Hauteur des points de Heegner

Thomas Vidick

Août 2004

Table des matières

1 Introduction

Les points de Heegner sur une courbe elliptique ont été introduits par Heegner dans [], et leur étude s'est développée après la découverte par Gross et Zagier [GZ] d'un lien remarquable entre la hauteur de Néron-Tate de ces points et la valeur de la dérivée d'une série L en son centre de symétrie.

Dans ce rapport, on se pose la question de la dépendance de cette hauteur sur la courbe elliptique considérée, et en particulier sur son conducteur et sur le degré de sa paramétrisation modulaire. En effet, des calculs préliminaires montrent une grande variété de comportements de la hauteur des points de Heegner en fonction de la courbe elliptique, mais une relative uniformité lorsque l'on fixe la courbe.

Après quelques préliminaires sur les courbes elliptiques et les points de Heegner, nous analyserons l'algorithme qui nous a permis de calculer ces points et leurs hauteurs. Puis, nous montrerons une formule asymptotique pour les hauteurs de ces points (ainsi que pour la hauteur de leurs traces), et donnerons des résultats expérimentaux l'illustrant.

Remerciements

2 Préliminaires

Nous introduisons ici l'ensemble des notions qui seront nécessaires à la définition des points de Heegner sur une courbe elliptique, et à l'étude de leur hauteur. Nous commençons ainsi par rappeler un peu de théorie des courbes elliptiques sur les nombres complexes, puis sur les corps finis. Ensuite, nous donnons la définiton des différents types de séries L qui interviendront dans notre étude. Nous définissons la hauteur de Néron-Tate sur une courbe elliptique, puis nous expliquons comment une courbe elliptique peut s'obtenir à partir de la courbe modulaire $X_0(N)$. Finalement, nous donnons les théorèmes concernant le groupe de classe et la multiplication complexe qui nous seront utiles.

2.1 Courbes elliptiques

On commence par donner quelques définitions et propriétés concernant les courbes elliptiques. Pour plus de détails, je renvoie à [Si86], qui est la référence en la matière.

Définition 2.1. *Une* courbe elliptique *est une courbe de genre* 1 *munie d'un point particulier* O*. On dira que la courbe* E *est* définie sur le corps K *si elle l'est en tant que variété projective, et si* $O \in E(K)$*. On le notera* E/K*.*

Les corps K que l'on considérera se limitent essentiellement aux corps de nombres et aux corps finis.

On peut donner la forme générale de l'équation d'une courbe elliptique :

Théorème 2.2. *Soit* E *une courbe elliptique définie sur* K*.*

1. *Il existe des fonctions* $x, y \in K(E)$ *telles que l'application* $\Phi : E \to \mathbb{P}^2$ *définie par* $\Phi = [x, y, 1]$ *induise un isomorphisme de* E *sur une courbe définie par une équation de Weierstrass*

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,\ a_i \in K,$$

   et telle que $\Phi(O) = [0, 1, 0]$*. On appelle* x, y *des coordonnées de Weierstrass sur* E*.*

2. *Deux telles équations de Weierstrass pour* E *sont reliées par un changement de variables de la forme*

$$X = u^2X' + r$$
$$Y = u^3Y' + su^2X' + t,$$

   avec $u, r, s, t \in K$ *et* $u \neq 0$*.*

3. *Réciproquement, toute cubique lisse* C *donnée par une équation de Weierstrass comme en* 1. *est une courbe elliptique définie sur* K*, avec* $O = [0, 1, 0]$*.*

Démonstration. [Si86], III.3.1. L'ingrédient principal est le théorème de Riemann-Roch. □

On associe habituellement les quantités suivantes à l'équation de Weierstrass d'une courbe elliptique :

$$
\begin{aligned}
b_2 &= a1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= c_4^3/\Delta \\
\omega &= \frac{dx}{2y - a_1x - a_3}.
\end{aligned}
$$

Δ s'appelle le discriminant de la courbe elliptique, j est son j-invariant. ω est la forme différentielle de Néron associée à l'équation de Weierstrass.

Le discriminant permet de déterminer si une courbe est singulière ; j détermine sa classe d'isomorphisme :

Théorème 2.3. *1. Une courbe E donnée par son équation de Weierstrass peut être classifiée de la façon suivante :*

(a) Elle est non-singulière si et seulement si $\Delta \neq 0$.

(b) Elle est singulière si $\Delta = 0$. Dans ce cas, E a un unique point singulier. Si $c_4 \neq 0$, alors ce point admet une tangente unique (c'est un point de rebroussement). On dit que E a une node. *Si $c_4 = 0$, le point singulier admet deux tangentes distinctes, et on dit que E a une* cusp.

2. Deux courbes elliptiques sont isomorphes sur $\bar{K}$ si et seulement si elles ont le même j-invariant.

3. Soit $j_0 \in \bar{K}$. Alors il existe une courbe elliptique, définie sur $K(j_0)$, de j-invariant égal à j_0.

Démonstration. [Si86], III.1.4. □

Le grand intérêt porté aux courbes elliptiques est en partie dû au fait que l'ensemble des points de E à coordonnées dans K puisse être muni d'une loi de groupe ([Si86], III.2), le rôle du neutre étant joué par O. D'après le théorème de Mordell-Weil, ce groupe est finiment engendré. On pense en général qu'il n'y a pas de borne sur le rang du groupe de Mordell-Weil d'une courbe elliptique définie sur $\mathbb{Q}$. Nous verrons comment, grâce au théorème de Gross-Zagier, et à travers la conjecture de Birch et Swinnerton-Dyer, on peut relier ce rang aux points de Heegner.

2.1.1 Courbes elliptiques sur $\mathbb{C}$

On rappelle le théorème d'uniformisation de Weierstrass ([Si86],VI.5.1) :

Théorème 2.4. *Soit $E/\mathbb{C}$ une courbe elliptique. Alors il existe un réseau $\Lambda \in \mathbb{C}$, unique à homothétie près, et un isomorphisme analytique*

$$\Phi : \mathbb{C}/\Lambda \to E(\mathbb{C}), \quad \Phi(z) = [\wp(z,\Lambda), \wp'(z,\Lambda), 1],$$

où $\wp$ est la fonction de Weierstrass.

Soit Λ un réseau de $\mathbb{C}$. On note $g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$ et $g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$.

Les fonctions $\wp$ et $\wp'$ sont reliées par l'équation différentielle suivante ([Si86], VI.3.5) :

Proposition 2.5.

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

E est donc isomorphe sur $\mathbb{C}$ à la courbe elliptique $E(\Lambda)$ définie sur $\mathbb{C}$ par l'équation :

$$E(\Lambda) : Y^2 Z = 4X^3 - g_2(\Lambda) X Z^2 - g_3(\Lambda) Z^3.$$

Le discriminant de cette courbe est $\Delta(\Lambda) = g_2(\Lambda)^2 - 27 g_3(\Lambda)^3$, et son j-invariant est

$$j(\Lambda) = \frac{1728 g_2(\Lambda)^3}{g2(\Lambda)^3 - 27 g_3(\Lambda)^2}.$$

Pour $c \in \mathbb{C}^*$, $g_2(c\Lambda) = c^{-4} g_2(\Lambda)$ et $g_3(c\Lambda) = c^{-6} g_3(\Lambda)$. On peut ainsi définir, pour tout $\tau \in \mathcal{H} = \{z \in \mathbb{C}, Im(z) > 0\}$,

$$j(\tau) = j(\mathbb{Z} + \tau\mathbb{Z}).$$

Pour toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $j(\frac{a\tau + b}{c\tau + d}) = j(\tau)$, et j définit une fonction de $\mathcal{H}/SL_2(\mathbb{Z})$ dans $\mathbb{C}$.

Théorème 2.6. *$j : \mathcal{H}/SL_2(\mathbb{Z}) \to \mathbb{C}$ est un isomorphisme.*

Démonstration. [Si94], I théorème 4.1. □

En couplant ce théorème au théorème 2.3, on voit qu'il y a bijection entre les points de $\mathcal{H}/SL_2(\mathbb{Z})$ et les classes d'isomorphismes de courbes elliptiques définies sur $\mathbb{C}$.

2.1.2 Réduction

Soit K un corps local, muni d'une valuation v pour laquelle il est complet. On note R l'anneau des entiers de K, $\mathcal{M}$ l'idéal maximal de R, π une uniformisante pour R et $k = R/\mathcal{M}$ le corps des résidus de R.

Soit E une courbe elliptique définie sur K. On dit qu'une équation de Weierstrass est *minimale* par rapport à v si $v(\Delta)$ est minimal parmi toutes les équations de Weierstrass de E vérifiant $a_i \in R$.

Proposition 2.7. *Toute courbe elliptique E/K admet une équation de Weierstrass minimale. De plus, une telle équation est unique modulo un changement de coordonnées de la forme*

$$x = u^2 x' + r, \quad y = u^3 y' + u^2 s x + t,$$

avec $u \in R^*$ et $r, s, t \in R$.

Démonstration. [Si86],VII.1.3. □

On s'intéresse à la courbe $\tilde{E}$, définie sur k, dont une équation est donnée par la réduction modulo π d'une équation de Weierstrass minimale de E/K. La proposition précédente montre que cette équation est unique modulo un changement de variables standard *sur* k.

Définition 2.8. *On dira que :*

1. *E a* bonne réduction *sur K si $\tilde{E}$ est non-singulière.*

2. *E a* réduction multiplicative *sur K si $\tilde{E}$ a une* node. *On distingue alors deux sous-cas :*
   - *Si les tangentes au point singulier sont définies sur k, on dit que E a réduction* split multiplicative.
   - *Si les tangentes ne sont pas définies sur k, on dit que E a réduction* non-split multiplicative.
3. *E a réduction* additive *sur K si $\tilde{E}$ a une* cusp.

Les noms des différents types de réduction viennent du fait que, même si $\tilde{E}$ est singulière, l'ensemble de ses points non singuliers sur $\bar{k}$ forme encore un groupe $\tilde{E}_{ns}(\bar{k})$ tel que
- $\tilde{E}_{ns}(\bar{k}) \simeq \bar{k}^*$ si E a réduction multiplicative,
- $\tilde{E}_{ns}(\bar{k}) \simeq \bar{k}^+$ si E a réduction additive.

Définition 2.9. *Soit K un corps de nombre, et E/K une courbe elliptique. Soit v une place finie de K. Alors on dira que E a* bonne réduction, réduction additive, réduction multiplicative split ou non-split *suivant que E considérée comme courbe sur la complétion K_v de K en v a la même propriété.*

Il n'est pas possible en général de trouver une équation de Weierstrass pour E qui soit minimale pour toutes les valuations v, mais c'est vrai si $K = \mathbb{Q}$ ([Si86], VIII.8). Si une telle équation existe, on dira que c'est une équation de Weierstrass *globale minimale* pour E.

Le dernier invariant lié à une courbe elliptique que nous souhaitons définir est son *conducteur*. Celui-ci joue un rôle très important dans l'étude du comportement de la série L de E, que nous définirons dans la section suivante.

Définition 2.10. *Soit E une courbe elliptique définie sur $\mathbb{Q}$. Alors son conducteur N est caractérisé par les propriétés suivantes :*
- *$ord_p(N) = 0$ si et seulement si E a bonne réduction en p.*
- *$ord_p(N) = 1$ si et seulement si E a réduction multiplicative en p.*
- *Si $p > 3$, $ord_p(N) = 2$ dans tous les autres cas.*
- *Si $p = 2, 3$ et E a réduction additive en p, on peut calculer $ord_p(N)$ à l'aide d'un algorithme de Tate (ref).*

2.2 Séries L

Soit K un corps de nombres. Une série de Dirichlet sur K est une série de la forme

$$L(s) = \sum_{\mathfrak{n} \neq 0} a_{\mathfrak{n}} (N\mathfrak{n})^{-s},$$

où la somme se fait sur tous les idéaux (entiers) non nuls de K, et les $a_{\mathfrak{n}}$ sont des nombres complexes ; $N\mathfrak{n}$ désigne la norme de l'idéal $\mathfrak{n}$ sur $\mathbb{Q}$. Pourvu que les $a_{\mathfrak{n}}$ aient une croissance polynômiale, la série converge absolument pour $Re(s)$ assez grand.

Une telle série étant donnée, il peut être intéressant de considérer sa *tordue* par un *caractère* χ du groupe de classe de K :

$$L(\chi, s) = \sum_{\mathfrak{n} \neq 0} a_{\mathfrak{n}} \chi(\mathfrak{n}) (N\mathfrak{n})^{-s}.$$

Nous allons d'abord définir ce qu'est un caractère, puis nous donnerons deux séries de Dirichlet particulières : la série ζ de Dedekind et la série L d'une courbe elliptique.

2.2.1 Caractères

Dans la suite de cette section, G désigne un groupe abélien fini.

Définition 2.11. *Un* caractère *de G est un morphisme de G dans le groupe multiplicatif des nombres complexes de norme 1. On note $\hat{G}$ l'ensemble des caractères de G.*

Le produit de deux caractères est défini par :

$$\forall a \in A, \quad \chi_1\chi_2(a) = \chi_1(a)\chi_2(a).$$

Ceci fait de $\hat{A}$ un groupe abélien. Le neutre est appelé le *caractère principal*, il est constamment égal à 1.

On peut ainsi définir $\hat{\hat{A}}$. Ce groupe est canoniquement isomorphe à A par l'application qui à $a \in A$ fait correspondre le caractère $\chi \to \chi(a)$.

Les propriétés principales des caractères qui nous seront utiles sont les relations d'orthogonalité :

Proposition 2.12.

$$\forall \chi_1, \chi_2 \in \hat{A}, \ \sum_{a \in A} \chi_1(a)\chi_2(a) = \begin{cases} 0 & si\ \chi_1 \neq \chi_2^{-1} \\ \#A & si\ \chi_1 = \chi_2^{-1}. \end{cases} \tag{1}$$

$$\forall a_1, a_2 \in A, \ \sum_{\chi \in A} \chi(a_1)\chi(a_2) = \begin{cases} 0 & si\ a_1 \neq a_2^{-1} \\ \#A & si\ a_1 = a_2^{-1}. \end{cases} \tag{2}$$

Démonstration. Soit χ un caractère non principal de A et $b \in A$ tel que $\chi(b) \neq 1$. On a alors

$$\sum_{a \in A} \chi(a) \ = \ \sum_{a \in A} \chi(ab) \ = \ \chi(b) \sum_{a \in A} \chi(a).$$

Comme $\chi(b) \neq 1$, nécessairement $\sum_{a \in A} \chi(a) = 0$, d'où le (1) en prenant $\chi = \chi_1\chi_2$.

Pour le (2), on raisonne par dualité. □

2.2.2 Série ζ de Dedekind

Soit K un corps de nombres, et $\mathcal{O}_K$ l'anneau des entiers de K. La fonction ζ de Dedekind du corps K est la fonction définie par

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{(N\mathfrak{a})^s},$$

où la sommation se fait sur tous les idéaux non nuls de K.

Cette somme converge pour $Re(s)$ assez grand, et ζ_K se prolonge en une fonction méromorphe sur $\mathbb{C}$, avec un unique pôle en $s = 1$. La fonction de Dedekind de $\mathbb{Q}$ est simplement la fonction de Riemann.

ζ_K vérifie l'équation fonctionnelle

$$\zeta_K^*(s) = \zeta_K^*(1-s), \ \zeta_K^*(s) = \left(\frac{\sqrt{|d_K|}}{2^{r_2}\pi^{n/2}} \right)^s \Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s),$$

où d_K est le discriminant de K, $r1$ et $2r_2$ sont le nombre de plongements réels et complexes de K, et $n = r_1 + 2r_2$.

2.2.3 Série L d'une courbe elliptique

Soit E une courbe elliptique définie sur le corps de nombres K. Soit $v \in M_K$ une place finie de K. On note k_v la complétion de K en v, et $q_v = \#k_v$.

– Si E a bonne réduction en v, alors soit $N_v = \#\tilde{E}(k_v) = q_v + 1 - a_v$ (cf. 2.1.2). On pose

$$L_v(T) = 1 - a_v T + q_v T^2 \in \mathbb{Z}[T].$$

– Si E a réduction additive en v, on pose

$$L_v(T) = 1.$$

– Si E a réduction *split multiplicative* en v, alors on définit

$$L_v(T) = 1 - T.$$

– Finalement, si E a rédution *non-split multiplicative*, on pose

$$L_v(T) = 1 + T.$$

Définition 2.13. *La* série L *de E sur K est définie par le produit Eulerien*

$$L(E/K, s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1}.$$

La proposition suivante fait partie d'un ensemble de théorèmes concernant le nombre de points d'une variété sur un corps fini, apellés *conjectures de Weil* :

Proposition 2.14. *Avec les notations ci-dessus,*

$$1 - a_v T + q_v T^2 = (1 - \alpha T)(1 - \beta T),$$

où α et β sont des complexes conjugués de norme $\sqrt{q}$.

De plus, pour tout entier n, si $k_{v,n}$ désigne l'extension de degré n de k_v, alors

$$\#\tilde{E}(k_{v,n}) = 1 - \alpha^n - \beta^n + q^n.$$

Démonstration. [Si86], chapitre V, théorème 2.4. □

On en déduit en particulier le théorème de Hasse : $|a_v| < 2\sqrt{q_v}$), et donc la serie L de E/K converge pour $Re(s) > 3/2$.

Si $K = \mathbb{Q}$, on sait suite aux travaux de Taylor et de Wiles que la série L de $E/\mathbb{Q}$ satisfait une équation fonctionnelle, et se prolonge en une fonction entière sur $\mathbb{C}$. Ce résultat est conjectural dans le cas général.

Théorème 2.15. *$L(E/\mathbb{Q}, s)$ se prolonge en une fonction entière sur $\mathbb{C}$ et vérifie une équation fonctionnelle pour $s \to 2 - s$, de la forme*

$$L^*(E/\mathbb{Q}, s) = \pm L^*(E/\mathbb{Q}, 2 - s), \;\; L^*(E/\mathbb{Q}, s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(E, s),$$

où $\Gamma(s)$ est la fonction d'Euler.

Une des plus célèbres conjectures de la théorie des courbes elliptiques relie l'ordre de la série L d'une courbe elliptique $E/\mathbb{Q}$ en 1 au rang du groupe de Mordell-Weill $E(\mathbb{Q})$.

Conjecture 2.16. *(Birch et Swinnerton-Dyer). Soit E une courbe elliptique définie sur $\mathbb{Q}$. Alors, le rang r de $E(\mathbb{Q})$ est égal à l'ordre de $L(E,s)$ en 0. Plus précisement, soient*

- *R_E le régulateur de E, $R_E = det(< P_i, P_j >_{\mathbb{Q}})_{1\leq i,j\leq r}$, où $(P_1,\ldots,P_r)$ est un ensemble de générateurs indépendants de $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$, et $< \cdot,\cdot >_{\mathbb{Q}}$ est la forme bilinéaire de Néron-Tate définie en 2.3.*
- *c_p les nombres de Tamagawa, définis dans [Si86], VIII.9. Ce sont des entiers qui ne dépendent que du comportement de E sur $\mathbb{Q}_p$.*
- *$\#III(E/\mathbb{Q})$ le cardinal du groupe de Tate-Shafarevitch de E, defini dans [Si86], X.4. S'il est fini, alors c'est le carré d'un entier.*
- *$\Omega = \int_{E(\mathbb{R})} \omega$ est la période réelle.*

Alors

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \prod_{p|N} c_p \frac{\Omega R_E}{\#E(\mathbb{Q})^2_{tors}} \#III(E/\mathbb{Q}).$$

Un cas particulier de cette conjecture a été prouvé par Gross et Zagier, et découle de leur théorème que nous présenterons dans la section 3.3.

