  $\mathbb{C}$ . Soit  $\tau = a + ib$  dans le domaine fondamental de  $SL(2, \mathbb{Z})$  tel qu'on ait un isomorphisme  $E \simeq \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$ . Soit  $g_\tau(x, y)$  la fonction de Green canonique sur  $E$ . Elle est caractérisée par les propriétés suivantes :

$$\begin{aligned} i) \quad & g_\tau(z_1, z_2) = g_\tau(z_1 - z_2, O) \\ ii) \quad & \int_E g_\tau(O, z) dz \wedge d\bar{z} = 0 \\ iii) \quad & \frac{1}{i\pi} \partial_z \partial_{\bar{z}} g_\tau(O, z) = \frac{i}{2} \frac{dz \wedge d\bar{z}}{\text{Im}(\tau)} \end{aligned}$$

On en déduit alors le lemme suivant:

**Lemme 6.1** *Pour tout entier  $n$ ,*

$$\sum_{P \in E[n]} g_\tau\left(\frac{z_1}{n}, \frac{z_2}{n} + P\right) = g_\tau(z_1, z_2)$$

*Preuve.* La fonction du membre de gauche vérifie toutes les propriétés caractérisant la fonction de Green.

**Lemme 6.2** *Pour tout point  $Q \neq O$  de  $E$ , on a :*

$$i) \quad \sum_{P \in E[n]} g_\tau(Q + P, O) = g_\tau(nQ, O) \tag{21}$$

$$ii) \quad \sum_{P \in E[n] - O} g_\tau(P, O) = \log n \quad (22)$$

Quand  $n = p^\alpha$  pour un nombre premier  $p$

$$iii) \quad \sum_{P \in \overline{E}[p^\alpha]} g_\tau(P, O) = \log p \quad (23)$$

*Preuve.* Le premier point est un cas particulier du lemme précédent. On obtient le second point en faisant tendre  $z$  vers  $O$  dans l'égalité

$$\sum_{P \in E[n]} g_\tau(O, \frac{z}{n} + P) = g_\tau(O, z)$$

et en utilisant la singularité logarithmique de la fonction de Green-Arakelov au voisinage de  $O$ . Le dernier point s'obtient alors par la formule d'inversion de Moebius.

Par ailleurs Szpiro a calculé dans [12] la valeur de l'énergie du noyau d'une isogénie:

**Proposition 6.3 (Szpiro)** *Soit  $\pi : E \rightarrow E'$  une isogénie de courbes elliptiques semi-stables définies sur un corps de nombres  $L$ . Soit  $H$  le noyau de cette isogénie et  $h$  son degré. Pour chaque place archimédienne  $\sigma$  de  $K$  notons  $P_i^\sigma$ ,  $i = 1, \dots, h$ , les points de  $H$  sur  $E \otimes_\sigma \mathbb{C}$ . Alors on a*

$$\sum_{\sigma} \sum_{i \neq j} g(P_i^\sigma, P_j^\sigma) = \frac{[L : \mathbb{Q}]}{2} h \log h + \frac{h}{12} \sum_{\sigma} \log \frac{|\Delta(\tau'_\sigma)(\text{Im } \tau'_\sigma)^6|}{|\Delta(\tau_\sigma)(\text{Im } \tau_\sigma)^6|}. \quad (24)$$

Dans la suite, on fixe une courbe elliptique  $E$  sur un corps de nombres  $K$  à réduction semi-stable. Pour tout point  $P \neq O$  à valeurs dans  $K(P)$ , on pose

$$\phi_\infty(P) = \frac{1}{[K(P) : \mathbb{Q}]} \sum_{\sigma \in S_{\infty, K(P)}} g(P^\sigma, O). \quad (25)$$

Cette quantité ne dépend pas du corps de rationalité du point  $P$  et est invariante sous l'action du groupe de Galois  $G_K = \text{Gal}(\overline{K}/K)$ . On pose  $\phi_\infty(O) = 0$ . On se propose de calculer  $\phi_\infty(P)$  pour les points de torsion d'ordre une puissance d'un nombre premier  $p$ . Le calcul pour  $n$  quelconque se fait facilement en utilisant la proposition 3.1, mais il ne sera pas utilisé dans la suite. On rappelle que  $H_n$  désigne l'image de  $G$  dans  $\text{Gl}(2, \mathbb{Z}/n\mathbb{Z})$ .

**Lemme 6.4** Soit  $p$  un nombre premier et  $n = p^\alpha$ . Soit  $P$  un point d'ordre exactement  $p^\alpha$  de  $E$ . Si  $H_n$  agit transitivement sur les point d'ordre exactement  $n$ , on a :

$$\phi_\infty(P) = \frac{\log p}{\Theta(p^\alpha)}. \quad (26)$$

De manière générale, on a :

$$|\phi_\infty(P)| \leq \frac{c(p)}{p^{2\alpha}}, \quad (27)$$

pour une constante  $c(p)$  dépendant de  $p$  mais pas de  $\alpha$ .

*Preuve.* Si  $H_{p^\alpha}$  agit transitivement sur les points d'ordre exactement  $p^\alpha$ , on fixe un corps  $L$  contenant tous les points d'ordre  $p^\alpha$ . Par l'invariance sous  $G$  de la fonction  $\phi_\infty$ , on a :

$$\phi_\infty(P) = \frac{1}{\Theta(p^\alpha)} \sum_{Q \in \overline{E}[p^\alpha]} \phi_\infty(Q)$$

donc

$$\phi_\infty(P) = \frac{1}{[L : \mathbb{Q}]\Theta(p^\alpha)} \sum_{\sigma \in S_{\infty,L}} \sum_{Q \in \overline{E}_\sigma[p^\alpha]} g(Q, O). \quad (28)$$

On obtient la première partie du lemme en utilisant (22). Dans le cas où  $H_{p^\alpha}$  n'agit pas transitivement, on sait par le théorème de l'image ouverte de Serre et la proposition 3.1, qu'il existe un entier  $\alpha_0$  tel que pour tout  $\alpha \geq \alpha_0$  l'orbite du point  $P$  contient les points de  $P + E[p^{\alpha-\alpha_0}]$ . On fixe un corps  $L$  contenant tous les points d'ordre  $p^\alpha$ . Par l'invariance sous  $G$  de la fonction  $\phi_\infty$ , on a :

$$\phi_\infty(P) = \frac{p^{2\alpha_0}}{p^{2\alpha}} \sum_{Q \in P + E[p^{\alpha-\alpha_0}]} \phi_\infty(Q)$$

donc

$$\phi_\infty(P) = \frac{p^{2\alpha_0}}{p^{2\alpha}} \sum_{\sigma \in S_{\infty,L}} \sum_{Q \in E_\sigma[p^{\alpha-\alpha_0}]} g(O, P^\sigma + Q). \quad (29)$$

En utilisant (23), on trouve que

$$\phi_\infty(P) = \frac{p^{2\alpha_0}}{p^{2\alpha}} \phi_\infty(p^{\alpha-\alpha_0} P). \quad (30)$$

Comme  $p^{\alpha-\alpha_0}P$  est un point de  $E[p^{\alpha_0}]$ , on obtient le lemme. Notons par ailleurs que toujours d'après le théorème de l'image ouverte de Serre, il n'y a qu'un nombre fini de nombres premiers pour lesquels les hypothèses de la première partie du lemme ne soient pas vérifiées.

En reprenant les notations de la deuxième partie, on note  $n_o = \prod_{i=1}^s p_i^{r_i}$  un entier qui décompose et stabilise la représentation du groupe de Galois sur les points de torsion de  $E$ .

**Proposition 6.5** *Soit  $E$  une courbe elliptique sur un corps de nombres  $K$ . Soit  $P$  un point de  $E$  d'ordre exactement  $p^\alpha$ . Si  $H_{p^\alpha}$  agit transitivement sur les points d'ordre exactement  $p^\alpha$ , on a*

$$\sum_{i=1}^{p^\alpha-1} \phi_\infty(iP) = \frac{p^\alpha - 1}{(p^2 - 1)p^{\alpha-1}} \log p. \quad (31)$$

*Dans tous les cas, il existe une constante  $c > 0$  ne dépendant que de la courbe elliptique  $E$  telle que :*

$$\sum_{i=1}^{p^\alpha-1} \phi_\infty(iP) \leq c \quad (32)$$

*Preuve.* On rappelle que  $\varphi(x)$  désigne la fonction indicatrice d'Euler. Si  $H_{p^\alpha}$  agit transitivement sur les points d'ordre exactement  $p^\alpha$ , d'après (26), on a:

$$\sum_{i=1}^{p^\alpha-1} \phi_\infty(iP) = \sum_{j=1}^{\alpha} \frac{\varphi(p^j) \log p}{\Theta(p^j)}.$$