Théorème 2.17. *(Gross-Zagier). Soit E une courbe elliptique définie sur $\mathbb{Q}$.*

1. *Si $L(E,1) \neq 0$, alors $\#E(\mathbb{Q}) < \infty$, c'est-à-dire $r = 0$.*
2. *Si $L(E,1) = 0$ et $L'(E,1) \neq 0$, alors $r = 1$.*

Nous terminons cette section en donnant la définition de la série L du carré symétrique d'une courbe elliptique. Cette série apparaîtra dans la section 5.2

Définition 2.18. *Soit E/K une courbe elliptique. Soit v une place finie de K. Si E a mauvaise réduction en v, on pose $L_v(sym^2E,T) = L_v(T)$. Si E a bonne réduction en v, soient α_v et β_v tels que $L_v(T) = (1-\alpha_v T)(1-\beta_v T)$, et*

$$L_v(sym^2E,T) = (1-\alpha_v^2 T)(1-\alpha_v\beta_v T)(1-\beta_v^2 T).$$

La série L du carré symétrique de E est definie par :

$$L(sym^2E,s) = \prod_{v\in M_K^0} L(sym^2E, q_v^{-s})^{-1}.$$

Cette série L vérifie une équation fonctionnelle reliant s et $3-s$. La valeur de la série en son centre de symétrie est proportionnelle au degré de la paramétrisation modulaire de E (2.4.3) :

Proposition 2.19. *On suppose que le conducteur N de E est sans facteurs carrés. Soit c la constante de Manin de E (cf 2.4.3) et $\Omega = Im(\omega_1\bar{\omega}_2)$ le volume complexe. Alors :*

$$\frac{L(sym^2E,2)}{\pi\Omega} = \frac{deg(\Phi_N)}{Nc^2}.$$

Démonstration. [Wa], $(1-1)$. □

2.3 Hauteurs

Nous allons définir une hauteur sur l'espace projectif en général, puis nous donnerons la définition de la hauteur de Néron-Tate sur les points d'une courbe elliptique. Pour plus de détails, on renvoie à [Si86], VIII.5, 6, 9.

Soit K un corps de nombres, et M_K l'ensemble des valeurs absolues de K. Chaque $v \in M_K$ prolonge une des valeurs absolues de $\mathbb{Q}$, qui sont la valeur absolue usuelle et les valeurs absolues p-adiques.

Pour $v \in M_K$, soient K_v et $\mathbb{Q}_v$ les complétions desdits corps par rapport à v. On note $n_v = [K_v : \mathbb{Q}_v]$ le degré local en v.

Définition 2.20. *Soit $P \in \mathbb{P}^N(K)$ ayant les coordonnées homogènes*

$$P = [x_0, \ldots, x_N], \ x_i \in K.$$

La hauteur (logarithmique) de P (par rapport à K) est définie par

$$h_K(P) = \log\left(\prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}\right).$$

Proposition 2.21. *Soit $P \in \mathbb{P}^N(K)$.*

1. *La hauteur $h_K(P)$ ne dépend pas du choix de coordonnées homogènes pour P.*
2. *$h_K(P) \geq 0$.*
3. *Si L est une extension finie de K, alors*

$$h_L(P) = [L : K]h_K(P).$$

Démonstration. [Si86], Chap. VIII, prop 5.4. □

Le troisième point de cette proposition permet de définir une *hauteur absolue* ne dépendant pas du corps K :

Définition 2.22. *Soit $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$, et K une extension finie de $\mathbb{Q}$ telle que $P \in \mathbb{P}^N(K)$. La hauteur absolue de P, notée $h(P)$, est définie par :*

$$h(P) = \frac{h_K(P)}{[K : \mathbb{Q}]}.$$

Nous donnons maintenant trois propriétés de la hauteur ainsi définie qui nous serviront en 5.1.

Proposition 2.23. *Soit $F : \mathbb{P}^N \to \mathbb{P}^M$ un morphisme de degré d. Alos il existe des constantes C_1 et C_2, dépendant de F, telles que pour tout $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$,*

$$C_1 + dh(P) \leq h(F(P)) \leq C_2 + dh(P).$$

Démonstration. [Si86], Chap. VIII, théorème 5.6. □

Proposition 2.24. *Soit*

$$f(X) = a_0X^d + a_1X^{d-1} + \ldots + a_d = a_0\prod_{i=1}^{d}(X - \alpha_i) \in \overline{\mathbb{Q}}[X]$$

un polynome de degré d. Alors

$$-2d + \sum_{j=1}^{d} h(\alpha_j) \leq h([a_0, \ldots, a_d]) \leq 2(d-1) + \sum_{j=1}^{d} h(\alpha_j).$$

Démonstration. [Si86], Chap. VIII, proposition 5.9. □

Proposition 2.25. *Soit $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ et $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Alors*

$$h(P^\sigma) = h(P).$$

Démonstration. Soit $K/\mathbb{Q}$ un corps tel que $P \in \mathbb{P}^N(K)$. Par définition, σ donne un isomorphisme $K \to K^\sigma$, et il identifie de même les ensembles de valeurs absolues : pour $x \in K$ et $v \in M_K$, $|x^\sigma|_{v^\sigma} = |x|_v$. σ induit également un isomorphisme $K_v \to K^\sigma_{v^\sigma}$, donc $n_v = n_{v^\sigma}$. D'où :

$$\begin{aligned} h_{K^\sigma}(P^\sigma) &= \prod_{w \in M_{K^\sigma}} \max\{|x_i^\sigma|_w\}^{n_w} \\ &= \prod_{w \in M_K} \max\{|x_i^\sigma|_{v^\sigma}\}^{n_{v^\sigma}} \\ &= \prod_{w \in M_K} \max\{|x_i^\sigma|_v\}^{n_v} \\ &= h_K(P). \end{aligned}$$

Comme $[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$, on obtient le résultat voulu. □

Corollaire 2.26. *Soit $x \in K$ un entier algébrique. Soit $f(X) = a_0X^d + a_1X^{d-1} + \ldots + a_d$ le polynôme minimal de x sur $\mathbb{Q}$. On peut identifier $K \cup \{\infty\}$ avec $\mathbb{P}^1(K)$, et on a alors :*

$$h([a_0, \ldots, a_d]) \sim d \cdot h(x) \text{ lorsque } d \text{ tend vers l'infini.}$$

Nous pouvons à présent définir une hauteur sur les points d'une courbe elliptique en les plongeant dans $\mathbb{P}^N(K)$:

Définition 2.27. *Soit E une courbe elliptique définie sur K et $f \in \bar{K}(E)$. La hauteur sur E (relative à f) est la fonction :*

$$\begin{aligned} h_f : E(\bar{K}) &\to \mathbb{R} \\ P &\to h(f(P)). \end{aligned}$$

Proposition 2.28. *Soit E une courbe elliptique définie sur K et $f \in K(E)$ une fonction paire. Alors pour tous $P, Q \in E(\bar{K})$,*

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + O(1).$$

Le $O(1)$ dépend uniquement de la courbe E et de f.

Démonstration. [Si86], Chap. VIII, prop 6.2. □

Cette proposition montre que la hauteur h_f est "presque" une forme quadratique. André Néron a demandé s'il était possible de trouver une forme quadratique qui ne diffère de h_f que par une quantité bornée (dépendant de f). Il a construit une telle forme quadratique à partir de fonctions locales. À la même époque, Tate a donné une définition globale plus simple, qui s'est ensuite avérée être la même. La construction de Tate est la suivante :

Proposition 2.29. *Soit E une courbe elliptique définie sur K, $f \in K(E)$ une fonction paire non constante, et $P \in E(\bar{K})$. Alors la limite*

$$\frac{1}{deg(f)} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

existe, et est indépendante de f ($[m]$ désigne la multiplication par m sur E).

Démonstration. [Si86], Chap. VIII, prop 9.1. □

Définition 2.30. *La hauteur de Néron-Tate sur E/K, notée $\hat{h}_K$, est la fonction*

$$\hat{h}_K : E(\bar{K}) \to \mathbb{R}$$

définie par

$$\hat{h}_K(P) = \frac{1}{deg(f)} \lim_{N\to\infty} 4^{-N} h_f([2^N]P),$$

où $f \in \bar{K}(E)$ est une fonction paire non-constante quelconque.

Théorème 2.31. *(Néron-Tate). Soit E une courbe elliptique définie sur K, et $\hat{h}_K$ la hauteur de Néron-Tate sur E.*

1. *Pour tous $P, Q \in E(\bar{K})$,*
$$\hat{h}_K(P+Q) + \hat{h}_K(P-Q) = 2\hat{h}_K(P) + 2\hat{h}_K(Q).$$
2. *Pour tous $P \in E(\bar{K})$ et $m \in \mathbb{Z}$,*
$$\hat{h}_K([m]P) = m^2\hat{h}_K(P).$$
3. *$\hat{h}_K$ est une forme quadratique sur E : $\hat{h}_K$ est paire, et la forme*
$$<,>_K : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R} \tag{3}$$
$$P, Q \to \hat{h}_K(P+Q) - 2\hat{h}_K(P) - 2\hat{h}_K(Q) \tag{4}$$
est bilinéaire.
4. *Soit $P \in E(\bar{K})$. Alors $\hat{h}_K(P) \geq 0$, et $\hat{h}_K(P) = 0$ si et seulement si P est un point de torsion.*

Démonstration. [Si86], Chap. VIII, prop 9.3. □

Proposition 2.32. *La hauteur de Néron-Tate est une forme quadratique défini-positive sur l'espace vectoriel $\mathbb{R} \otimes E(K)$.*

Démonstration. [Si86], Chap. VIII, prop 9.6. □

2.4 Courbes modulaires

Les séries L de courbes elliptiques sont difficiles à analyser. L'approche qui a eu le plus de succès consiste à utiliser la *modularité* de la courbe elliptique, qui permet d'étudier la série L à travers la théorie plus générale des *formes modulaires*. Nous allons présenter certains aspects de cette théorie.

2.4.1 Formes modulaires

On se contente ici de rappeler quelques définitions concernant les formes modulaires. Pour une introduction plus complète, on pourra se reporter à [Se]. Le groupe $GL_2(\mathbb{R})$ agit sur le demi-plan de Poincaré $\mathcal{H}$ de la manière suivante :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

On appelle *groupe modulaire* tout sous-groupe de $SL_2(\mathbb{Z})$ d'indice fini. Soit Γ un groupe modulaire.

Définition 2.33. *Une* fonction modulaire *de poids k pour Γ est une fonction méromorphe $f : \mathcal{H} \to \mathbb{C}$ telle que*

1. $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ *pour tout* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.
2. *Pour tout $\gamma \in SL_2(\mathbb{Z})$, la fonction*

$$f_{|\gamma}(\tau) = (c\tau + d)^{-k} f(\gamma\tau)$$

admet un développement de la forme

$$\sum_{n=n_0^\gamma}^{\infty} a_n^\gamma q^{n/h}, \ \text{où } q = e^{2i\pi\tau},$$

$n_0^\gamma \in \mathbb{Z}$ *et h est un entier positif.*

Une forme modulaire *est une fonction modulaire holomorphe partout (i.e., f est holomorphe et $n_0^\gamma = 0$ pour tout γ)*

Une forme modulaire f pour Γ est appelée une *forme parabolique* si $a_0^\gamma = 0$ pour tout $\gamma \in \Gamma$. On note $S_k(\Gamma)$ l'espace vectoriel complexe des formes paraboliques de poids k pour Γ. Il est de dimension finie.

Le cas qui nous intéresse le plus est celui où $k = 2$ et

$$\Gamma = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ N|c \right\}$$

est le *sous-groupe de congruence principal de niveau N*, pour N un entier positif. On note alors $S_2(N) = S_2(\Gamma_0(N))$ l'espace des formes paraboliques de poids 2 sur $\Gamma_0(N)$.

À chaque $f \in S_2(N)$, on peut associer la forme différentielle $w_f = 2i\pi f(\tau)d\tau$ sur $X_0(N)$ (définie dans la section suivante), du fait de l'holomorphie de f et de son invariance par $\Gamma_0(N)$. Les conditions d'invariance a priori artificielles de la définition se traduisent ainsi en une identification naturelle de $S_2(N)$ avec l'espace des formes différentielles holomorphes sur $X_0(N)$.

$S_2(N)$ est muni du produit scalaire hermitien de Petersson

$$< f_1, f_2 >= \int_{\mathcal{H}/\Gamma_0(N)} f_1(\tau) f_2(\bar{\tau}) dx dy,$$

Il est également muni de l'action des *opérateurs de Hecke T_p*, définis par

$$T_p(f) = \begin{cases} \frac{1}{p} \sum_{i=0}^{p-1} f(\frac{\tau + i}{p}) + p f(p\tau) & \text{si } p \nmid N \\ \frac{1}{p} \sum_{i=0}^{p-1} f(\frac{\tau + i}{p}) & \text{si } p|N \end{cases}$$

pour p premier. On étend cette définition à tous les entiers n en identifiant formellement les coefficients des séries de Dirichlet

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p|N} (1 - T_p p^{-s})^{-1} \prod_{p \nmid N} (1 - T_p p^{-s} + p^{1-2s})^{-1}.$$

On note $\mathbb{T}$ la sous-algèbre commutative de $\mathrm{End}_{\mathbb{C}}(S_2(N))$ engendrée par les T_n sur $\mathbb{Z}$. L'algèbre $\mathbb{T}$ est finiment engendrée de rang $g = dim_{\mathbb{C}}(S_2(N))$ ([Da1], Proposition 2.4).

Soit $\lambda : \mathbb{T} \to \mathbb{C}$ un morphisme d'anneaux, et S_λ le sous-espace propre de $S_2(N)$ correspondant. Alors S_λ est unidimentionnel ([Da1], lemme 2.7). Il n'est pas vrai que $S_2(N)$ soit somme directe de ces sous-espaces propres ; mais c'est cependant le cas pour un certain sous-espace de $S_2(N)$, appelé espace des *newforms*.

Définition 2.34. *Soit $f \in S_2(N)$. On dira que f est une* oldform *si elle est combinaison linéaire de formes $g(d'z)$ avec $g \in S_2(N/d)$ et $d'|d > 1$. Le sous-espace des* newform *est le complémentaire orthogonal de l'espace des oldform dans $S_2(N)$ pour le produit scalaire de Petersson. On note respectivement $S_2^{new}(N)$ et $S_2^{old}(N)$ l'espace des newform et celui des oldform.*

Théorème 2.35. *(Atkin-Lehner). $S_2(N)$ se décompose en somme de sous-espaces orthogonaux*

$$S_2(N) = S_2^{old}(N) \oplus_\lambda \mathbb{C} f_\lambda,$$

où la somme se fait sur tous les morphismes d'algèbre $\lambda : \mathbb{T} \to \mathbb{C}$ correspondant à des vecteurs propres dans $S_2^{new}(N)$, et $f_\lambda(\tau) = \sum_{n=1}^{\infty} \lambda(T_n) e^{2i\pi n\tau}$.

2.4.2 $X_0(N)$

Soit N un entier non nul.

Définition 2.36. *La courbe modulaire $Y_0(N)$ classifie l'ensemble des paires (E, E') de courbes elliptiques reliées par une isogénie cyclique de degré N, c'est-à-dire un morphisme de courbes algébriques $\phi : E \to E'$ tel que $\phi(O) = O'$ et $\ker \phi = \mathbb{Z}/N\mathbb{Z}$.*

On peut donner une autre définition de $Y_0(N)$ en termes de surfaces de Riemann, qui sera plus utile d'un point de vue calculatoire :

Proposition 2.37. *$Y_0(N)$ est isomorphe au quotient $\mathcal{H}/\mathit{\Gamma}_0(N)$, qui peut être muni d'une structure de surface de Riemann.*

Démonstration. $\mathcal{H}/\mathit{\Gamma}_0(N)$ est une surface de Riemann en tant que quotient. Mais attention, cette surface n'est pas compacte.

Soit $(E, E') \in Y_0(N)$. Le théorème d'uniformisation complexe de Weierstrass permet d'écrire $E = \mathbb{C}/M, E' = \mathbb{C}/M'$, où M et M' sont des réseaux de $\mathbb{C}$. Quitte à modifier M par une homothétie, on peut de plus supposer que $M \subset M'$, et que l'isogénie ϕ est obtenue à partir de l'identité : $\mathbb{C} \to \mathbb{C}$ par passage au quotient. Comme $\ker \phi = M'/M \simeq \mathbb{Z}/N\mathbb{Z}$, il existe une base $< \omega_1, \omega_2 >$ de M telle que $M' =< \omega_1, \omega_2/N >$ et $\tau = \omega_2/\omega_1 \in \mathcal{H}$. La $\Gamma_0(N)$-orbite du point τ est bien définie par le point (E, E') car, si l'on considère une autre base $< \omega_1', \omega_2' >$ satisfaisant aux conditions ci-dessus, alors il existe $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ telle que $\omega_1' = a\omega_1 + b\omega_2,\ \omega_2' = c\omega_1 + d\omega_2$. De même, on peut trouver une matrice $Q = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$ telle que $\omega_1' = a'\omega_1 + b'\omega_2/N,\ \omega_2'/N = c'\omega_1 + d'\omega_2/N$, d'où $c = Nc'$, donc $P \in \Gamma_0(N)$. La construction ci-dessus est donc bien définie, et injective. Pour voir qu'elle est surjective, à chaque orbite $\tau \in \mathcal{H}/\mathit{\Gamma}_0(N)$ on peut associer les réseaux $M =< 1, \tau >$ et $M' =< 1, \tau/N >$. Les courbes elliptiques ainsi définies sont alors reliées par l'isogénie évidente. □

On note $X_0(N)$ la compactification naturelle de $Y_0(N)$ obtenue en adjoignant à $\mathcal{H}$ l'ensemble $\mathbb{P}_1(\mathbb{Q}) \cup \{\infty\}$. Les classes des points ainsi ajoutés dans $\mathcal{H} \cup \mathbb{P}_1(\mathbb{Q}) \cup \{\infty\}/\mathit{\Gamma}_0(N)$ sont appelées les *cusps*.

Notre troisième decription de $X_0(N)$ sera celle d'une courbe algébrique définie sur $\mathbb{Q}$. Ce modèle nous sera utile pour démontrer certaines propriétés des points de Heegner. Même si toute surface de Riemann compacte peut etre identifiée avec l'ensemble des points complexes d'une courbe projective plane non-singulière, il n'est en général pas vrai que cette courbe puisse être définie sur $\mathbb{Q}$; il suffit de considérer une surface dont l'invariant j est transcendant. Le cas de $X_0(N)$ est donc très particulier.

Théorème 2.38. *Le corps des fonctions méromorphes sur $X_0(1)$ est $\mathbb{C}(j)$.*

Démonstration. [Si94], I corollaire 4.2. □

Nous allons utiliser ce théorème pour trouver toutes les fonctions méromorphes sur $X_0(N)$. Soit j_N la fonction definie sur $\mathcal{H}$ par $j_N(z) = j(Nz)$. Alors j_N est $\Gamma_0(N)$-invariante :
Pour tous $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ et $z \in \mathbb{C}$,

$$j_N(\gamma z) = j\left(\frac{Naz + Nb}{cz + d}\right) = j\left(\frac{a(Nz) + Nb}{c'(Nz) + d}\right) = j(\gamma' Nz),$$

où $c' \in \mathbb{Z}$ est tel que $c = Nc'$, et $\gamma' = \begin{pmatrix} a & Nb \\ c' & d \end{pmatrix} \in \Gamma_0(1)$, donc

$$j(N\gamma' z) = j(Nz) = j_N(z).$$

j et j_N définissent ainsi des fonctions méromorphes sur $X_0(N)$.

Proposition 2.39. *Le corps des fonctions méromorphes sur $X_0(N)$ est $\mathbb{C}(j, j_N)$.*

Démonstration. Soient $\{\gamma_1, \ldots, \gamma_m\}$ un ensemble de représentants des classes de résidus de $SL_2(\mathbb{Z})$ pour l'action à gauche de $\Gamma_0(N)$, de sorte que :

$$SL_2(\mathbb{Z}) = \bigcup_{i=1}^{m} \Gamma_0(N)\gamma_i.$$

Soit $f(z)$ une fonction modulaire pour $\Gamma_0(N)$, alors $f(\gamma_i z)$ ne dépend que de la classe $\Gamma_0(N)\gamma_i$. Pour $\gamma \in SL_2(\mathbb{Z})$, l'ensemble $\{f(\gamma_i \gamma z)\}$ est donc une permutation de $\{f(\gamma_i z)\}$, et n'importe quel polynôme symétrique en les $f(\gamma_i z)$ est invariant par $SL_2(\mathbb{Z})$. Un tel polynôme est donc une fonction modulaire pour $SL_2(\mathbb{Z})$ (les autres conditions étant évidentes), et ainsi une fonction rationnelle de j d'après le théorème 2.38. $f(z)$ est racine du polynôme $\prod(Y - f(\gamma_i z))$ de degré m et à coefficients dans $\mathbb{C}(j)$. Comme ceci est vérifié pour toute fonction méromorphe sur $X_0(N)$, on a montré que le corps de ces fonctions était de degré au plus m sur $\mathbb{C}(j)$.

Les $f(\gamma_i(z))$ sont conjugués à $f(z)$ sur $\mathbb{C}(j)$: soit $F(j, Y)$ le polynôme minimal de f sur $\mathbb{C}(j)$. En remplaçant z par $\gamma_i z$, comme $j(\gamma_i z) = j(z)$, on obtient $F(j(z), f(\gamma_i z)) = 0$.

Il suffit maintenant de montrer que j_N est de degré exactement m sur $\mathbb{C}(j)$, c'est-à-dire que les $j(N\gamma_i z)$ sont deux à deux distincts.

Soient $i \neq j$, $j(N\gamma_i z) = j(N\gamma_j z)$. Comme j définit un isomorphisme : $\mathcal{H}/\mathit{\Gamma}_0(N) \to \mathbb{C}$, on a :

$$\forall z, j(N\gamma_i z) = j(N\gamma_j z) \implies \exists \gamma \in SL_2(\mathbb{Z}), \forall z, N\gamma_i z = \gamma N\gamma_j z,$$

d'où

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_i = \pm\gamma \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_j.$$

Donc $\gamma_i \gamma_j^{-1} \in SL_2(\mathbb{Z}) \cap \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} SL_2(\mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \Gamma_0(N)$, ce qui contredit le fait que γ_i et γ_j soient dans des classes différentes.

Le polynôme minimal de j_N sur $\mathbb{C}(j)$ est donc de degré exactement m, et le corps des fonctions méromorphes de $X_0(N)$ est engendré par j_N sur $\mathbb{C}(j)$. □

Dans la preuve ci-dessus, nous avons montré que le polynôme minimal de j_N sur $\mathbb{C}(j)$ était

$$F_N(j,Y) = \prod_{i=1}^{m} (Y - j(N\gamma_i z)).$$

Les polynômes symétriques en les $j(N\gamma_i z)$ sont holomorphes sur $\mathcal{H}$, et sont donc des polynômes en j (plutôt que des fractions rationnelles en j, comme on l'a vu dans la preuve), donc $F_N(j,Y) \in \mathbb{C}[j,Y]$. En remplaçant j par X, on obtient un polynôme $F_N(X,Y) \in \mathbb{C}[X,Y]$.

Proposition 2.40. *Le polynôme F_N est à coefficients dans $\mathbb{Q}$.*

Démonstration. La fonction j admet un développement en puissances de $q = e^{2i\pi z}$ à coefficients entiers ([Se], VII) :

$$j(z) = q^{-1} + \sum_{n=0}^{\infty} c(n)q^n, \ c(n) \in \mathbb{Z}.$$

Quand on effectue la substitution dans l'équation $F(j(z), j(Nz)) = 0$, on obtient un système d'équations linéaires en les coefficients de F_N, à coefficients dans $\mathbb{Q}$.

Or, comme $F_N(j,Y)$ est le polynôme minimal de j_N sur $C(j)$, il est clair que F_N engendre l'idéal des polynômes de $C[X,Y]$ s'annulant en (j, j_N). Ainsi, si on impose que le coefficient dominant de $F_N(j,Y)$ soit 1, le système ci-dessus a une unique solution sur $\mathbb{C}$. La matrice définissant ce système a donc une sous-matrice inversible de taille $(m+1)^2$. Cette matrice est inversible sur $\mathbb{C}$ à coefficients dans $\mathbb{Q}$, elle est donc inversible dans $\mathbb{Q}$, et le système a une solution rationnelle. □

Soit C_N la courbe affine définie sur $\mathbb{Q}$ par le polynôme F_N, et $\bar{C}_N$ la courbe projective obtenue en rendant F_N homogène. Comme $j : \mathcal{H}/SL_2(\mathbb{Z}) \to \mathbb{C}$ et $j_N : \mathcal{H}/\Gamma_0(N) \to \mathbb{C}$ sont des isomorphismes, l'application

$$Y_0(N) \to C_N(\mathbb{C}) \tag{5}$$
$$z \to (j(z), j_N(z)) \tag{6}$$

se prolonge en une application $X_0(N) \to \bar{C}_N(\mathbb{C})$ qui est un isomorphisme, excepté en les points singuliers de $\bar{C}_N$.

2.4.3 La paramétrisation modulaire

Soit N un entier fixé pour toute cette section. À une newform f pour l'espace $S_2(N)$ (on dit que f est de *niveau* N) on peut associer la série L

$$L(f,s) = \sum_{n=1}^{\infty} \lambda(T_n) n^{-s}.$$

Le théorème 2.35 montre en effet que toute newform est le vecteur propre pour l'action de $\mathbb{T}$ sur $S_2(N)$ correspondant aux valeurs propres encodées dans le morphisme d'alèbres $\lambda : \mathbb{T} \to \mathbb{C}$.

Cette série L possède des propriétés analogues à celles qu'a la série L d'une courbe elliptique (produit Eulerien, équation fonctionnelle). Ce n'est pas un hasard, puisque Eichler et Shimura ont montré le

Théorème 2.41. *Soit f un vecteur propre pour l'action de $\mathbb{T}$ sur $S_2(N)$ dont les coefficients de Fourier $a_n(f)$ sont des entiers, et $a_1(f) = 1$. Alors il existe une courbe elliptique E_f définie sur $\mathbb{Q}$ telle que*

$$L(E_f, s) = L(f, s).$$

$X_0(N)$ peut être plongée dans sa jacobienne $J_0(N)$ en envoyant un point P sur la classe du diviseur de degré 0 $(P)-(i\infty)$. La construction d'Eichler et Shimura consiste à obtenir E_f comme quotient de $J_0(N)$.

Soit

$$\Phi_N : X_0(N) \to E_f$$

le morphisme obtenu en composant ces deux applications.

Par la suite, Wiles a montré que l'on pouvait effectuer l'opération inverse : à toute courbe elliptique E on peut associer une newform telle que E soit isogène à E_f, et donc E et E_f ont même série L.

On considère à présent une courbe elliptique $E/\mathbb{Q}$ de conducteur N, on note f la newform qui lui est associée, et $L(E,s) = L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Si ω est la forme différentielle de Néron associée à une équation de Weierstrass globale minimale de $E/\mathbb{Q}$, alors le *pullback* de ω par Φ_N est un multiple non-nul de la forme $\omega_f = 2i\pi f(\tau)d\tau$:

$$\Phi_N^*(\omega) = c \cdot 2i\pi f(\tau)d\tau,\ c \in \mathbb{Q}^*.$$

c est appellée la *constante de Manin* attachée a f. On pense que c vaut toujours 1 ; et on le sait lorsque N est sans facteur carré. Pour les calculs de la section 4, la description analytique suivante de $\Phi_N : \mathcal{H}/\Gamma_0(N) \to E(\mathbb{C})$ nous sera utile :

Proposition 2.42. *Soit Λ le réseau de $\mathbb{C}$ isomorphe à l'équation de Weierstrass globale minimale de E par la paramétrisation de Weierstrass. On note $\Phi_\omega = (\mathcal{P}_\Lambda, \mathcal{P}'_\Lambda)$ l'uniformisation de Weierstrass. Alors*

$$\Phi_N(\tau) = \Phi_\omega(z_\tau),\ \textit{où}\ z_\tau = c\int_{i\infty}^{\tau} 2\pi i f(z)dz = c\sum_{n=1}^{\infty} \frac{a_n}{n} e^{2i\pi\tau n}.$$

Démonstration. [Da1], proposition 2.10. □

Comme $X_0(N)$ et $E = \mathbb{C}/\Lambda$ peuvent être réalisées comme des surfaces de Riemann, on peut associer à Φ_N un degré topologique. Ce degré est aussi le degré de Φ_N en tant que morphisme de courbes algébriques, c'est-à-dire l'index du *pull-back* du corps de fonctions de E dans celui de $X_0(N)$. La proposition 2.19 montre comment calculer ce degré rapidement, en fonction de la série L du carré symétrique de la courbe elliptique.

2.5 Multiplication complexe

2.5.1 Théorie du corps de classe

Nous rappelons ici les constructions de base de la théorie du corps de classe, sans aborder la formulation moderne en termes d'Adèles. Pour plus de détails, je renvoie à [CF] ou [Ja].

Dans toute la suite, K désignera un corps de nombres et L une extension abélienne finie de K. On désignera par $\mathcal{O}_K$ et $\mathcal{O}_L$ les anneaux d'entiers de K et de L, et on note $G = Gal(L/K)$ le groupe de Galois de l'extension.

Soit $\mathfrak{p}$ un premier de K qui ne ramifie pas dans L, et $\mathfrak{P}$ un premier de L au-dessus de $\mathfrak{p}$. On note $K_\mathfrak{p} = K/\mathfrak{p}$, de même $L_\mathfrak{P} = L/\mathfrak{P}$. Le *groupe de décomposition* de $\mathfrak{P}$ est le sous-groupe $G_\mathfrak{P} = \{\sigma \in G, \sigma\mathfrak{P} = \mathfrak{P}\}$ de G.

Lemme 2.43. *L'extension $L_\mathfrak{P}/K_\mathfrak{p}$ est Galoisienne et son groupe de Galois est isomorphe à $G_\mathfrak{P}$.*

Démonstration. [CF], Chapitre VII, proposition 1.2. □

Comme $L_{\mathfrak{P}}$ et $K_{\mathfrak{p}}$ sont des corps finis, le groupe de Galois de $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est cyclique engendré par le Frobenius

$$F : x \to x^{N\mathfrak{p}},$$

où $N\mathfrak{p} = \#(K/\mathfrak{p})$ est la norme numérique. D'après le lemme 2.43, il existe un unique élément $\sigma_{\mathfrak{P}}$ de $G_{\mathfrak{P}}$ tel que

$$x^{\sigma_{\mathfrak{P}}} \equiv x^{N\mathfrak{p}} \mod \mathfrak{P},$$

pour tout $x \in L$. $\sigma_{\mathfrak{P}}$ est appelé l'*automorphisme de Frobenius* associé au premier $\mathfrak{P}$.

En général, $\mathfrak{p}$ détermine seulement la classe de conjugaison de $\sigma_{\mathfrak{P}}$, et un autre choix de $\mathfrak{P}$ change $\sigma_{\mathfrak{P}}$ par conjugaison. Mais nous avons supposé que L/K était abélienne, et donc $\sigma_{\mathfrak{P}}$ est uniquement déterminé par $\mathfrak{p}$; on le note alors $\sigma_{\mathfrak{p}}$.

Soit $\mathfrak{c}$ un idéal entier de K qui est divisible par tous les premiers qui ramifient dans L/K, et soit $I(\mathfrak{c})$ le groupe des idéaux fractionnaires de K qui sont premiers à $\mathfrak{c}$. Alors *l'application d'Artin* est définie par :

$$(\cdot, L/K) : I(\mathfrak{c}) \to Gal(L/K)$$
$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \to \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

Proposition 2.44. *(Réciprocité d'Artin). Soit L/K une extension finie de corps de nombres. Il existe un idéal entier $\mathfrak{c} \subset \mathcal{O}_K$, exactement divisible par tous les premiers de K qui ramifient dans L, tel que*

$$((\alpha), L/K) = 1 \text{ pour tout } \alpha \in K^* \text{ tel que } \alpha \equiv 1 \mod \mathfrak{c}.$$

Si la propriété est verifiée par les idéaux $\mathfrak{c}_1$ et $\mathfrak{c}_2$, alors elle est vérifiée par $\mathfrak{c}_1 + \mathfrak{c}_2$, et il existe donc un plus grand idéal pour lequel est vraie. On appelle cet idéal le *conducteur* de L/K, et on le note $\mathfrak{c}_{L/K}$.

Soit $P_1(\mathfrak{c}) = \{(\alpha), \alpha \in K^\star, \alpha \equiv 1 \mod \mathfrak{c}\}$. Alors la proposition ci-dessus dit que le noyau de l'application d'Artin contient $P_1(\mathfrak{c})$ pour un bon choix de $\mathfrak{c}$.

Définition 2.45. *Soit $\mathfrak{c}$ un idéal entier de K. Un* ray class field *de K (modulo $\mathfrak{c}$) est une extension abélienne finie $K_{\mathfrak{c}}/K$ telle que pour toute extension abélienne finie L/K,*

$$\mathfrak{c}_{L/K} | \mathfrak{c} \implies L \subset K_{\mathfrak{c}}.$$

Nous pouvons maintenant donner le théorème fondamental de la théorie du corps de classe :

Théorème 2.46. *Soit L/K une extension finie de corps de nombres, et $\mathfrak{c}$ un idéal entier de K.*

1. *L'application d'Artin*
$$(\cdot, L/K) : I(\mathfrak{c}_{L/K}) \to Gal(L/K)$$
est un morphisme surjectif.
2. *Son noyau est $(N_K^L I_L) P_1(\mathfrak{c}_{L/K})$, où I_L est le groupe des idéaux fractionnaires non nuls de L.*
3. *Il existe un unique* ray class field *$K_{\mathfrak{c}}$ de K modulo $\mathfrak{c}$. Le conducteur de $K_{\mathfrak{c}}/K$ divise $\mathfrak{c}$.*
4. *(Théorème d'existence). Pour tout groupe $P_1(\mathfrak{c}) \subset H \subset I(\mathfrak{c})$, il existe une unique extension abélienne L de K (dans une clôture algébrique fixée de K) telle que $N_K^L I_L = H$.*

Démonstration. [CF], Chapitre VII, théorème 5.1. □

Définition 2.47. *Soit K un corps de nombres. Un ordre $\mathcal{O}$ de K est un sous-anneau de K qui est finiment engendré en tant que $\mathbb{Z}$-module et vérifie $\mathcal{O} \otimes \mathbb{Q} = K$.*

On suppose à présent que K est un corps quadratique imaginaire.

On note $\mathcal{O}_K$ l'anneau des entiers de K, et $\mathcal{O}$ un ordre de K. Soit $c = [\mathcal{O}_K : \mathcal{O}]$ son conducteur.

Définition 2.48. *Le groupe de Picard de $\mathcal{O}$ est le groupe $Pic(\mathcal{O})$ formé par l'ensemble des $\mathcal{O}$-modules projectifs de rang 1. La loi de composition est donnée par le produit tensoriel des modules.*

Le groupe $Pic(\mathcal{O})$ est naturellement isomorphe au groupe de classe $Cl_{\mathcal{O}}$ de $\mathcal{O}$, c'est-à-dire le groupe des idéaux fractionnaires inversibles de $\mathcal{O}$ modulo le groupe des idéaux principaux.

Lemme 2.49. *Soit $I(c)$ le groupe des idéaux fractionnaires de K premiers à (c), et $P(c)$ le groupe des ideaux principaux de K premiers à (c). Alors,*

$$Cl_{\mathcal{O}} \simeq \frac{I(c)}{P(c)}.$$

Comme $P_1((c)) \subset P(c) \subset I(c)$, le théorème 2.46, point 4, montre qu'il existe une unique extension H de K telle que $Gal(H/K) \simeq Cl_{\mathcal{O}}$. On appellera ce corps le *ring class field* de $\mathcal{O}$, ou encore le *ring class field* de K *modulo* c.

2.5.2 Multiplication Complexe

Soit E une courbe elliptique définie sur $\mathbb{C}$. Le théorème d'uniformisation de Weierstrass nous dit qu'il existe un réseau Γ de $\mathbb{C}$ tel que $E \simeq \mathbb{C}/\Gamma$. Un endomorphisme de E est la multiplication par un $z \in \mathbb{C}$ tel que $z\Gamma \subset \Gamma$. En général, End$(E)\simeq \mathbb{Z}$. Lorsque End(E) est plus gros que $\mathbb{Z}$, on dit que E a *multiplication complexe*. Les courbes elliptiques ayant multiplication complexe ont des propriétés intéressantes ; nous en donnons quelques-unes dans cette section.

Proposition 2.50. *Soit $E/\mathbb{C}$ une courbe elliptique et ω_1, ω_2 des générateurs du réseau Γ associé à E par l'uniformisation de Weierstrass. Alors soit*

1. *End(E)$\simeq \mathbb{Z}$, ou*
2. *$\mathbb{Q}(\omega_1/\omega_2)$ est une extension quadratique imaginaire de $\mathbb{Q}$, et End(E) est isomorphe à un ordre de $\mathbb{Q}(\omega_1/\omega_2)$.*

Démonstration. Soit $\tau = \omega_1/\omega_2$, on peut se ramener à $\Gamma = \mathbb{Z}+\tau\mathbb{Z}$ en appliquant une homothétie. Soit $\mathcal{O}= \{\alpha \in \mathbb{C}, \alpha\Gamma \subset \Gamma\}$ $\simeq$End(E). Alors, pour tout $\alpha \in \mathcal{O}$, il existe des entiers a, b, c, d tels que

$$\alpha = a + b\tau \text{ et } \alpha\tau = c + d\tau.$$

En éliminant τ on obtient

$$\alpha^2 - (a + d)\alpha + bc = 0.$$

$\mathcal{O}$ est donc une extension entière de $\mathbb{Z}$. Supposons $\mathcal{O}\neq \mathbb{Z}$, et soit $\alpha \in \mathcal{O}$, $\alpha \notin \mathbb{Z}$. Alors, $b \neq 0$, et l'élimination de α dans les équations ci-dessus donne

$$b\tau^2 - (a - d)\tau + c = 0.$$

$\mathbb{Q}(\tau)$ est donc une extension quadratique imaginaire de $\mathbb{Q}$. Finalement, comme $\mathcal{O}\subset \mathbb{Q}(\tau)$ et $\mathcal{O}$ est entier sur $\mathbb{Z}$, $\mathcal{O}$ est un ordre de $\mathbb{Q}(\tau)$. □

Dans le cas 2, on dit que E a *multiplication complexe par* $\mathcal{O}$.

On peut effectuer le processus inverse, c'est-à-dire partir d'un ordre et essayer de construire une courbe elliptique ayant multiplication complexe par cet ordre.

Soit K un corps imaginaire quadratique, et $\mathfrak{a}$ un idéal fractionnaire inversible non nul de l'ordre $\mathcal{O}$ de K. En utilisant le plongement $\mathfrak{a} \subset K \subset \mathbb{C}$, on voit que $\mathfrak{a}$ est un réseau de $\mathbb{C}$. On peut donc construire une courbe elliptique $E_{\mathfrak{a}}$ dont l'anneau des endomorphismes est

$$\begin{aligned} End(E) &\simeq \{\alpha \in \mathbb{C}, \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K, \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \mathcal{O}, \text{ puisque } \mathfrak{a} \text{ est un idéal fractionnaire inversible de } \mathcal{O}. \end{aligned}$$

Comme deux réseaux de $\mathbb{C}$ reliés par une homothétie donnent deux courbes elliptiques isomorphes, on a ainsi défini une application

$$Cl_{\mathcal{O}} \to \mathcal{ELL}(\mathcal{O}),$$

où $\mathcal{ELL}(\mathcal{O})$ désigne l'ensemble des courbes elliptiques à multiplication complexe par $\mathcal{O}$, modulo isomorphisme.

Proposition 2.51. *1. Soit Γ un réseau tel que $E_\Gamma \in \mathcal{ELL}(\mathcal{O})$, et $\mathfrak{a}, \mathfrak{b}$ deux idéaux fractionnaires inversibles de $\mathcal{O}$.*
- *$\mathfrak{a}\Gamma$ est un réseau de $\mathbb{C}$.*
- *La courbe elliptique $E_{\mathfrak{a}\Gamma}$ est telle que End($E_{\mathfrak{a}\Gamma}$)$\simeq \mathcal{O}$.*
- *$E_{\mathfrak{a}\Gamma} \simeq E_{\mathfrak{b}\Gamma}$ si et seulement si $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$ dans $Cl_{\mathcal{O}}$.*

Il y a donc une action bien définie de $Cl_{\mathcal{O}}$ sur $\mathcal{ELL}(\mathcal{O})$ déterminée par :

$$\bar{\mathfrak{a}} * E_\Gamma = E_{\mathfrak{a}^{-1}\Gamma}.$$

2. Cette action est simplement transitive. En particulier,

$$\#Cl_{\mathcal{O}} = \#\mathcal{ELL}(\mathcal{O}).$$

Démonstration. [Si94], Chapitre II, proposition 1.2. □

À chaque courbe E on peut associer son j-invariant $j(E)$. Comme j ne dépend que de la classe d'isomorphisme de E, il y a exactement $h_{\mathcal{O}}$ tels nombres, où $h_{\mathcal{O}}$ est le cardinal du groupe de classe de $\mathcal{O}$.