On obtient la proposition dans ce cas quand on a remarqué que  $\varphi(p^j) = p^{j-1}(p-1)$  et que  $\Theta(p^j) = p^{2j-2}(p^2-1)$ . Pour montrer le deuxième point, il suffit, compte tenu des résultats précédent de regarder le nombre fini de nombres premiers qui divisent  $n_0$ . On peut prendre  $c = \max_{p/n_0} c(p)$ . Pour tout  $P$  d'ordre  $p^\alpha$  avec  $p$  divisant  $n_0$ , on a :

$$\left| \sum_{i=1}^{p^\alpha-1} \phi_\infty(iP) \right| \leq \frac{c}{p^{2\alpha}} \sum_{i=0}^{\alpha-1} p^{2i} \varphi(p^{\alpha-i}) \leq \frac{c}{p} \leq c.$$

**Proposition 6.6** *Soit  $E$  une courbe elliptique semi-stable sur un corps de nombres  $K$ . Soit  $p$  un nombre premier et  $n = p^\alpha$  pour un  $\alpha \in \mathbb{N}^\times$ . Soit  $P$  un point de torsion de  $E$  d'ordre exactement  $n$  défini sur le corps  $K(P)$ . Soit  $\pi : E \rightarrow E'$  la  $K(P)$ -isogénie dont le noyau est le sous-groupe engendré par  $P$ . Pour tout  $\sigma$  plongement de  $K(P)$  dans  $\mathbb{C}$ , on choisit  $\tau_\sigma$  et  $\tau'_\sigma$  dans le demi-plan de Poincaré tels que  $E \otimes_\sigma \mathbb{C} \simeq E/\mathbb{Z} + \tau_\sigma \mathbb{Z}$  et  $E' \otimes_\sigma \mathbb{C} \simeq E'/\mathbb{Z} + \tau'_\sigma \mathbb{Z}$ . Si  $H_n$  agit transitivement sur les points d'ordre exactement  $n$ , on a :*

$$\frac{1}{12[K(P) : \mathbb{Q}]} \sum_\sigma \log \frac{|\Delta(\tau_\sigma)(\text{Im } \tau_\sigma)^6|}{|\Delta(\tau'_\sigma)(\text{Im } \tau'_\sigma)^6|} = \frac{\log p}{2} - \frac{p^\alpha - 1}{(p^2 - 1)p^{\alpha-1}} \log p \quad (33)$$

Dans le cas général, on a :

$$\frac{1}{12[K(P) : \mathbb{Q}]} \sum_\sigma \log \frac{|\Delta(\tau_\sigma)(\text{Im } \tau_\sigma)^6|}{|\Delta(\tau'_\sigma)(\text{Im } \tau'_\sigma)^6|} = \frac{\log p}{2} + O(1) \quad (34)$$

où le  $O(1)$  ne dépend que de la courbe elliptique  $E$ .

*Preuve.* cela résulte immédiatement des propositions 6.5 et 6.3.

## 7 Preuve du théorème 1.1

On a maintenant tous les outils pour montrer le théorème 1.1. On commence par le lemme suivant:

**Lemme 7.1** *Soit  $\pi : E \rightarrow E'$  une isogénie entre des courbes semi-stables définies sur un corps de nombres  $L$ . Supposons que son noyau  $H$  soit fini et déployé sur  $\mathcal{O}_L$ . Soit  $P_1, \dots, P_{h-1}$  les points non nuls de  $H$  et  $E_1, \dots, E_{h-1}$  les  $\mathcal{O}_L$ -sections de  $H$  correspondantes. On a :*

$$\sum_{i=1}^{h-1} \frac{(E_i, O)_{\text{Fin}}}{[L : \mathbb{Q}]} = \frac{\log h}{2} + h(E) - h(E') \quad (35)$$

*Preuve.* Cela résulte immédiatement des propositions 5.3 et 6.3, de la définition de la hauteur de Faltings (1) et du calcul de l'intersection d'Arakelov de 2 sections (6).