Théorème 2.52. *1. Les $j(E)$ sont des entiers algebriques.*

2. Soit $\alpha = j(E)$ l'un d'eux. Le corps $K(\alpha)$ est le ring class field *de K modulo (c).*

Démonstration. [CF], XIII.1. □

D'après le théorème 2.46, le groupe de classe de $\mathcal{O}$ s'identifie, via l'application d'Artin, au groupe de galois de K_c/K, où K_c est le *ring class field* de conducteur c de K. $Cl_{\mathcal{O}}$ agit donc sur les j-invariants des courbes elliptiques ayant multiplication complexe par $\mathcal{O}$; le théorème suivant décrit cette action.

Théorème 2.53. *Soit $\mathfrak{p}$ un premier de K qui soit premier avec c, et $\mathfrak{p}_c = \mathfrak{p} \cap \mathcal{O}$ l'idéal correspondant de $\mathcal{O}$. Soit $\mathfrak{a} \in Cl_{\mathcal{O}}$ et $E_{\mathfrak{a}}$ la courbe elliptique correspondante. Alors le Frobenius $\sigma_{\mathfrak{p}}$ agit sur $j(E_{\mathfrak{a}})$ de la facon suivante :*

$$j(E_{\mathfrak{a}})^{\sigma_{\mathfrak{p}}} = j(E_{\mathfrak{p}_c\mathfrak{a}}).$$

Démonstration. [CF], XIII.1. □

3 Points de Heegner

3.1 Définition

On suit ici la présentation des points de Heegner donnée dans [Gr84].

Définition 3.1. *Soit N un entier strictement positif. Un point de Heegner sur $Y_0(N)$ est une paire (E, E') de courbes elliptiques (modulo isomorphisme) reliées par une isogénie cyclique de degré N, ayant* le même anneau de multiplication complexe $\mathcal{O} = EndE = EndE'$.

Pour mener à bien les calculs de la section 4, nous avons besoin de caractériser les points de Heegner en tant que points de $\mathcal{H}/\Gamma_0(N)$. Soit $y = (E, E')$ un point de Heegner. Comme on l'a vu en 2.4.2, on peut écrire $E = \mathbb{C}/M, E' = \mathbb{C}/M'$, où M et M' sont des réseaux de $\mathbb{C}$. On peut de plus choisir une base $< \omega_1, \omega_2 >$ de M telle que $< \omega_1, \omega_2/N >$ soit une base de M'. Au point y on fait correspondre l'orbite de $\tau = \omega_2/\omega_1$ dans $\mathcal{H}/\Gamma_0(N)$. E et E' sont des courbes à multiplication complexe, et donc leur anneau d'endomorphismes est un ordre $\mathcal{O}$ dans un corps imaginaire quadratique K. Soit $\alpha \in \mathcal{O} \setminus \mathbb{Z}$. Alors il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$ telles que

$$\alpha = a + b\tau, \;\; \alpha\tau = c + d\tau,$$
$$\alpha = a' + b'\tau/N, \;\; \alpha\tau/N = c' + d'\tau/N,$$

d'où $b\tau^2 + (a-d)\tau - c = 0$, et $c = Nc'$. Comme $b\tau = \alpha - a$, on a $b\tau \in \mathcal{O}$. En multipliant l'équation ci-dessus par b on obtient un polynôme unitaire en $b\tau$; son discriminant $(a-d)^2 + 4bc$ est donc le discriminant de $\mathcal{O}$, soit $c^2 D$, ou c est le conducteur de $\mathcal{O}$ et D le discriminant de K.

Réciproquement, soit $\tau \in \mathcal{H}$ satisfaisant une équation quadratique

$$A\tau^2 + B\tau + C = 0, \;\; A, B, C \in \mathbb{Z}, \;\; gcd(A, B, C) = 1, \;\; A = NA', \;\; B^2 - 4AC = c^2 D,$$

où D est un discriminant. Il n'est alors pas difficile de voir que les deux courbes elliptiques associées aux réseaux $< 1, \tau >$ et $< 1, \tau/N >$ ont toutes les deux multiplication complexe par l'unique ordre de conducteur c de $\mathbb{Q}(\sqrt{D})$.

3.2 Propriétés

Soit $y = (E, E')$ un point de Heegner, et $\mathcal{O} = \mathrm{End}E = \mathrm{End}E'$. Les réseaux M et M' tels que $E = \mathbb{C}/M$, $E' = \mathbb{C}/M'$ sont alors des $\mathcal{O}$-modules projectifs de rang 1. En les modifiant par une homothétie, on peut supposer que $M = \mathfrak{a}$ et $M' = \mathfrak{b}$ sont tous les deux des sous-$\mathcal{O}$-modules de K, et que $\mathfrak{a} \subset \mathfrak{b}$. Le module $\mathfrak{n} = \mathfrak{a}\mathfrak{b}^{-1}$ est tel que $\mathcal{O}/\mathfrak{n}$ soit cyclique d'ordre N. Le point y ne dépend que de $\mathcal{O}$, de la classe de $\mathfrak{a}$ dans $Pic(\mathcal{O})$ (puisque E et E' sont considérées modulo isomorphisme), et de $\mathfrak{n}$. Réciproquement, étant donnés ces trois éléments, on peut définir un point de Heegner $(\mathbb{C}/\mathfrak{a}, \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1})$. On notera ce point $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$.

Soit c le conducteur de $\mathcal{O}$, que l'on supposera dans la suite premier à N. On supposera également toujours que l'hypothèse suivante est vérifiée :

Hypothèse 3.2. *Tous les entiers premiers qui divisent N sont déployés dans $K/\mathbb{Q}$.*

Cette hypothèse est nécessaire pour qu'il existe un idéal $\mathfrak{n} \subset \mathcal{O}$ inversible de quotient cyclique d'ordre N. En effet, si un tel idéal existe, on peut construire un morphisme d'anneaux ϕ : $\mathcal{O} \to \mathbb{Z}/N\mathbb{Z}$, qui est simplement la réduction modulo $\mathfrak{n}$. Comme le conducteur est premier à N, ce morphisme s'étend à $\mathcal{O}_K$. Soit $p|N$ premier. Si p ramifiait dans $K/\mathbb{Q}$, on aurait $(p) = \mathfrak{p}^2$ et l'image de p par ϕ serait un carré, ce qui est absurde.

D'après le théorème 2.52, les points de conducteur c sont définis sur le corps $H = K(j(\mathcal{O}))$, de groupe de Galois $G = Gal(H/K)$ isomorphe à $Pic(\mathcal{O})$ (théorème 2.46). Le théorème suivant décrit l'action de G sur les points de Heegner :

Théorème 3.3. *Soit* $\mathfrak{b} \in Pic(\mathcal{O})$*, et* $(\mathfrak{b}, H/K)$ *son symbole d'Artin dans Gal*(H/K)*. Alors*

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^{(\mathfrak{b}, H/K)} = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]).$$

Démonstration. Cela découle du théorème 2.53. □

Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N. On s'intéresse à l'image des points de Heegner sur E par la paramétrisation modulaire Φ_N. Le théorème suivant donne le corps de définition de ces points.

Théorème 3.4. *Soit* $y = (E, E')$ *un point de Heegner sur* $X_0(N)$*. Alors* $\Phi_N(y) \in E(H)$*.*

Démonstration. Nous allons utiliser la description de $X_0(N)$ comme courbe définie sur $\mathbb{Q}$. À y on peut faire correspondre un point $\tau \in \mathcal{H}/\Gamma_0(N) \cap K$. D'après le théorème 2.52, $j(\tau) = j(E)$ et $j(N\tau) = j(E')$ sont tous les deux définis sur H, donc l'image de τ sur la courbe rationnelle $X_0(N)$ est définie sur H. L'application $X_0(N) \to E$ induite par Φ_N est alors un morphisme de courbes algébriques définies sur $\mathbb{Q}$, et donc $\Phi_N(\tau) \in E(H)$. □

La théorie de la multiplication complexe nous permet finalement de décrire l'action de $G = Gal(H/K)$ sur l'image des points de Heegner sur E.

Théorème 3.5. *Soit* $y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ *un point de Heegner. Soit* $\mathfrak{b} \in Pic(\mathcal{O})$*, et* $(\mathfrak{b}, H/K)$ *le symbole d'Artin de* $[\mathfrak{b}]$ *dans Gal*(H/K)*. Alors*

$$\Phi_N(y)^{(\mathfrak{b}, H/K)} = \Phi_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]) = \varPhi_N(y^{(\mathfrak{b}, H/K)}).$$

Démonstration. La première égalité est une conséquence immédiate de la description de $X_0(N)$ comme courbe algébrique sur $\mathbb{Q}$ et du théorème 2.53, la deuxième est le théorème 3.3. □

3.3 Points de Heegner et séries L

Dans l'article [GZ], Gross et Zagier ont montré l'existence d'un lien remarquable entre les dérivées de la série L d'une courbe elliptique et la hauteur des points de Heegner sur cette courbe.

Soit E une courbe elliptique définie sur $\mathbb{Q}$, et soit N son conducteur. On a vu dans les sections précédentes que l'on pouvait définir certains points particuliers sur cette courbe, les points de Heegner, qui sont définis comme l'image sur E par la paramétrisation modulaire de points de $X_0(N)$.

Si on se fixe un ordre $\mathcal{O}$ de conducteur c dans un corps quadratique K de discriminant D, et si l'on suppose que l'hypothèse 3.2 est vérifiée, alors on a vu qu'il y avait exactement $h = \#Pic(\mathcal{O}) = \mathcal{ELL}(\mathcal{O})$ points de Heegner distincts sur E, et que ces points étaient définis sur H, le *ring class field* de conducteur c de K. Soient $P = P_1, \ldots, P_h$ ces h points (les références à E et $\mathcal{O}$ sont implicites). Le théorème 3.5 montre qu'ils sont permutés par $G = Gal(H/K)$. Ainsi, si on se donne un caratère χ de G, toute combinaison linéaire

$$P_\chi = \sum_{\sigma \in G} \chi(\sigma) P^\sigma$$

est invariante par G, et est donc définie sur $E(K) \otimes \mathbb{C}$. On note $\hat{h}_K(P_\chi) =< P_\chi, P_\chi >_K$ sa hauteur de Néron-Tate (définie en 2.3).

Soit $L(E/\mathbb{Q}, s) = \sum a_n n^{-s}$ la série L de E sur $\mathbb{Q}$, comme définie en 2.2.3. Soit $\mathcal{A}$ une classe d'idéaux du groupe de classe de K. On note $r_{\mathcal{A}}(n) = \#\{\text{idéaux de } \mathcal{A} \text{ de norme } n\}$. La série considérée par Gross et Zagier est la suivante :

$$L_{\mathcal{A}}(E, s) = \sum_{(n,N)=1} \left(\frac{D}{n}\right) \frac{1}{n^{2s-1}} \sum_{n \in \mathbb{N}} \frac{a_n r_{\mathcal{A}}(n)}{n^s}.$$

C'est le produit de la série de Dirichlet de charactère $\left(\frac{D}{n}\right)$ (dont on a enlevé les termes divisant le conducteur) par le produit de convolution de la série L de $E/\mathbb{Q}$ et de la série de Dedekind du corps $K = \mathbb{Q}(\sqrt{D})$.

Posons :

$$L_K(E, \chi, s) = \sum_{\mathcal{A} \in Cl_K} \chi(\mathcal{A}) L_{\mathcal{A}}(E, s).$$

Gross et Zagier mettent en relation $L'_K(E, \chi, 1)$ et $\hat{h}_K(P\chi)$ de la manière suivante :

Théorème 3.6. *(Gross-Zagier). Soit E une courbe elliptique définie sur $\mathbb{Q}$. En reprenant les notations ci-dessus,*

$$L'_K(E, \chi, 1) = \frac{2\Omega}{u^2\sqrt{|D|}} \hat{h}_K(P\chi),$$

où $2u$ est le nombre de racines de l'unité de K et $\Omega = Im(\omega_1 \bar{\omega_2})$ est le volume complexe.

Pour faire apparaître la hauteur du point de Heegner seul, qui est l'objet qui nous intéresse, nous pouvons sommer la relation donnée par le théorème sur tous les caractères du groupe de Galois. Alors, d'après les relations d'orthogonalité 2.12, on obtient :

$$L'_{Id}(E, 1) = \frac{2\Omega}{u^2\sqrt{|D|}} \hat{h}_H(P),$$

où Id désigne l'identité de $Pic(\mathcal{O})$. On montrera en 5.2 qu'on a $L_K(E, \mathbf{1}, s) = L(E/K, s)$, où $\mathbf{1}$ désigne le caractère principal du groupe de classe.

On a ainsi la correspondance suivante :

$$\begin{array}{ccccc} L'(E/K,1) & = & L'_{Id}(E,1) & + & \sum_{\sigma \in G \setminus \{Id\}} L'_\sigma(E,1) \\ \updownarrow & & \updownarrow & & \updownarrow \\ \hat{h}_H(\sum_{\sigma \in G} P^\sigma) & = & h \cdot \hat{h}_H(P) & + & h \cdot \sum_{\sigma \in G \setminus \{Id\}} < P, P^\sigma >_H, \end{array}$$

les $\updownarrow$ désignant la multiplication par un même facteur $\frac{2\Omega}{u^2\sqrt{|D|}h}$. Cette décomposition nous conduit à nous interroger sur le rapport entre les hauteurs des points et celle de leur trace. Le troisième terme représente en quelque sorte l'angle formé par les points de Heegner. On pourrait espérer que cet angle soit, en moyenne (sur les différents discriminants D possibles), nul. Nous verrons dans les sections suivantes que ce n'est pas le cas, et que l'angle formé par les points de Heegner, et en particulier son signe (i.e. s'il est aigu ou grave), dépend de la courbe elliptique considérée.

4 Algorithmique

Dans cette partie, nous allons présenter plusieurs approches algorithmiques différentes au problème du calcul de la hauteur des points de Heegner, et analyser leur complexité.

La première méthode consiste naturellement à calculer le point de Heegner sur la courbe, puis à évaluer sa hauteur. Il est toutefois impossible en pratique de reconnaître le point comme élément du corps de classe, car il est très coûteux de calculer la structure de ce corps (le logiciel Magma permet de le faire pour des nombres de classe allant jusqu'à 6 ou 7). On se contente donc de calculer le polynôme minimal sur $\mathbb{Q}(\sqrt{D})$ des points de Heegner dont on aura calculé les coordonnées complexes avec suffisamment de précision. La hauteur (logarithmique) des coefficients du polynôme fournit alors une bonne approximation de la hauteur de Néron-Tate du point de Heegner (cf. la section 2.3).

On peut aussi calculer directement la valeur de la dérivée en 1 de la série de Rankin-Selberg qui apparaît dans la formule de Gross-Zagier, et en déduire la hauteur du point de Heegner. Cette méthode a plusieurs avantages, mais bien sûr elle ne permet pas de remonter au point de Heegner lui-même.

Dans une première partie nous allons présenter l'algorithme de calcul des points de Heegner sur une courbe elliptique de conducteur N, pour un discriminant D qui satisfait l'hypothèse 3.2, puis nous analyserons sa complexité. Dans une deuxième partie, nous montrerons comment tirer parti de la formule de Gross-Zagier pour calculer directement la hauteur du point de Heegner.

4.1 Calcul du polynôme minimal des points de Heegner

Dans cette section on fixe un entier N strictement positif et un discriminant D (non nécessairement fondamental) satisfaisant l'hypothse 3.2 pour ce N. Si $D = c^2 \cdot d$, où d est sans facteur carré, on note $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$ et $\mathcal{O}$ l'ordre de K de conducteur c.

4.1.1 Calcul des points de Heegner sur $X_0(N)$

Soit $Q(D)$ l'ensemble des formes quadratiques $q(x, y) = Ax^2 + Bxy + Cy^2$ de discriminant $B^2 - 4AC = D$, et $q_1, \dots, q_h$ ($h = \#Q(D)/SL_2(\mathbb{Z}) = \#Pic(\mathcal{O})$) des représentants de chacune des classes de $Q(D)/SL_2(\mathbb{Z})$ tels que, si s_D est une racine carrée de $D \mod 4N$ fixée, on ait : $\forall i \in \{1 \dots h\}$,

- $A_i \equiv 0 \mod N$,
- $B_i \equiv s_D \mod 2N$.

Alors, comme on l'a vu dans la section 3, les h points de Heegner $\tau_1, \dots, \tau_h$ sont définis par :

$$\forall i \in \{1, \dots, h\}, \quad \tau_i = \frac{-B_i + \sqrt{D}}{2A_i}$$

Théorème 4.1. *Pour tout $1 \leq i \leq h$, il existe une forme quadratique $A'_i x^2 + B'_i xy + C'_i y^2$ équivalente à q_i et telle que $|A'_i| \leq \sqrt{|D|} \cdot N/2$. De plus, il suffit de $O(|D|)$ opérations pour calculer un tel représentant de chaque classe, et donc pour calculer les h points de Heegner.*

Démonstration. La première étape consiste à calculer des représentants réduits de chacune des classes de formes quadratiques. L'algorithme 5.3.5 de [Coh93] permet de le faire en $O(|D|)$ opérations élémentaires.

La deuxieme étape consiste à déterminer, pour chacun de ces représentants, une forme équivalente qui vérifie les conditions du théoreme. On veut donc minimiser le premier coefficient de la forme quadratique, parmi ceux qui sont divisibles par N.

Lorsque l'on multiplie une forme quadratique par une matrice $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in SL_2(\mathbb{Z})$, on obtient une forme de coefficient $A_i a_i^2 + B_i a_i c_i + C_i c_i^2$ en x^2. La congruence à 0 modulo N est équivalente à la congruence $a_i \equiv \lambda_i c_i \mod N$, où λ_i est une racine de $A_i x^2 + B_i x + C_i \mod N$. Le changement de variables $a_i = \lambda_i \alpha_i + \beta_i N$, $c_i = \alpha_i$, nous ramène à minimiser la forme quadratique $q_i' = (A_i \lambda_i^2 + B_i \lambda_i + C_i)\alpha_i^2 + (2A_i\lambda_i N + B_i N)\alpha_i \beta_i + A_i N^2 \beta_i^2$ sur $\mathbb{Z}^2$, ce qui peut se faire avec les techniques standard de réduction en $O(\log N)$, et garantit une valeur inférieure à $\sqrt{|D|}/2$.

Soit (α_i^0, β_i^0) tel que $q_i'(\alpha_i^0, \beta_i^0)$ soit inférieur a $\sqrt{|D|}/2$. α_i^0 et β_i^0, donc a_i et c_i, étant premiers entre eux (sinon ils ne réaliseraient pas le minimum), on peut trouver b_i et d_i tels que $T_i = \begin{pmatrix} \lambda_i \alpha_i^0 + \beta_i^0 N & b_i \\ \alpha_i^0 & d_i \end{pmatrix} \in SL_2(\mathbb{Z})$. Pour un bon choix de λ_i parmi les deux possibles, les formes $q_i * T_i$ ainsi obtenues vérifient les conditions du théorème. □

4.1.2 L'image des points de Heegner sur la courbe elliptique

Pour trouver l'image des points τ_i dans le quotient C/Λ isomorphe à la courbe elliptique considérée par la paramétrisation de Weierstrass, il faut calculer l'image de ces points par la paramétrisation modulaire ; ceci est fait en utilisant la proposition 2.42.

Soit $f(q) = \Sigma_{n=1}^{\infty} a_n q^n$ la *newform* attachée à E. La proposition 2.42 montre que l'image z_i de τ_i est donnée par :

$$z_i = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2i\pi n \tau_i}.$$

Théorème 4.2. *Étant donné $\tau \in \mathfrak{H}$, on peut calculer $f(\tau)$ avec une précision de d chiffres en $O(d^2 \log d/(Im\tau)^2)$ opérations élémentaires.*

Démonstration. [Da2] □

Ici, $Im\tau > 1/N$, d'où une complexité en $O(d^2 \log d \cdot N^2)$ par point, soit $O(h \cdot d^2 \log d \cdot N^2)$ au total. Tout l'objet de la section 5 sera de parvenir à estimer d a priori, pour que la précision soit suffisante pour reconnaître les coefficients du polynôme minimal des $f(\tau_i)$ dans K.

Il reste à calculer l'image du point ainsi obtenu sur la coube elliptique par la paramétrisation de Weierstrass. La complexité de ce calcul est dominée par celle du calcul précédent.

4.1.3 Conclusion

Lorsque l'on a calculé les points $(x_1, y_1) \dots, (x_h, y_h)$, on peut former le polynôme $\Pi(X - x_i)$ et reconnaître ses coefficients dans $\mathbb{Q}(\sqrt{D})$. Pour cela, on utilise les fractions continues. Si on suppose à priori que la hauteur (logarithmique) des coefficients du polynôme est k, alors pour les reconnaître il suffit de connaître les x_i avec une précision de $2k$ chiffres. L'algorithme des fractions continues a une complexite en $O(\log k)$. Il faut l'appliquer $2h$ fois (partie réelle et partie imaginaire), d'où une complexité qui est majorée par celle du calcul de l'image des points par la paramétrisation modulaire ($h = O(\sqrt{D})$).

Théorème 4.3. *Soit E une courbe elliptique de conducteur N, et D un discriminant négatif. Soit k la hauteur logarithmique présumée des coefficients du polynôme minimal des points de Heegner.*

Alors la complexité de l'algorithme décrit pour calculer ce polynôme est de $O(k^2 \log k \cdot \sqrt{D} \cdot N^2)$ opérations élémentaires.

Remarque. *Nous verrons dans la section 5.3.2 que l'on a essentiellement $k = O(\sqrt{D}\log D)$, où le "essentiellement" veut dire que cette majoration est valable pour la moyenne des hauteurs des points de Heegner sur tous les dicriminants plus petits qu'une constante fixée. Ainsi, on s'attend à ce que la complexité de l'algorithme décrit soit en $O(D^{3/2}(\log D)^3 \cdot N^2)$.*

4.1.4 Une autre approche

On peut également décider de calculer l'image d'un seul point de Heegner, puis d'utiliser l'algorithme LLL ou des variantes ([HJLS]) pour trouver le polynôme minimal du point de Heegner sur $\mathbb{Q}(\sqrt{|D|})$, connaissant a priori sa hauteur h. Le principal avantage de cette méthode est que l'on peut choisir le point τ qui a la plus grande partie imaginaire, ce qui permet d'économiser un facteur $\sqrt{|D|}$ dans la complexité. L'inconvénient est qu'il faut appliquer LLL, et pour cela il faut connaître le point de Heegner avec une précision de $k \cdot h$ chiffres. Cette précision est donc exponentielle en le nombre de classe du corps considéré. Puis, l'application de LLL a une complexité de $O(h^3(h+k)) = O(D^{3/2}(\sqrt{D}+h))$ (dans la version de [HJLS]). Finalement, la complexité de cette méthode est de $O(k^2\log(k\sqrt{D})N^2 + D^{3/2}(\sqrt{D}+h))$ opérations élémentaires.

Remarque. *En reprenant la remarque de la section précédente, on voit que le complexité de cette méthode est de $O(D(\log D)^3 N^2 + D^2\log D)$ en moyenne. Ainsi, l'approche basée sur l'algorithme LLL pour reconaître les coefficients du polynôme est plus efficace lorsque $N \gg D^{1/4}$; alors que notre première approche sera plus efficace si $N \ll D^{1/4}$. Les calculs que nous avonc menés ont en général concerné des conducteurs compris entre 11 et 200, alors que les discriminants sont restés en-dessous de 10^4 ; la deuxième méthode aurait donc été plus efficace. Mais, l'estimation de k que l'on a donnée n'est valable qu'en moyenne, et en pratique il m'a paru beaucoup plus facile de travailler avec la première méthode.*

4.2 Évaluation de séries L

Soit $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ une série L (formelle), c'est-à-dire simplement la donnée d'une suite de coefficients $(a_n) \in \mathbb{C}^{\mathbb{N}}$. Alors, sous réserve d'hypothèses très générales, il est possible de calculer efficacement la valeur de la série et de ses dérivées en tout point du plan complexe, connaissant suffisamment de coefficients. Ceci est détaillé dans [Coh00], nous allons nous contenter d'expliciter l'algorithme employé dans le cas de la série

$$L_{\mathcal{A}}(s) = \sum_{n \nmid N} \chi_D(n) n^{1-2s} \cdot \sum_{n=1}^{\infty} r_{\mathcal{A}}(n) a_n n^{-s} =: \sum_{n=1}^{\infty} b_n n^{-s}$$

où $\mathcal{A}$ désigne la classe d'idéaux jouant le rôle du neutre dans le groupe de classe de $K = \mathbb{Q}(\sqrt{D})$, et $r_{\mathcal{A}}(n)$ est le nombre d'idéaux dans cette classe de norme n. N est le conducteur de la courbe elliptique E que l'on considère, les a_n sont les coefficients de la paramétrisation modulaire, et $\chi_D(n) = \left(\frac{D}{n}\right)$ est le caractère de Dirichlet associé à K.

Cette série L est la série qui apparaît dans [GZ] et dont la dérivée en 1 est mise en relation avec la hauteur d'un point de Heegner (cf la section 3.3). Gross et Zagier ont montré que cette série se prolongeait en une fonction entière de s sur $\mathbb{C}$, et vérifiait l'équation fonctionnelle :

$$L^*_{\mathcal{A}}(s) = -\chi_D(N) L^*_{\mathcal{A}}(2-s), \quad L^*_{\mathcal{A}}(s) = (2\pi)^{-2s} N^s |D|^s \Gamma(s)^2 L_{\mathcal{A}}(s).$$

Comme nous supposons toujours que l'hypothèse 3.2 est vérifiée, on a $\chi_D(N) = 1$.

On note $\gamma(s) = (2\pi)^{-2s} N^s |D|^s \Gamma(s)^2$ le facteur qui apparait dans l'équation fonctionnelle de $L_{\mathcal{A}}(s)$.

Théorème 4.4. *Soit*
$$F(s,x) = \frac{x^s}{2i\pi}\int_{1-i\infty}^{1+i\infty} \frac{x^{-z}\gamma(z)}{z-s}dz = \frac{1}{2i\pi}\int_{1-i\infty}^{1+i\infty} \frac{x^{-z}\gamma(z+s)}{z}dz.$$
Alors, pour tout $t_0 > 0$,
$$L^*_{\mathcal{A}}(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}F(s, nt_0) - \sum_{n=1}^{\infty} \frac{b_n}{n^{2-s}}F(2-s, n/t_0).$$

Démonstration. [Coh00], Appendix A, Théorème 10.3.4. □

L'intérêt de ce théorème est qu'il permet de calculer $L^*_{\mathcal{A}}(s)$ en tout point du plan complexe, alors que la série de Dirichlet qui la définit ne converge absolument que pour $s > 3/2$. De plus, la fonction $F(s,x)$ décroît plus vite vers 0 que n'importe quelle puissance de x, ce qui permet de conduire le calcul en pratique avec une bonne efficacité, puisque les b_n ont, eux, une croissance au plus polynômiale.

Pour $s = t_0 = 1$, on obtient $L^*_{\mathcal{A}}(s) = 0$. On désire calculer la dérivée de cette série en 1, pour cela il ne nous reste qu'à donner une manière de calculer la dérivée de $F(s,x)$ par rapport à s en 1.

Théorème 4.5. *Pour tout pôle* a *de* $\gamma(z)$ *on note*
$$\gamma(z) = \sum_{k=1}^{m} \frac{u_{k,a}}{(z-a)^k} + \textit{holomorphe en } a.$$
Alors, si s *n'est pas un pôle de* γ,
$$F(s,x) = \gamma(s) - \sum_a x^{s-a} \sum_{j=0}^{m-1} (-1)^j \frac{\log^j x}{j!} \sum_{k=j+1}^{m} \frac{u_{k,a}}{(s-a)^{k-j}}.$$

Démonstration. [Coh00], Appendix A, 10.3.2. □

Il nous reste à calculer les $u_{i,j}$ dans notre cas ; on le fait pour $\gamma(s) = \Gamma(s)^2$, les autres termes ne jouant pas de rôle. Les seuls pôles de γ sont les entiers négatifs, écrivons
$$\Gamma(s) = \frac{\alpha_n}{s+n} + \beta_n + o((s+n))$$
au voisinage de $s = -n$. Alors, il est bien connu qu'on a $\alpha_n = \dfrac{(-1)^n}{n!}$. On peut calculer β_n par
$$\beta_n = \frac{\partial}{\partial s}\left((s+n)\Gamma(s)\right)_{s=1}.$$
En utilisant l'égalité
$$\forall z \in \mathbb{C},\ -\frac{\Gamma'(z)}{\Gamma(z)} = \frac{1}{z} + \gamma + \sum_{n=1}^{\infty}\left(\frac{1}{z+n} - \frac{1}{n}\right)$$
qu'on obtient en prenant la dérivée logarithmique de Γ, on obtient
$$\beta_n = \frac{(-1)^n}{n!}\left(-\gamma + \sum_{k=0}^{n-1}\frac{1}{n-k}\right).$$

Dans notre cas, la formule exprimant $F(s,x)$ se réécrit donc :

$$F(s,x) = \gamma(s) - (2\pi)^{-2s} N^s |D|^s \sum_{a=0}^{\infty} x^{s+a} \left(\frac{2\alpha_{-a}\beta_{-a} - (\log x)\alpha_{-a}^2}{s+a} + \frac{\alpha_{-a}^2}{(s+n)^2} \right).$$

On peut ensuite dériver terme à terme. Cependant, cette formule n'est pas intéressante pour calculer $F(s,x)$ dès que x est grand, car il y a beaucoup d'annulations entre les termes : par exemple, pour $\gamma(s) = \Gamma(s)$ on aurait obtenu pour $F(s,x)$ le dévelopement en série entière de e^{-x}, qui n'est pas une bonne manière de calculer cette fonction si x est grand. Dans ce cas, on utilise une méthode basée sur les développements en fractions continues ([Coh00], Appendix A).

5 Étude expérimentale

Nous présentons ici les résultats expérimentaux que nous avons obtenus, ainsi que quelques résultats théoriques sur les hauteurs en moyenne des points de Heegner et de leur trace. Nous commençons par donner quelques exemples de polynômes minimaux de ces points, avant de nous intéresser à la hauteur de leurs traces, puis à leur hauteur elle-même. On pourra se reporter à l'annexe 6.2 pour quelques notes d'implémentation.

5.1 Polynômes minimaux

Une implémentation de l'algorithme décrit dans la section précédente nous a permis de calculer les polynômes minimaux d'un grand nombre de points de Heegner, pour des courbes et des corps quadratiques variés. Comme on n'a, pour l'instant, aucune connaissance a priori de la hauteur des polynômes, j'ai choisi d'implémenter la première version de l'algorithme (celle qui ne fait pas appel à la réduction LLL). Le tableau ci-dessous donne quelques exemples de polynômes obtenus, pour des discriminants et des courbes variés.

rg désigne le rang de la courbe elliptique, et *deg* le degré de la paramétrisation modulaire Φ_N.

N	E	rg	deg	D	P
11	$y^2+y=x^3-x^2-10x-20$	0	1	-24	$46+17\sqrt{-24}+(4-3\sqrt{-24})x+2x^2$
				-39	$1394+388\sqrt{-39}+(-121+223\sqrt{-39})x$ $+(154+68\sqrt{-39})x^2+(47-3\sqrt{-39})x^3+2x^4$
				-96	$(-70244-1476\sqrt{-96})+(-48688-2571\sqrt{-96})x$ $+(-8656-912\sqrt{-96})x^2+(1000+15\sqrt{-96})x^3+4x^4$
37	$y^2+y=x^3-x$	1	2	-40	$2+x^2$
				-63	$-3-6x+3x^3+x^4$
37	$y^2+y=x^3+x^2-23x-50$	0	2	-40	$(7238+307\sqrt{-40})+(4798+46\sqrt{-40})x+722x^2$
				-63	$(24862416+2283318\sqrt{-63})+(23215518+1803866\sqrt{-63})x$ $+(8590851+470019\sqrt{-63})x^2$ $+(1468494+44338\sqrt{-63})x^3+96774x^4$
67	$y^2+y=x^3+x^2-12x-21$	0	5	-20	$29+24x+5x^2$
				-63	$2305+2924x+1242x^2+179x^3+x^4$
				-87	$17681+43193x+41798x^2+20260x^3+5092x^4+608x^5+25x^6$
116	$y^2=x^3-4831x-129242$	0	120	-23	$50256691740461875+3757711971630382x$ $+93655184609273x^2+778070418889x^3$
431	$y^2+xy=x^3-1$	1	10	-31	$-9-9x-7x^2+x^3$
				-39	$1+x-x^2-x^3+x^4$
431	$y^2+xy+y=x^3-x^2-9x-8$	0	40	-31	$744+76x-324x^2+81x^3$
				-39	$2061+2628x+918x^2+123x^3+49x^4$

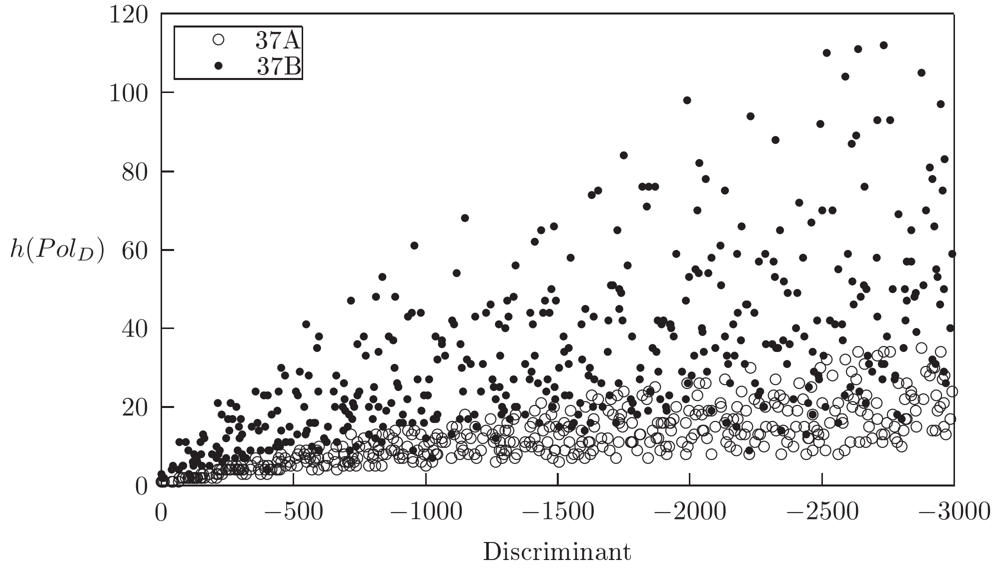

FIG. 1 – Comportement des points de Heegner sur les courbes $37A$ et $37B$

La table est trop petite pour pouvoir représenter tout l'éventail des comportements rencontrés (on pourra se reporter à l'annexe 6.1 pour des tables plus complètes, reprenant notamment toutes les courbes de conducteur premier plus petit que 100, et tous les discriminants associés plus petits que 100). En particulier, la proposition 2.23 pourrait faire espérer une corrélation claire entre le degré de la paramétrisation et la hauteur des points, mais cela n'a pas l'air d'être le cas, comme en témoigne l'exemple des deux courbes de conducteur 37.

Par la suite, je ferai référence aux courbes par le nom qui leur est donné dans les tables de Cremona [Cre]. Par exemple, $37A$ désigne la *strong Weil curve* de la première classe d'isogénies de courbes de conducteur 37. On emploiera les notations suivantes concernant les hauteurs :

- $\hat{h}_K(P_D)$ est la hauteur de Néron-Tate du point de Heegner associé au discriminant D, prise sur le corps K.
- $\hat{h}_K(Tr_D)$ est la hauteur de Néron-Tate de la trace (sur $\mathbb{Q}(\sqrt{D})$) des points de Heegner associés au discriminant D, prise sur le corps K.
- $h(Pol_D)$ désignera la hauteur logarithmique du polynome minimal des abscisses des points de Heegner de discriminant D, comme définie dans la section 2.3. Elle est toujours prise sur $\mathbb{Q}(\sqrt{D})$.

Finalement, $h(D)$ désigne le nombre de classe du corps $\mathbb{Q}(\sqrt{D})$. On le notera simplement h lorsque le discriminant est sous-entendu.

Pour une courbe fixée, la hauteur du polynôme varie de facon très irrégulière avec le discriminant, comme en témoigne la figure 1 concernant les courbes $37A$ et $37B$. Cette irrégularité rend l'étude expérimentale de ces hauteurs difficile. En particulier, on voudrait une estimation de la vitesse de croissance de ces hauteurs avec le discriminant.

5.2 Les traces

On s'intéresse à présent aux hauteurs des traces des points de Heegner sur une courbe elliptique donnée. Étant données les irrégularités constatées dans la partie précédente, il est plus facile d'étudier ces hauteurs en moyenne. Nous allons d'abord adapter un théorème de H. Iwaniec qui nous permettra de donner une formule asymptotique pour la hauteur en moyenne des traces, valable dans le cas où la courbe elliptique est de rang 0. Puis, nous adapterons cette formule au cas d'une courbe de rang 0, et obtiendrons une faible mais surprenante différence dans les vitesses de croissance.

5.2.1 Courbes de rang 0

On ne considère ici que des courbes de rang 0. Nous commençons par citer le théorème suivant de H. Iwaniec [Iw] :

Théorème 5.1. *Soit E une courbe elliptique de conducteur N, et $L(E,s)=\sum a_n n^{-s}$ sa série L. Soit*

$$\mathcal{D}=\{d \text{ sans facteur carré, } 0<d\equiv -\nu^2 \mod 4N, \text{ pour un } \nu \text{ premier à } 4N\}.$$

Pour tout $d\in D$, on note $\chi_d=\left(\frac{-d}{\cdot}\right)$ le symbole de kronecker, et $L(E,\chi_d,s)=\sum a_n\chi_d(n)n^{-s}$ la série L tordue. Alors

$$\sum_{d\in\mathcal{D}} L'(E,\chi_d,1)F(d/Y)=\alpha Y\log Y+O(Y),$$

où F est une fonction continue à support compact. α est une constante explicite définie comme la valeur en 1 d'une certaine série L.

Posons $\gamma(4N)=\#\{d \mod 4N : d\equiv -\nu^2 \mod 4N, (\nu,4N)=1\}$, et

$$c_N=\frac{3\gamma(4N)}{\pi^2 N}\prod_{p|4N}\left(1-\frac{1}{p^2}\right)^{-1}.$$

Pour tout $n\in\mathbb{N}$, soit

$$b_n=a_n\prod_{p|n,p\nmid 4N}\left(1+\frac{1}{p}\right)^{-1}\prod_{p|\gcd(n,2)}\left(1-\frac{1}{p}\right).$$

Alors, on définit une série de Dirichlet par

$$L(s)=\sum_{n=kl^2} b_n n^{-s},$$

où la sommation se fait sur tous les entiers $n=kl^2$ avec $p|k \implies p|N$ et $\gcd(l,N)=1$. On a alors :

$$\alpha=c_N L(1)\int F(t)dt^1$$

On peut réécrire cette série L de la façon suivante :

[1]Il semblerait que quelques petites erreurs se soient glissées dans la démonstration de H. Iwaniec. La formule donnée ici est la formule corrigée.

$$L(s)=\prod_{p|N}\left(1-\frac{a_p}{p^s}\right)^{-1}\prod_{p\nmid N}\left(1+\left(1+\frac{1}{p}\right)^{-1}\left(\sum_{i=1}^{\infty}\frac{a_{p^{2i}}}{p^{2is}}\right)\right)\prod_{p|\,\gcd(2,N-1)}\left(1+\left(1-\frac{1}{p}\right)\left(\sum_{i=1}^{\infty}\frac{a_{p^{2i}}}{p^{2is}}\right)\right)$$
$$=\frac{L(2s,sym^2E)}{\zeta(4s-2)\prod_{p|N}(1-p^{2-4s})}\prod_{p|N}\left(1-\frac{a_p}{p^s}\right)^{-1}\left(1-\frac{a_{p^2}}{p^2}\right)\mathcal{P}(s).$$

$\mathcal{P}(s)$ est un produit Eulerien qui converge dès que $s>3/4$, il est défini par :

$$\mathcal{P}(s)=\prod_{p\nmid N}\left(\frac{1}{1+1/p}+\left(\frac{1}{1+p}\right)\left(\frac{1+p^{2-4s}-(a_p^2-2p)p^{-2s}}{1+p^{1-2s}}\right)\right)$$
$$\prod_{p|\,\gcd(2,N-1)}\left(1-\frac{1}{p}+\frac{1}{p}\cdot\frac{1+p^{2-4s}-(a_p^2-2p)p^{-2s}}{1+p^{1-2s}}\right).$$

La formule de Gross-Zagier permet de relier la hauteur des traces des points de Heegner aux séries L tordues dont on vient de donner une estimation asymptotique :

$$L(1,E/\mathbb{Q})L'(1,E/\mathbb{Q},\chi_d)=\frac{4\Omega}{\sqrt{d}}\cdot\hat{h}_K(Tr_d),$$

En effet, on a le

Lemme 5.2. *Soit d un discriminant fondamental et $K=\mathbb{Q}(\sqrt{d})$. En reprenant les notations de la section 3.3, on a :*

$$L(E/K,s)=L(E/\mathbb{Q},s)L(E/\mathbb{Q},\chi_d,s)=L_K(E,\mathbf{1},s).$$

Démonstration. On commence par montrer la première égalité. Soit p un premier rationnel. Alors on a les trois cas suivants :

$$\chi_d(p)=\begin{cases}1 & \text{si } p\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2 \text{ (p est complètement déployé)}\\ -1 & \text{si } p\mathcal{O}_K=\mathfrak{p} \text{ (p reste premier)}\\ 0 & \text{si } p\mathcal{O}_K=\mathfrak{p}^2 \text{ (p ramifie)}\end{cases}$$

Pour tout premier $\mathfrak{p}$ de K et tout entier positif n, on note $K_\mathfrak{p}=K/\mathfrak{p}$. On définit $q_\mathfrak{p}=\#K_\mathfrak{p}$, et $a_\mathfrak{p}=q_\mathfrak{p}+1-\#E(K_\mathfrak{p})$. Soient α,β tels que $a_p=\alpha_p+\beta_p$, $|\alpha_p|=|\beta_p|=\sqrt{p}$. Alors, d'après les conjectures de Weil pour la courbe elliptique E, on a : $\#E(\mathbb{F}_{p^2})=\alpha_p^2+\beta_p^2=a_p^2-2p$. D'où :

$$\begin{aligned}L(E/K,s)&=\prod_{\mathfrak{p}}\left(1-a_\mathfrak{p}q_\mathfrak{p}^{-s}+q_\mathfrak{p}^{1-s}\right)^{-1}\\&=\prod_{\chi_d(p)=1}\left(1-a_pq_p^{-s}+q_p^{1-2s}\right)^{-2}\prod_{\chi_d(p)=-1}\left(1-(a_p^2-2p)p^{-2s}+p^{2-4s}\right)^{-1}\prod_{\chi_d(p)=0}\left(1-a_pp^{-s}+p^{1-2s}\right)^{-1}\\&=\prod_p\left(1-\chi_d(p)a_pp^{-s}+\chi_d(p)^2p^{1-2s}\right)^{-1}\prod_p\left(1-a_pp^{-s}+p^{1-2s}\right)^{-1}\\&=L(E/\mathbb{Q},s)L(E/\mathbb{Q},\chi_d,s).\end{aligned}$$

Les égalités ci-dessus ne sont vraies que pour les premiers de bonne réduction. Cependant, les premiers qui divisent le conducteur ne posent pas de problème particulier.