*Preuve du théorème 1.1.* On se place donc dans les hypothèses du théorème 1.1. On a donc un point  $P$  de  $E$  d'ordre  $n = \prod_{i=1}^r p_i^{\alpha_i}$ . On pose  $P_i = iP$  pour

$i$  variant de 1 à  $n - 1$ . On note aussi  $Q_i = \frac{n}{p_i^{\alpha_i}}P$  et  $E_i$  la courbe elliptique obtenue en quotientant  $E$  par le sous groupe cyclique engendrée par  $Q_i$ . On travaille sur le corps de définition  $L = K(P)$  du point  $P$ . Par le lemme 7.1 on a :

$$\sum_{i=1}^{n-1} \frac{(E_i P, O)_{Fin}}{[L : \mathbb{Q}]} = \frac{\log n}{2} + h(E) - h(E'). \quad (36)$$

Par ailleurs pour tout point  $Q$  de torsion dont l'ordre n'est pas une puissance d'un nombre premier, on a  $(E_Q, O)_{Fin} = 0$ . On a donc

$$\sum_{i=1}^{n-1} \frac{(E_i P, O)_{Fin}}{[L : \mathbb{Q}]} = \sum_{i=1}^r \sum_{j=1}^{p_i^{\alpha_i-1}} \left( \frac{(E_{jQ_i}, O)}{[L : \mathbb{Q}]} + \sum_{\sigma \in S_{\infty, L}} \frac{g_{\sigma}(jQ_i^{\sigma}, O)}{[L : \mathbb{Q}]} \right) \quad (37)$$

Pour tout  $i$  on a :

$$\sum_{j=1}^{p_i^{\alpha_i-1}} \frac{(E_{jQ_i}, O)}{[L : \mathbb{Q}]} = d_E - d_{E_i} \quad (38)$$

qui d'après le théorème 1.3 est nul si  $G_K$  agit transitivement sur les points d'ordre exactement  $p_i^{\alpha_i}$  et est uniformément borné de manière générale. De même pour tout  $i$  la proposition 6.5 nous assure que

$$\sum_{j=1}^{p_i^{\alpha_i-1}} \sum_{\sigma \in S_{\infty, L}} \frac{g_{\sigma}(jQ_i^{\sigma}, O)}{[L : \mathbb{Q}]} = \frac{p^{\alpha_i} - 1}{(p_i^2 - 1)p^{\alpha_i-1}} \log p \quad (39)$$

si  $G_k$  agit transitivement sur les points d'ordre exactement  $p^{\alpha_i}$  et est uniformément borné autrement. Si  $G_K$  agit transitivement sur les points d'ordre  $n$  il agit transitivement sur les points d'ordre  $p_i^{\alpha_i}$  pour tout  $i$  et on obtient la première partie du théorème 1.1. La deuxième partie s'obtient en remarquant que le théorème de l'image ouverte de Serre nous assure qu'il y a au plus un nombre fini de nombres premiers  $p$  pour lesquels  $G_K$  n'agit pas transitivement sur les points d'ordre  $p^{\alpha}$ .

## 8 Interprétation en terme de points de Hecke

Soit  $X = X(1)$  la courbe modulaire associée au groupe  $SL_2(\mathbb{Z})$ . La correspondance de Hecke induit pour tout  $m \in \mathbb{N}$  une application

$$T_m : X(\overline{\mathbb{Q}}) \longrightarrow \text{Div}_{\overline{\mathbb{Q}}}(X)$$

de degré  $\sigma_1(m)$  (somme des diviseurs de  $m$ ). Pour  $x \in X(\overline{\mathbb{Q}})$ , on pose

$$T_m(x) = \sum_{i=1}^{\sigma_1(m)} y_i \in \text{Div}_{\overline{\mathbb{Q}}}(X).$$

Silverman [10] appelle les  $y_i$  les  $m$ -ième points de Hecke associée à  $x$ . On définit une fonction hauteur  $h_F$  sur  $Y(\overline{\mathbb{Q}}) = X(\overline{\mathbb{Q}}) - \infty$  par la formule

$$h_F(x) = h_{F_s}(E_x)$$

où  $E_x$  est une courbe elliptique dont la classe est  $x$  et  $h_{F_s}$  désigne la hauteur de Faltings stable (calculée sur un corps où la courbe a réduction semi-stable). Par analogie avec [10], on pose pour tout point  $x \in Y(\overline{\mathbb{Q}})$  :

$$h_F(T_m(x)) = \sum_{i=1}^{\sigma_1(m)} h_F(y_i)$$

$$\text{si } T_m(x) = \sum_{i=1}^{\sigma_1(m)} y_i.$$

**Proposition 8.1** *Pour tout  $m = \prod_{i=1}^r p_i$  entier sans facteurs carrés et tout*

*$x \in Y(\overline{\mathbb{Q}})$ . On a*

$$\frac{1}{\sigma_1(m)} h_F(T_m(x)) = h_F(x) + \frac{\log m}{2} - \sum_{i=1}^r \frac{\log p_i}{p_i + 1}.$$

*De plus, si  $x$  n'est pas à multiplication complexe, quand  $m$  varie parmi les entiers sans facteurs carrés, on a*

$$h_F(y_m) = h_F(x) + \frac{\log m}{2} - \sum_{i=1}^r \frac{\log p_i}{p_i + 1} + O(1)$$

pour tout point de Hecke  $y_m$  d'ordre  $m$  associée à  $x$ . Il existe un entier  $r(x)$ , tel que pour tout entier sans facteurs carrés  $m = \prod_{i=1}^r p_i$ , avec  $p_i \geq r(x)$  pour tout  $i \in \{1 \dots r\}$  et tout point de Hecke  $y_m$  d'ordre  $m$  associé à  $x$  on a :

$$h_F(y_m) = h_F(x) + \frac{\log m}{2} - \sum_{i=1}^r \frac{\log p_i}{p_i + 1}$$

*Preuve.* Soit  $E_x$  une courbe elliptique dont la classe est  $x$ . On peut, en faisant une extension du corps de base supposer que  $E_x$  est à réduction semi-stable. Les points de Hecke d'ordre  $m$  sont les classes représentant les  $E_x/H$  où  $H$  parcourt les sous-groupes cycliques d'ordre  $m$  de  $E_x$ . Les deux derniers points ne sont alors qu'une simple réécriture du théorème 1.1. Le lecteur courageux démontrera le premier point en utilisant les arguments de moyenne qui apparaissent de manière récurrente dans la démonstration du théorème 1.1. Les méthodes de ce texte devraient permettre de donner une formule en moyenne pour la hauteur des points de Hecke de degré quelconque en utilisant les propriétés combinatoire des opérateurs de Hecke.

## Références

- [1] S. J. Arakelov, *Intersection theory of divisors on an arithmetic surface*, Math. USSR-Izv. **8**, (1974), 1167–1180.
- [2] G. Faltings, *Calculus on arithmetic surfaces*, Ann. of Math. **119**, (1984) 387–424.
- [3] M. Flexor et J. Oesterlé, *Sur les points de torsion des courbes elliptiques*, dans Séminaire sur les pinceaux elliptiques. Asterisque **183** (1990), 25–36.
- [4] P. Hriljac, *Splitting Fields of Principal Homogenous Spaces*, Lecture Notes in Math, vol **1240**, (1987), 214–229.
- [5] S. Lang, *Introduction to Arakelov Theory*, Springer-Verlag, New York, 1988.
- [6] B. Mazur, *Rational Isogenies of Prime Degree* Inventiones Math. **44** (1978), 129–162.

- [7] M. Raynaud, *Hauteurs et isogénies* dans "Seminaire sur les pinceaux arithmétiques" Astérisque **127**, (1985), 199–232.
- [8] J.-P. Serre, *Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math. **15**, (1972), 259–331.
- [9] J. H. Silverman, *Heights and elliptic curves*, Arithmetic Geometry, Springer-Verlag, New York, (1985), 253–265.
- [10] J. H. Silverman, *Hecke points on modular curves*, Duke Math. Journ., vol **60**, No. 2, (1990), 401–423
- [11] L. Szpiro, *Degrés, intersections, hauteurs*, Asterisque **127**, (1985), 11–28.
- [12] L. Szpiro, *Sur les propriétés numériques du dualisant relatif d'une surface arithmétique*, The Grothendieck Festschrift, Progr. Math, vol 3, Birkhäuser, Boston, (1990), 229–246.
- [13] E. Ullmo, *Points entiers, Points de torsion et amplitude arithmétique*, American Journal of Maths **117**, (1995), 1039–1055.