Pour montrer la deuxième égalité, comme il s'agit d'une égalité entre deux séries de Dirichlet dont les coefficients sont des fonctions multiplicatives, il suffit de montrer que pour tout nombre premier p et tout entier naturel a,

$$\sum_{i=0}^{a} a_{p^i}\chi_d(p^i)a_{p^{a-i}} = \sum_{i=0}^{\lfloor a/2\rfloor} a_{p^i}r(p^i)\chi_d(p^{a-2i})$$

($r(p^i)$ est le nombre d'idéaux de $\mathcal{O}_K$ de norme p^i). $r(p^i)$ s'exprime simplement en fonction de $\chi_d(p)$, en effet :

$$r(p^i) = \begin{cases} i+1 & \text{si } \chi_d(p) = 1 \\ 1+(-1)^i & \text{si } \chi_d(p) = -1 \\ 1 & \text{si } \chi_d(p) = 0. \end{cases}$$

L'égalite ci-dessus peut alors se montrer par récurrence, en utilisant les relations

$$\begin{cases} a_{p^i} = a_p^i & \text{si } p|N \\ a_p a_{p^i} = a_{p^{i+1}} + p^{2i-1}a_{p^{i-1}} & \text{si } p \nmid N \end{cases}$$

Le lemme est donc vrai pour les s tels que les séries convergent absolument, donc pour tout s puisqu'il s'agit de séries de Dirichlet. □

On obtient ainsi une estimation asymptotique en moyenne pour la somme des hauteurs des traces divisées par $\sqrt{d}$, pour $d \in \mathcal{D}$. En prenant pour F la fonction qui vaut $\sqrt{t}$ sur $[0,1]$ et 0 en-dehors de cet intervalle[2], on obtient le corollaire suivant :

Corollaire 5.3. *Soit E une courbe elliptique de rang 0 et de conducteur N. Alors, avec les notations définies ci-dessus,*

$$\sum_{d\in\mathcal{D},\ d\leq Y} \hat{h}_K(Tr_d) = \frac{2}{3}c_N \cdot \mathcal{P}(1) \cdot \frac{L(1,E)\cdot L(2, sym^2 E)}{2\Omega} \cdot L_E \cdot Y^{3/2}\log Y + O(Y^{3/2}),$$

où L_E est un produit de facteurs locaux, correspondant aux facteurs Euleriens de la série L, et de son carré symétrique, pour les nombres premiers qui divisent le conducteur :

$$L_E = \frac{1}{\zeta(2)}\prod_{p|N}\left(1-\frac{a_p}{p}\right)^{-1}\left(1-\frac{1}{p^2}\right)^{-1}\left(1-\frac{a_{p^2}}{p^2}\right).$$

Le tableau ci-dessous donne quelques exemples de valeurs de α (ici, α est le coefficient en $Y^{3/2}\log Y$ du corollaire 5.3) et des différents termes qui entrent en jeu. On a choisi de calculer $\alpha/\gamma(4N)$ plutôt que α pour pouvoir comparer les courbes entre elles, le facteur $\gamma(4N)$ supprimant la difference artificielle dûe au fait que le nombre de discriminants satisfaisant l'hypothese de Heegner varie beaucoup d'un conducteur à l'autre.

[2]L'énoncé du théorème parle de fonction continue, mais c'est par commodité et continue par morceaux bornée convient parfaitement.

Courbe	c_N	$\mathcal{P}(1)$	$L(2, sym^2E)$	L_E	$L(1)$	$deg(\Phi_N)$	$10^4\dfrac{\alpha}{\gamma(4N)}$
$11-1$	0.185	1.01	0.571	0.668	0.253	1	6.10
$14-1$	0.0886	1.04	0.448	0.472	0.330	1	3.59
$15-1$	0.0633	1.19	0.418	0.570	0.350	1	5.27
$17-1$	0.191	1.27	0.369	0.646	0.386	1	4.68
$19-1$	0.192	1.25	0.330	0.641	0.453	1	4.30
$21-1$	0.0665	1.18	0.299	0.798	0.451	1	4.71
$26-1$	0.0941	1.05	0.483	0.439	0.515	2	3.01
$26-2$	0.0941	0.941	0.483	1.12	0.621	2	8.33
$30-1$	0.0316	0.993	0.418	0.506	0.558	2	3.10
$33-1$	0.0696	1.16	0.571	0.501	0.747	3	5.79
$34-1$	0.0957	1.00	0.369	1.14	0.749	2	6.39
$35-1$	0.0738	1.32	0.359	0.591	0.703	2	4.06
$37-2$	0.197	1.39	0.339	0.624	0.725	2	3.91
$38-1$	0.0962	1.09	0.992	0.427	0.630	6	5.23
$38-2$	0.0962	1.01	0.330	1.15	0.819	2	5.66
$39-1$	0.0705	1.16	0.322	0.494	0.826	2	2.99
$42-1$	0.0332	1.00	0.598	0.798	0.869	4	7.68
$46-1$	0.0971	1.02	0.683	0.423	0.661	5	2.87
$51-1$	0.0717	1.21	0.246	0.861	0.860	2	3.31
$55-1$	0.0774	1.28	0.228	0.696	1.02	2	2.71
$57-2$	0.0722	1.19	0.330	0.866	1.08	3	4.97
$57-3$	0.0722	0.935	1.32	0.866	0.586	12	8.40

Remarque. *Les données théoriques collent raisonnablement bien à l'expérience. On a fait le calcul des hauteurs des traces pour $Y = 10^4$ et les courbes ci-dessus, et le rapport entre la valeur théorique et la valeur pratique est toujours compris entre 1 et 1.15. Il n'est pas surprenant que la convergence soit si lente, car le terme suivant dans l'estimation asymptotique de H. Iwaniec est en Y, à comparer au terme dominant qui est en $Y \log Y$. De plus, les traces se comportent de manière très irrégulière. Il est possible d'avoir de meilleurs resultats en ne sommant qu'une classe de congruence modulo $8N$, comme le fait R. Murty dans [Mur].*

Le produit Eulerien $\mathcal{P}(s)$ varie peu, en effet si l'on effectue un développement limité du facteur en p de $\mathcal{P}(1)$, on obtient

$$\mathcal{P}_p(1) = 1 - \frac{a_p^2 - 2p}{p^3} + O\left(\frac{1}{p^2}\right),$$

d'où l'existence d'une constante absolue C (ne dépendant pas de la courbe E considérée) telle que

$$C\prod_{p=1}^{\infty}\left(1-\frac{2}{p^2}\right) < \mathcal{P}(1) < C\prod_{p=1}^{\infty}\left(1+\frac{2}{p^2}.\right)$$

Finalement, les termes importants sont le degré de la paramétrisation modulaire, la valeur de la série L de la courbe en 1, ainsi que le conducteur, qui intervient en $1/N^2$.

À conducteur et degré fixé, les petits nombres premiers qui divisent le conducteur ont un rôle décisif, et les hauteurs des traces auront alors tendance à être plus ou moins grandes suivant que E a une réduction *split multiplicative* ou *non-split multiplicative* à ces nombres premiers, ce qui est surprenant. Cette influence se voit très bien dans le cas des deux courbes de conducteur 26, qui ont même degré 2 alors que les traces sont presque trois fois plus grosses sur la $26B$ que sur la $26A$. Ceci s'explique (analytiquement !) par le fait que 26 est divisible par 2, et que la $26A$ a réduction *split multiplicative* en 2 alors que la $26B$ a réduction *non-split multiplicative*. Ceci induit un facteur 3 entre les produits pour les p divisant le conducteur des facteurs Euleriens de la série L en p de ces deux courbes. La figure 2 illustre cette différence de comportement. On voit également que, dans ce cas, la courbe représentant la somme des hauteurs des traces est très proche de la courbe théorique, même si elle est relativement irrégulière.

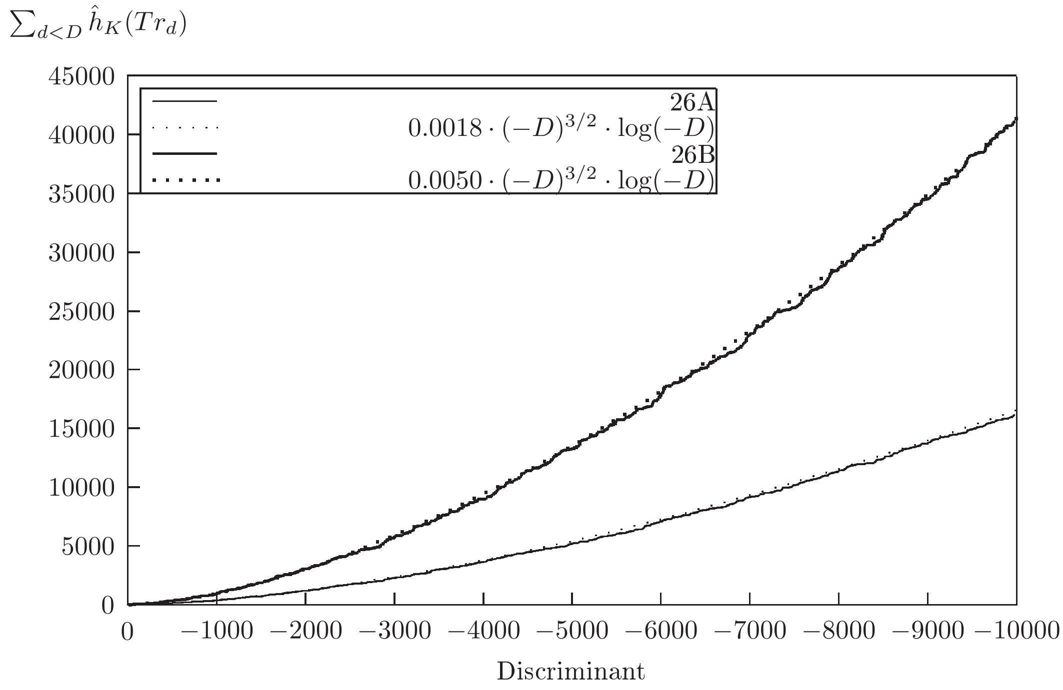

FIG. 2 – Hauteur des traces en moyenne sur les courbes $26A$ et $26B$: pratiques et théoriques.

5.2.2 Le cas du rang 1

La démonstration d'H. Iwaniec dans [Iw] concerne les dérivées des séries L tordues. Dans le cas d'une courbe elliptique de rang 1, on sait que $L(E/\mathbb{Q}, 1) = 0$ (théorème 2.17), et donc d'après le lemme 5.2, nous voulons une formule pour les séries L tordues elles-même.

Il n'est pas difficile d'adapter la démonstration à ce cas. Dans son article, Iwaniec exprime la dérivé de la série L comme une série convergeant exponentiellement vite, ce qui lui permet de faire des majorations astucieuses ; cette série est du même type que celle que l'on présente dans la section 4.2. Dans notre cas, il suffit de remplacer la fonction $V(X)$ définie au paragraphe 4, p.369, par la fonction

$$V'(X) = e^{-X}.$$

On a alors, en gardant les notations de l'article,

$$\mathcal{A}(X, \chi_d) = \frac{1}{2i\pi} \int_{(3/4)} L(s+1, E, \chi_d)\Gamma(s) \left(\frac{X}{2\pi}\right)^s ds^3.$$

La majoration $\mathcal{A}(X, \chi_d) \ll \sqrt{X}$, qui découle de l'inégalité de Hölder et d'une estimation des a_n tient toujours, et ainsi les majorations successives effectuées dans la démonstration ne posent pas de problème.

La seule différence notable vient à la page 374, lors du calcul de $\mathcal{B}(X)$. On a alors :

$$res_{s=0} L(s+1)\Gamma(s) \left(\frac{X}{2\pi}\right)^s = L(1),$$

[3] À noter une erreur dans l'article, il s'agit bien de $\left(\frac{X}{2\pi}\right)^s$ et non $\left(\frac{2\pi}{X}\right)^s$

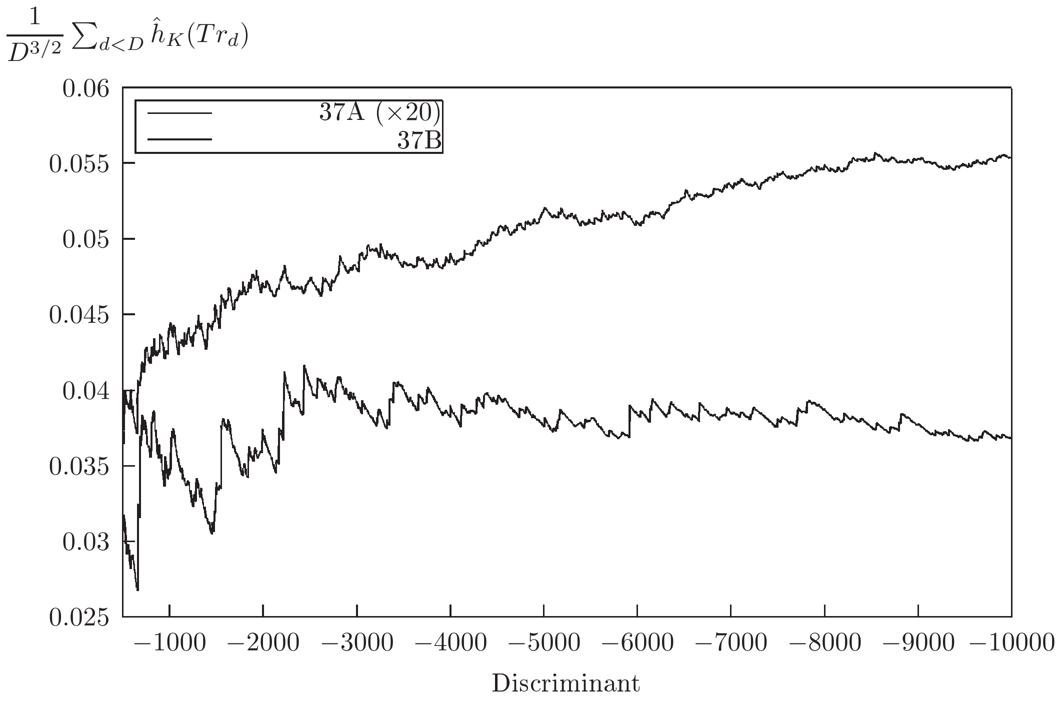

FIG. 3 – Hauteur des traces en moyenne sur les courbes $37A$ et $37B$.

et il n'apparaît pas de terme en $\log X$.

On obtient ainsi une formule similaire à celle donnée dans le corollaire 5.3 :

Proposition 5.4. *Soit E une courbe elliptique de rang 1 et de conducteur N. Alors, avec les notations définies dans la section précédente,*

$$\sum_{d\in\mathcal{D},\ d\le Y} \hat{h}_K(Tr_d) = \frac{2}{3}c_N \cdot \mathcal{P}(1) \cdot \frac{L'(1,E)\cdot L(2, sym^2 E)}{4\Omega} \cdot L_E \cdot Y^{3/2} + O(Y^{41/28}).$$

La table suivante donne quelques exemples de valeurs numériques du coefficient α de cette formule :

Courbe	c_N	$\mathcal{P}(1)$	$L(2, sym^2E)$	L_E	$L(1)$	$deg(\Phi_N)$	$10^4 \frac{\alpha}{\gamma(4N)}$
$37-1$	0.197	0.846	0.339	0.592	0.306	2	0.951
$43-1$	0.198	0.886	0.292	0.594	0.343	2	0.830
$53-1$	0.198	1.07	0.237	0.596	0.435	2	0.842
$57-1$	0.0722	0.881	0.441	0.433	0.417	4	0.940
$58-1$	0.0979	0.894	0.433	0.391	0.463	4	0.821
$61-1$	0.199	1.15	0.412	0.598	0.485	4	1.53
$65-1$	0.0784	1.15	0.386	0.470	0.505	4	1.15
$77-1$	0.0812	1.15	0.326	0.487	0.627	4	1.03
$79-1$	0.200	1.24	0.636	0.600	0.581	8	2.35

[explication algébrique ?]

La figure 3 illustre les différences de croissance des hauteurs des traces sur les courbes $37A$ (rang 1) et $37B$ (rang 0). On remarque que le comportement est très irrégulier ; ceci est en partie

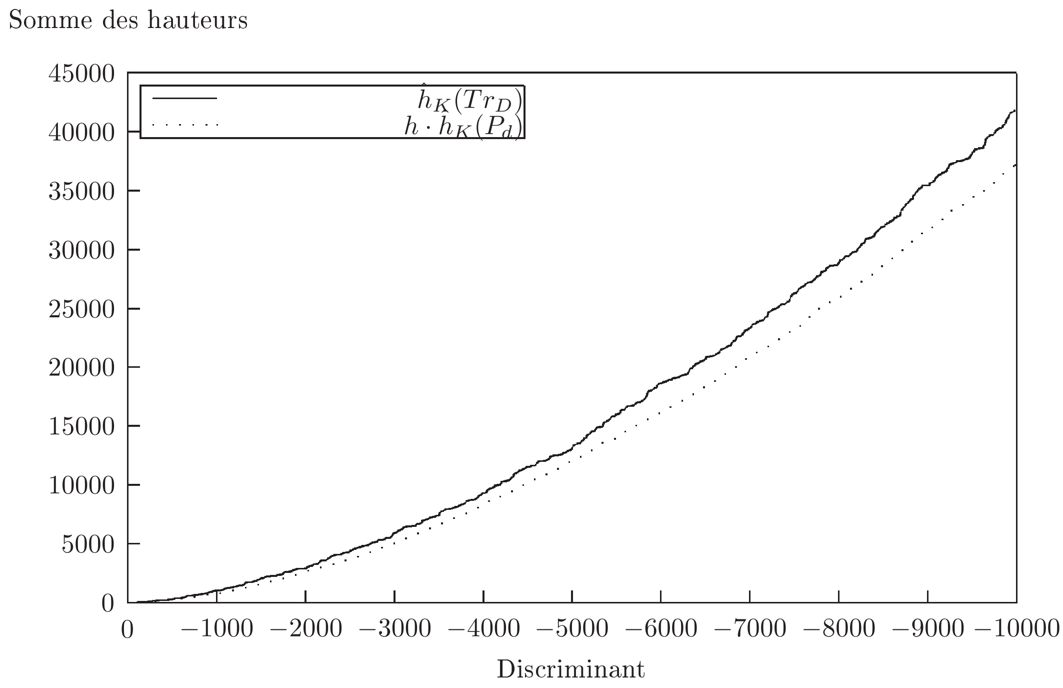

FIG. 4 – Somme des hauteur des traces et des points sur la courbe $34A$.

dû à la division par $D^{3/2}$ qui rend les irrégularités plus apparentes que dans la figure 2. De plus, pour la courbe $37A$ de rang 1, il arrive fréquemment que la trace soit nulle, ce qui “casse la moyenne”. Il est conjecturé que la proportion de tordues de rang supérieur ou égal à 2 (ce qui correspond aux cas de trace nulle selon la formule de Gross-Zagier et la conjecture de Birch et Swinnerton-Dyer) tend vers 0 lorsque le discriminant tend vers l'infini, mais cela ne se voit pas dans l'échelle de discriminants étudiée.

5.3 Hauteur des points de Heegner

Dans une première partie nous allons présenter les résultats expérimentaux obtenus ; ils montrent une corrélation entre le comportement des hauteurs des traces et celles des points. Dans une seconde partie, nous essaierons de donner des arguments heuristiques pour appuyer nos observations.

5.3.1 Données numériques

Les figures 9 et 10 illustrent le comportement en moyenne des hauteurs de Néron-Tate des points de Heegner sur les courbes elliptiques $34A$ et $37B$. Il a paru plus judicieux de multiplier la hauteur associée à un discriminant d par le nombre de classe de $\mathbb{Q}(\sqrt{d})$, de sorte à pouvoir comparer les hauteurs des points et celle des traces selon la correspondance détaillée dans la section 3.3.

La première remarque que l'on peut faire concerne la croissance de la courbe : on a l'impression que les deux sommes ont la même croissance, en $D^{3/2} \log D$ d'après la section précédente. Nous verrons en 5.3.2 qu'il y a de bonnes raisons pour que cela soit effectivement le cas.

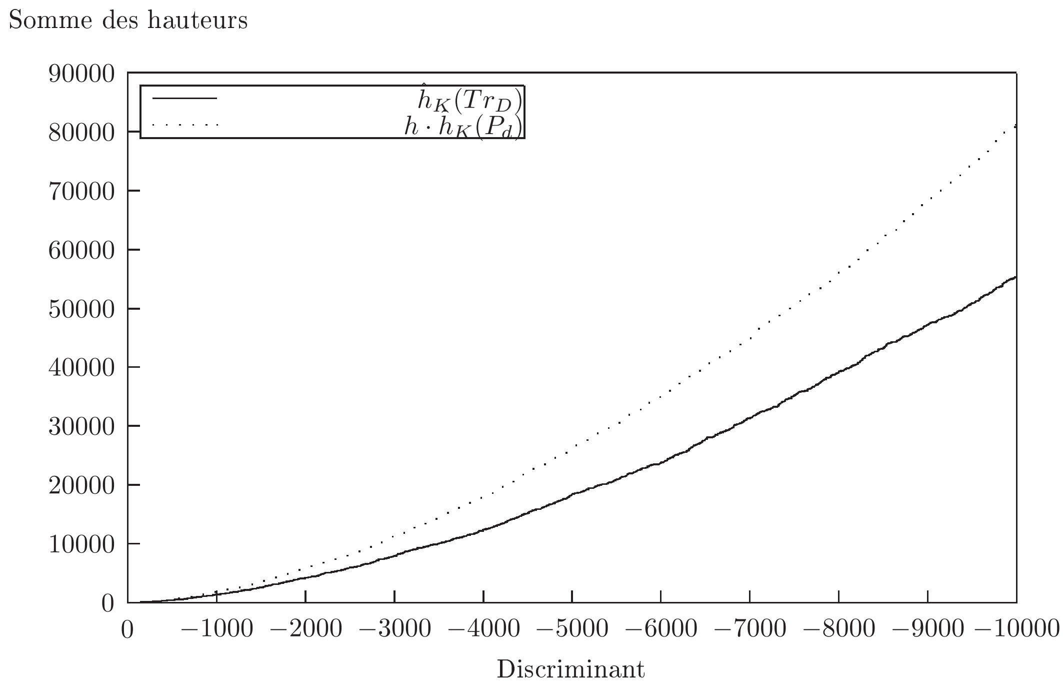

FIG. 5 – Somme des hauteur des traces et des points sur la courbe $37B$.

Par contre, il est assez net que dans le cas de la courbe $37A$ (figure 6), la croissance de la somme des hauteurs des points (multipliées par le nombre de classe, toujours) est plus rapide que celle des traces. Ainsi, on aurait une croissance en $D^{3/2} \log D$ pour les hauteurs des points dans tous les cas, alors que, comme on l'a vu, la vitesse de croissance des traces dépend du rang (ici, les courbes $34A$ et $37B$ sont de rang 0, alors que la $37A$ est de rang 1). Algébriquement, ceci signifierait qu'il y a une plus grande cancellation lorsque l'on prend la trace d'un point de Heegner sur une courbe de rang 1 que sur une courbe de rang 0.

On s'intéresse à présent au positionnement des deux courbes l'une par rapport à l'autre sur chacune des trois figures. En fait, la courbe $34A$ est la première pour laquelle la courbe représentant les traces est au-dessus de celle représentant les points (cette question n'a bien sûr d'intêret que pour les courbes de rang 0, selon les remarques précédentes).

Le tableau suivant donne la valeur numérique du rapport

$$\frac{\sum_{d\in\mathcal{D},\ d\leq Y} \hat{h}_K(Tr_d)}{\sum_{d\in\mathcal{D},\ d\leq Y} h \cdot \hat{h}_K(P_d)}$$

pour $Y = 6000, 12000$ et 18000, pour toutes les courbes de rang 0 de conducteur plus petit que 90 et sans facteur carré. La dernière colonne donne la valeur du produit de la série L de la courbe elliptique en 1 par les facteurs Euleriens de cette série pour les premiers qui divisent le conducteur. Le facteur 0.8 est là pour rendre la comparaison entre les deux dernières colonnes plus aisée.

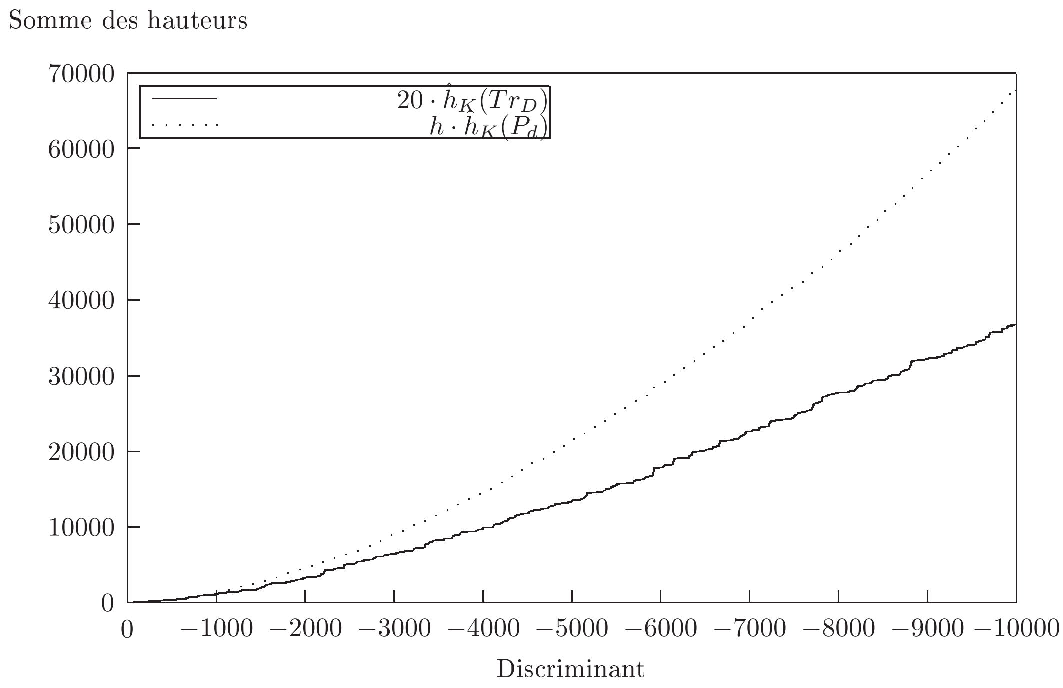

FIG. 6 – Somme des hauteur des traces et des points sur la courbe $37A$.

Courbe	6000	12000	18000	$0.8 \cdot L(1)L_N(1)$	Courbe	6000	12000	18000	$0.8 \cdot L(1)L_N(1)$
$11-1$	0.280	0.271	0.268	0.223	$51-1$	0.938	0.930	0.927	0.974
$14-1$	0.233	0.227	0.219	0.205	$55-1$	1.04	1.00	1.00	0.942
$15-1$	0.287	0.282	0.279	0.262	$57-2$	1.24	1.24	1.20	1.23
$17-1$	0.394	0.386	0.379	0.328	$57-3$	0.636	0.650	0.653	0.668
$19-1$	0.432	0.425	0.413	0.382	$58-2$	1.56	1.58	1.57	1.59
$21-1$	0.522	0.494	0.486	0.473	$62-1$	1.75	1.73	1.70	1.71
$26-1$	0.332	0.321	0.326	0.297	$66-1$	0.536	0.555	0.547	0.584
$26-2$	0.873	0.871	0.852	0.922	$66-2$	1.13	1.12	1.08	1.21
$30-1$	0.367	0.366	0.360	0.372	$66-3$	2.38	2.37	2.36	3.14
$33-1$	0.534	0.520	0.512	0.493	$67-1$	1.13	1.10	1.06	1.03
$34-1$	1.14	1.12	1.10	1.13	$69-1$	1.37	1.32	1.33	1.38
$35-1$	0.616	0.594	0.586	0.546	$70-1$	1.44	1.35	1.37	1.37
$37-2$	0.678	0.675	0.670	0.596	$73-1$	1.05	1.04	1.03	0.959
$38-1$	0.403	0.389	0.393	0.354	$77-2$	0.923	0.922	0.897	0.883
$38-2$	1.21	1.22	1.21	1.24	$77-3$	1.04	1.05	1.02	1.02
$39-1$	0.547	0.566	0.557	0.537	$78-1$	0.323	0.306	0.300	0.314
$42-1$	0.879	0.878	0.864	0.912	$85-1$	0.999	0.977	0.996	0.990
$46-1$	0.404	0.387	0.380	0.368	$89-2$	1.18	1.17	1.14	1.15

Remarque. *On a représenté les valeurs numériques pour plusieurs valeurs de Y. En effet, idéalement ces valeurs ne devraient pas dépendre de Y, comme on l'a souligné plus haut. Mais en pratique, on observe une décroissance de l'ordre d'une petite puissance de $\log Y$, au plus $\sqrt{\log Y}$. On pense que cela est un artefact, mais on l'a mis en évidence pour souligner la relativement faible précision des données présentées : il se pourrait que la corrélation que l'on observe entre les deux dernîres colonnes (et en particulier le facteur 0.8) ne soit dûe qu'à la valeur $Y = 10^4$ choisie.*

On observe une corrélation très claire entre les deux dernières colonnes, qui est renforcée par le fait que les valeurs numériques données varient du simple au quintuple, alors que l'écart constaté entre les deux dernières colonnes ne dépasse pas les 10% (à l'exception de la courbe $66-3$, qui vient confirmer la règle...cf la remarque ci-dessus).

Le but de la section suivante est de donner une heuristique permettant d'expliquer l'apparition de ce facteur $L(1)L_N(1)$.

5.3.2 Un théorème sur la hauteur en moyenne des points

Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N, et $L(E/\mathbb{Q},s)=\sum a_n n^{-s}$ sa série L. Pour tout discriminant $d\in\mathcal{D}$ (cf la section 5.2.1), on considère la série

$$L(E,s,d)=\sum_{n\in\mathbb{N}}\frac{a_n r_d(n)}{n^s}\sum_{(m,N)=1}\left(\frac{d}{m}\right)\frac{1}{m^{2s-1}},$$

(c'est la série $L_1(E,s)$ de la section 3.3). On s'intéresse alors au comportement asymptotique de la somme

$$S\ =\sum_{d\in\mathcal{D},\ d\leq Y}L'(E,1,d)$$

lorsque Y tend vers l'infini. La démarche exposée en 4.2 nous permet de réécrire $L'(E,s,d)$ comme une série convergeant exponentiellement vite. Soit

$$V(X)=\frac{1}{2i\pi}\int_{(3/4)}\Gamma(s)^2X^{-s}ds,$$

et

$$\mathcal{A}(X,d)=\sum_{n=1}^{\infty}\frac{a_n r_d(n)}{n}\sum_{(m,N)=1}\left(\frac{d}{m}\right)\frac{1}{m}V\left(\frac{4\pi^2nm^2}{X}\right).$$

Alors,

$$\mathcal{A}(X,d)=\frac{1}{2i\pi}\int_{(3/4)}L(E,s+1,d)\Gamma(s)^2\left(\frac{X}{4\pi^2}\right)^s ds.$$

On déplace la ligne d'intégration en $Re(s)=-3/4$, laissant un résidu égal à $L'(E,1,d)$ en $s=0$, puis on revient en $s=3/4$ grâce à l'équation fonctionnelle satisfaite par $L(E,1,s)$ (cf 4.2). On obtient ainsi

$$L'(E,1,d)=\mathcal{A}(X,d)+\mathcal{A}\left(\frac{N^2d^2}{X},d\right),$$

et en particulier

$$L'(E,1,d)=2\mathcal{A}(dN,d).$$

Nous majorons $V(X)$, pour $X>0$, de la manière suivante :

$$V(X)=\frac{1}{2i\pi}\int_{u=0}^{\infty}\frac{e^{-u}}{u}\int_{v=0}^{\infty}e^{-v}\left(\int_{(3/4)}\left(\frac{uv}{X}\right)^s\frac{1}{s}ds\right)dvdu\ll\int_0^{\infty}\frac{e^{-(u+X/u)}}{u}du$$
$$\ll X^{-1/4}e^{-2\sqrt{X}}.$$

Comme $d\in\mathcal{D}$, d est un carré modulo 4 et d est premier à 4, donc $d\equiv 1 \mod 4$. Ainsi,

$$r_d(n)=\#\{(u,v)\in\mathbb{N}^*\times\mathbb{Z}\cup\{0\}\times\mathbb{N},\ u^2+dv^2=4n\}.$$

On observe que, si n est un carré, alors pour tout d on a $r_d(n) \geq 1$, et donc

$$\sum_{d\in\mathcal{D},\ d\leq Y} r_d(n) \geq \#\{d \in \mathcal{D},\ d \leq Y\} \ \sim_{+\infty} C \cdot Y.$$

Si n n'est pas un carré, alors $u \leq \sqrt{n}$ et à chaque u correspond au plus un couple (d, v) (car d est supposé sans facteur carré), d'où $\sum_{d\in\mathcal{D},\ d\leq Y} r_d(n) \leq 2\sqrt{n}$.

On écrit ainsi $S = S_0 + S_1$, où

$$S_0 = \sum_{n\in\mathbb{N}} \frac{a_{n^2}}{n^2} \sum_{(m,N)=1} \frac{1}{m} \sum_{d\in\mathcal{D},\ d\leq Y} \left(\frac{d}{m}\right) V\left(\frac{4\pi^2 n^2 m^2}{Nd}\right),$$

et

$$S_1 = \sum_{d\in\mathcal{D},\ d\leq Y} \sum_{n\in\mathbb{N}} \frac{a_n r'_d(n)}{n} \sum_{(m,N)=1} \frac{1}{m} \left(\frac{d}{m}\right) V\left(\frac{4\pi^2 n m^2}{Nd}\right),$$

où $r'_d(n) = \#\{(u,v) \in \mathbb{N} \times \mathbb{Z}^*,\ u^2 + dv^2 = 4n\}$.

On peut calculer la somme

$$S' = \sum_{(m,N)=1} \frac{1}{m} \sum_{d\in\mathcal{D},\ d\leq Y} \left(\frac{d}{m}\right) V\left(\frac{4\pi^2 n^2 m^2}{Nd}\right),$$

où n est considéré comme un paramètre, exactement comme dans l'article [Iw]. En effet,

$$\sum_{(m,N)=1} \frac{1}{m} V\left(\frac{4\pi^2 n^2 m^2}{X}\right) \ll X^{1/4} \sum_{m\in\mathbb{N}} \frac{1}{m^{3/2}} e^{-\frac{2\pi n}{\sqrt{X}} m} \ll X^{1/4},$$

ce qui est une meilleure majoration que dans l'article, et le reste suit. On obtient ainsi :

$$S' = c_N Y \int F(t)\mathcal{B}_n(tNY)dt + O(Y),$$

où le $O(Y)$ ne dépend pas de n, et

$$\mathcal{B}_n(X) = \sum_{p|l \implies p|N} \frac{b_{l^2}}{l^2} V\left(\frac{4\pi^2 n^2 l^4}{X}\right),$$

avec

$$b_l = \prod_{p|l} \left(1 + \frac{1}{p}\right)^{-1} \prod_{p|(l,2)} \left(1 - \frac{1}{p}\right).$$

On revient à S_0 en posant

$$\mathcal{B}(X) = \sum_{n=1}^{\infty} \frac{a_{n^2}}{n^2} \mathcal{B}_n(X),$$

d'où

$$S_0 = c_N Y \int F(t)\mathcal{B}(tNY)dt + O(Y),$$

et on conclut de la même manière que dans l'article :

$$S_0 = \beta_0 Y \log Y + O(Y),$$

avec

$$\beta_0 = c_N L(1) \int F(t)dt,$$

où

$$L(s) = \sum_{n=1}^{\infty} \frac{a_{n^2}}{n^{2s}} \sum_{(m,N)=1} \frac{b_m}{m^{2s-1}}.$$

En notant $\zeta_N(2)$ la fonction de Riemann à laquelle on a enlevé les facteurs Euleriens correspondant aux premiers divisant le conducteur, on a

$$\sum_{n\in\mathbb{N}} \frac{a_{n^2}}{n^2} = \frac{L(sym^2E,2)}{\zeta_N(2)}.$$

Ainsi,

$$\beta_0 = c_N \frac{L(sym^2E,2)}{\zeta_N(2)} \prod_{p\nmid 4N} \left(1 + \frac{1}{(1+1/p)(p^2-1)}\right) \prod_{p|(N-1,2)} \frac{7}{6}.$$

Nous donnons à présent une majoration de S_1. On utilisera le

Lemme 5.5. *Soit f une forme modulaire de poids 2 et (a_n) les coefficients de sa série L. Alors,*

$$\sum_{n=1}^{X} \frac{a_n^2}{n^2} = O(\log X).$$

Démonstration. On effectue une sommation par parties en utilisant la majoration $\sum_{n<N} |a_n|^2 \ll N^2$. □

On découpe S_1 suivant que n est inférieur ou supérieur à Y^2. Comme on l'a vu, pour tout n on a $\sum_{d\in\mathcal{D},\ d\leq Y} r_d(n) \leq 2\sqrt{n}$. D'où :

$$\begin{aligned}
&\Big|\sum_{n=1}^{Y^2} \frac{a_n}{n} \sum_{(m,N)=1} \frac{1}{m} \sum_{d\in\mathcal{D},\ d\leq Y} r_d(n) \left(\frac{d}{m}\right) V\left(\frac{2\pi n m^2}{dN}\right)\Big| \\
&\quad \leq Y^{1/4} \sum_{(m,N)=1} \frac{1}{m^{3/2}} \left(\sum_{n=1}^{Y^2} \frac{a_n^2}{n^2}\right)^{1/2} \left(\sum_{n=1}^{Y^2} \sqrt{n} e^{-2\pi\sqrt{n}/\sqrt{NY}}\right)^{1/2} \\
&\quad \ll Y^{1/4}\sqrt{\log Y} \left(\int_{t=1}^{Y^2} \sqrt{t} e^{-2\pi\sqrt{t/NY}} dt\right)^{1/2} \\
&\quad \ll Y\sqrt{\log Y}.
\end{aligned}$$

De la même manière,

$$\begin{aligned}
&\Big|\sum_{n=Y^2}^{\infty}\frac{a_n}{n}\sum_{(m,N)=1}\frac{1}{m}\sum_{d\in\mathcal{D},\ d\le Y} r_d(n)\left(\frac{d}{m}\right)V\left(\frac{2\pi n m^2}{dN}\right)\Big|\\
&\le Y^{1/4}\sum_{(m,N)=1}\frac{1}{m^{3/2}}\left(\sum_{n=Y^2}^{\infty}\frac{a_n^2}{n^{5/2}}\right)^{1/2}\left(\sum_{n=Y^2}^{\infty} n e^{-2\pi\sqrt{n}/\sqrt{NY}}\right)^{1/2}\\
&\ll Y^{1/4}\left(\int_{t=Y^2}^{\infty} t e^{-2\pi\sqrt{t/NY}}dt\right)^{1/2}\\
&\ll Y^{1/4}Y\left(\int_{u=\sqrt{Y}}^{\infty} u^3 e^{-u}du\right)^{1/2}\\
&\ll Y^{11/4}e^{-\sqrt{Y}}.
\end{aligned}$$

On a ainsi montré que

$$S_1 = O(Y\sqrt{\log Y})$$

lorsque Y tend vers l'infini. Appliquons finalement la formule de Gross-Zagier pour obtenir une estimation asymptotique de la hauteur en moyenne des points de Heegner, du même type que celle que l'on avait obtenue pour les traces :

Théorème 5.6. *Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N sans facteurs carrés. On a :*

$$\sum_{d\in\mathcal{D},\ d\le Y}\hat{h}_H(P_d) = \frac{2}{3}c_N\cdot\frac{L(2,sym^2E)}{2\Omega\zeta_N(2)}\mathcal{Q}(N)\cdot Y^{3/2}\log Y + O(Y^{3/2}\sqrt{\log Y}),$$

où

$$\mathcal{Q}(N) = \prod_{p\nmid 4N}\left(1+\frac{1}{(1+1/p)(p^2-1)}\right)\prod_{p\mid(N-1,2)}\frac{7}{6}.$$

Soit

$$\beta = \frac{2}{3}c_N\cdot\frac{L(2,sym^2E)}{2\Omega\zeta_N(2)}\mathcal{Q}(N).$$

En remplaçant c_N par son expression, et en utilisant la proposition 2.19 sur la série L du carré symétrique, on peut réécrire

$$\beta = \left(\frac{2}{\pi}\right)^3\frac{\gamma(4N)}{N^2}deg\ \phi\prod_{p\mid N}\left(1-\frac{1}{p^2}\right)^{-2}\mathcal{Q}(N).$$

Il est clair que $\mathcal{Q}(N)\ge 1$; d'autre part

$$\mathcal{Q}(N) < \frac{7}{6}\prod_{p}\left(1+\frac{1}{p^2}\right) < \frac{7}{6}\zeta(2).$$

Le produit Eulerien $\mathcal{Q}(N)$ est donc compris entre 1 et 2, et il joue un relativement faible rôle dans l'expression de β. On a ainsi

$$1\le\prod_{p\mid N}\left(1-\frac{1}{p^2}\right)^{-2}\mathcal{Q}(N)\le\frac{7}{6}\zeta(2)^3 < 5.2.$$

Le terme principal, du moins si l'on s'intéresse à des valeurs asymptotiques du conducteur ou du degré de la paramétrisation modulaire, est donc $\frac{\gamma(4N)}{N^2} deg\ \phi$. On peut donner le corollaire suivant, plus faible que le théorème mais peut-être plus expressif :

Corollaire 5.7. *Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N sans facteurs carrés. On a :*

$$\sum_{d \in \mathcal{D},\ d \leq Y} \hat{h}_H(P_d) = O\left(\frac{\gamma(4N)}{N^2} deg\ \phi \cdot Y^{3/2} \log Y\right).$$

Le tableau suivant donne quelques exemples de la valeur de β :

Courbe	c_N	$\frac{L(2, sym^2 E)}{2\Omega\zeta_N(2)}$	$\mathcal{Q}(N)$	deg	$\frac{10^4\beta}{\gamma(4N)}$
$11-1$	0.185	0.086	1.37	1	29.7
$14-1$	0.088	0.050	1.16	1	21.3
$15-1$	0.063	0.054	1.22	1	19.2
$17-1$	0.191	0.055	1.37	1	12.4
$19-1$	0.192	0.050	1.38	1	9.92
$21-1$	0.066	0.039	1.24	1	9.59
$26-1$	0.094	0.054	1.18	2	12.1
$26-2$	0.094	0.054	1.18	2	12.1
$30-1$	0.031	0.040	1.04	2	11.0
$33-1$	0.069	0.076	1.25	3	11.4
$34-1$	0.095	0.041	1.18	2	7.08
$35-1$	0.073	0.051	1.31	2	6.25
$37-1$	0.197	0.051	1.38	2	5.22
$37-2$	0.197	0.051	1.38	2	5.22

Courbe	c_N	$\frac{L(2, sym^2 E)}{2\Omega\zeta_N(2)}$	$\mathcal{Q}(N)$	deg	$\frac{10^4\beta}{\gamma(4N)}$
$38-1$	0.096	0.112	1.18	6	17.0
$38-2$	0.096	0.037	1.18	2	5.67
$39-1$	0.070	0.043	1.25	2	5.46
$42-1$	0.033	0.059	1.06	4	10.9
$43-1$	0.198	0.044	1.38	2	3.86
$46-1$	0.097	0.077	1.18	5	9.66
$51-1$	0.071	0.033	1.26	2	3.18
$53-1$	0.198	0.036	1.38	2	2.54
$55-1$	0.077	0.033	1.32	2	2.49
$57-1$	0.072	0.059	1.26	4	5.10
$57-2$	0.072	0.044	1.26	3	3.82
$57-3$	0.072	0.178	1.26	12	15.3
$58-1$	0.097	0.049	1.18	4	4.86
$58-2$	0.097	0.049	1.18	4	4.86

On remarque que, contrairement à la constante α intervenant lorsque l'on considère les traces, à conducteur fixé β ne dépend que du degré de la paramétrisation modulaire, puisque le produit $\mathcal{Q}(N)$ ne dépend que de N. Par contre, lorsque l'on varie le conducteur, il n'y a plus une dépendance directe sur le degré.

Comparons à présent les valeurs expérimentales de β à la valeur théorique donnée ci-dessus. Pour chaque courbe de conducteur sans facteur carré plus petit que 100, on a représenté le rapport entre la valeur expérimentale

$$\beta_{exp}(Y) = \frac{1}{Y^{3/2} \log Y} \sum_{d \in \mathcal{D},\ d \leq Y} \hat{h}_H(P_d),$$

pour quelques valeurs de Y, et la valeur théorique :

Courbe	6000	13000	20000
$11-1$	0.819	0.844	0.857
$14-1$	0.707	0.736	0.742
$15-1$	0.804	0.826	0.846
$17-1$	0.841	0.860	0.873
$19-1$	0.820	0.842	0.855
$21-1$	0.800	0.836	0.848
$26-1$	0.714	0.730	0.744
$26-2$	0.682	0.702	0.717
$30-1$	0.687	0.703	0.722
$33-1$	0.796	0.828	0.841
$34-1$	0.707	0.724	0.735
$35-1$	0.856	0.873	0.885
$37-1$	0.756	0.787	0.805
$37-2$	0.921	0.937	0.949
$38-1$	0.760	0.775	0.784
$38-2$	0.702	0.722	0.733
$39-1$	0.815	0.823	0.844

Courbe	6000	13000	20000
$42-1$	0.683	0.722	0.735
$43-1$	0.774	0.799	0.816
$46-1$	0.699	0.720	0.729
$51-1$	0.813	0.822	0.842
$53-1$	0.788	0.818	0.829
$55-1$	0.935	0.939	0.943
$57-1$	0.777	0.795	0.805
$57-2$	0.884	0.891	0.897
$57-3$	0.831	0.844	0.852
$58-1$	0.663	0.687	0.703
$58-2$	0.808	0.818	0.828
$61-1$	0.840	0.859	0.880
$62-1$	0.832	0.835	0.847
$65-1$	0.859	0.865	0.875
$66-1$	0.752	0.773	0.785
$66-2$	0.693	0.719	0.734
$66-3$	0.671	0.699	0.714
$67-1$	0.829	0.861	0.872

Courbe	6000	13000	20000
$69-1$	0.909	0.911	0.922
$70-1$	0.762	0.774	0.785
$73-1$	0.917	0.939	0.953
$77-1$	0.810	0.844	0.860
$77-2$	0.876	0.904	0.917
$77-3$	0.880	0.908	0.921
$78-1$	0.722	0.722	0.742
$79-1$	0.908	0.611	0.306
$82-1$	0.731	0.495	0.248
$83-1$	0.899	0.602	0.302
$85-1$	0.924	0.938	0.945
$89-1$	0.941	0.626	0.313
$89-2$	0.915	0.934	0.942
$91-1$	0.844	0.554	0.277
$91-2$	0.875	0.573	0.287
$94-1$	0.996	0.980	0.974

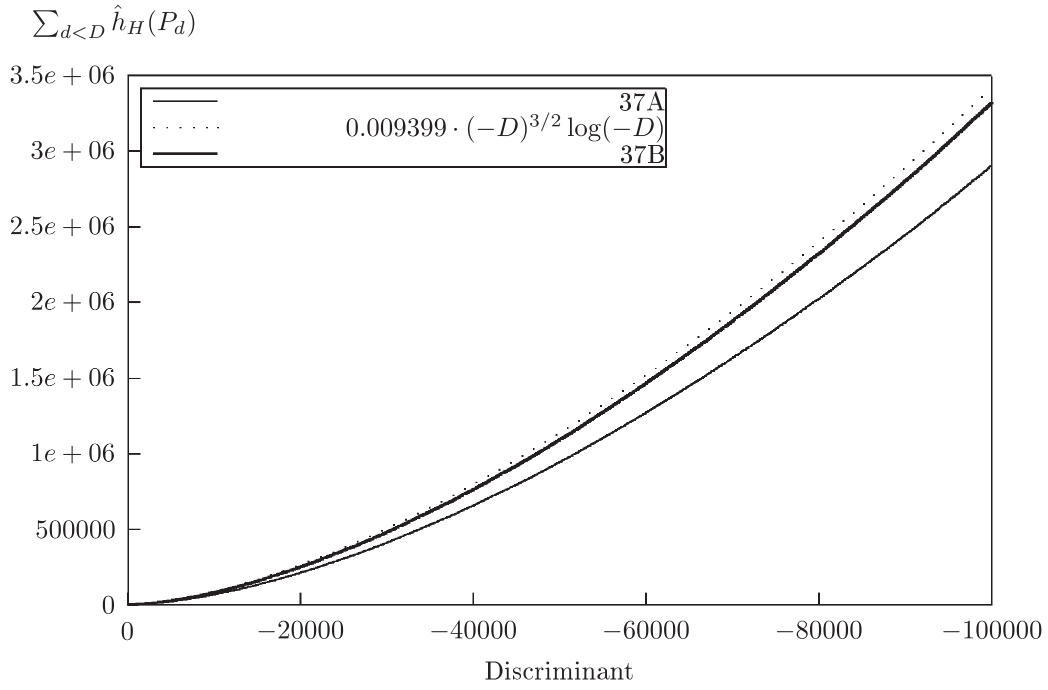

FIG. 7 – Hauteur des points en moyenne sur les courbes $37A$ et $37B$.

Ainsi, même pour des discriminants assez grands ($2 \cdot 10^4$), la constante expérimentale est souvent de l'ordre de 80% de la constante théorique. On a représenté plusieurs valeurs de Y pour bien montrer que ce rapport augmente toutefois, mais très lentement.

Nous allons étudier plus en profondeur les courbes $37A$ et $37B$.

La figure 7 représente la valeur de $\sum_{d \in \mathcal{D},\ d \leq Y} \hat{h}_H(P_d)$ pour ces deux courbes, ainsi que la courbe théorique.

Les courbes sont en apparence très lisses, mais cela est dû au grand nombre de points (presque 10^4), et à la forte croissance. Pour y voir plus clair, on a représenté $\beta_{exp}(Y)$ sur la figure 8. Il y a de fortes irrégularités pour les petits discriminants (ceci se comprend au vu de la figure 1), puis les deux courbes croissent très lentement vers la constante β.

On a l'impression que la courbe $37A$ est nettement en-dessous de la $37B$, sans paraître la rejoindre. Cependant une analyse plus fine de la différence entre ces deux courbes montre qu'elle est (ou semble être) en $Y^{3/2}$, et que donc les deux courbes se rapprochent à une vitesse de $1/\log Y$, ce qu'il est difficile d'observer dans l'échelle de discriminants représentée. Soit

$$\delta(Y) = \frac{1}{Y^{3/2}} \sum_{d \in \mathcal{D},\ d \leq Y} \left(\hat{h}_{H,37B}(P_d) - \hat{h}_{H,37A}(P_d) \right),$$

où les notations parlent d'elles-même. Le tableau suivant donne la valeur de δ pour plusieurs valeurs de Y :

Y	$2 \cdot 10^4$	$4 \cdot 10^4$	$6 \cdot 10^4$	$8 \cdot 10^4$	$10 \cdot 10^4$
$\delta(Y)$	0.01337	0.01329	0.01328	0.01326	0.01324

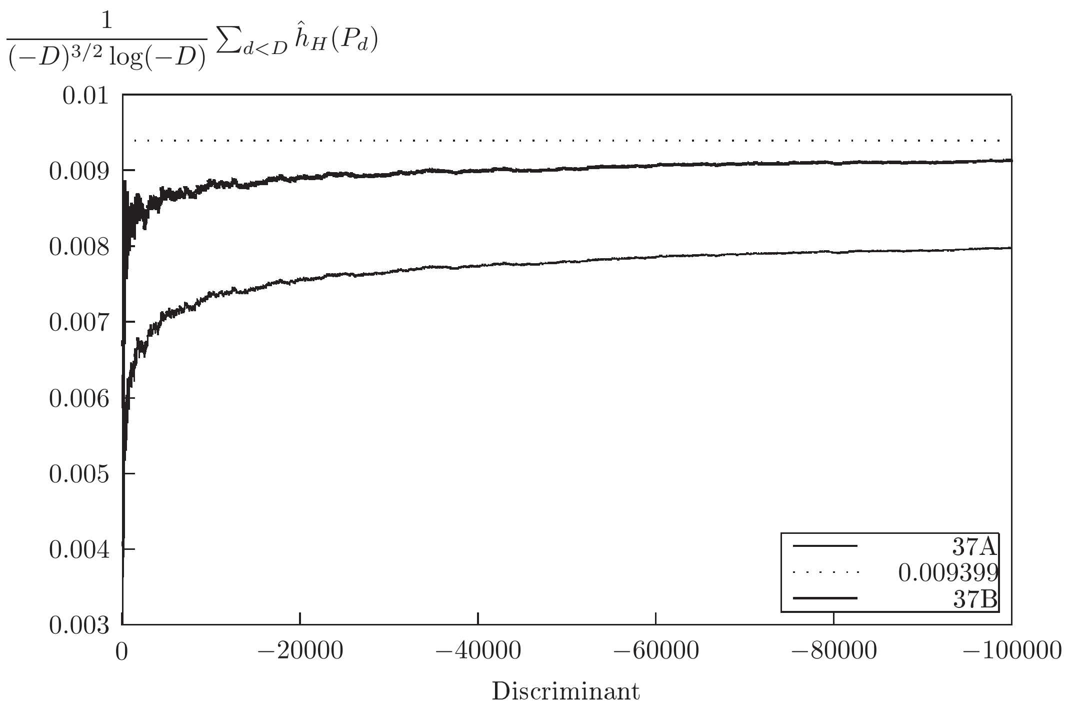

FIG. 8 – Constantes théoriques et pratiques pour les courbes $37A$ et $37B$.

Ainsi, $\delta(Y)$ décroît très légèrement avec Y. Ceci suggère que le terme en $Y^{3/2}$, dans le développement du corollaire 5.6, est non nul, et même de l'ordre du terme principal pour des petits discriminants. Pour obtenir une expression de ce terme, il est probable qu'il faille analyser en profondeur la somme

$$\sum_{d \in \mathcal{D}} r_d(n) \left(\frac{d}{p}\right)$$

pour tout premier p, et ainsi distinguer de multiples cas suivant les positions respectives de d, n et p.

Pour conclure, revenons à la remarque que l'on faisait dans la section 5.3.1 sur le rôle du facteur $L(E,1)L_N(1)$ dans la comparaison entre la hauteur du point de Heegner, et celle de la trace, dans le cas d'une courbe de rang 1. Le rapport entre ces deux hauteurs vaut

$$\frac{\alpha}{\beta} = \frac{\mathcal{P}(1)}{\mathcal{Q}(N)} L(E,1) \prod_{p|N} \left(1 - \frac{a_p}{p}\right)^{-1} \left(1 - \frac{a_{p^2}}{p^2}\right).$$

Pour simplifier, on néglige le rôle du rapport $\frac{\mathcal{P}(1)}{\mathcal{Q}(N)}$, qui est de toute façon borné. Ainsi, la position de

$$\gamma_E = L(E,1) \prod_{p|N} \left(1 - \frac{a_p}{p}\right)^{-1} \left(1 - \frac{a_{p^2}}{p^2}\right)$$

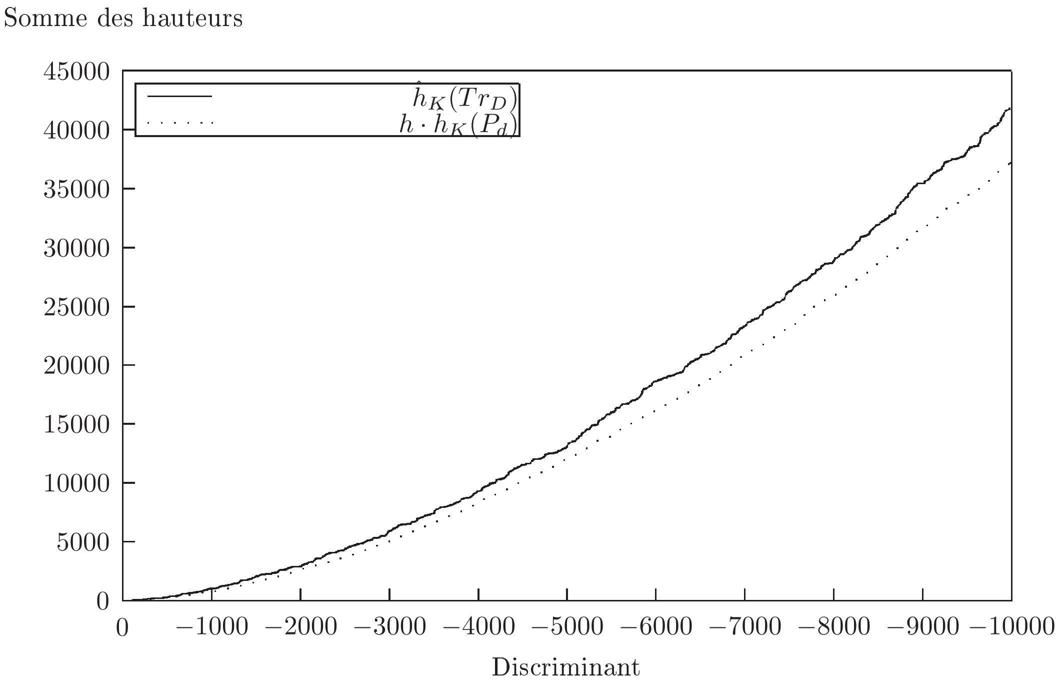

FIG. 9 – Somme des hauteur des traces et des points sur la courbe $34A$.

par rapport à 1 indique essentiellement le signe du terme

$$\sum_{\sigma \in G \setminus \{Id\}} < P, P^{\sigma} >_H .$$

Plus γ_E sera grand, plus ce produit scalaire sera grand, et, de manière imagée, on pourrait dire que les points de Heegner sont essentiellement resserés autour d'une même direction ; alors que si γ_E est petit devant 1, cette somme est négative et les points sont éclatés dans l'espace à h dimensions. Pour illustrer, nous donnons quelques valeurs de γ_E :

Courbe	γ_E
11 − 1	0.276
14 − 1	0.188
15 − 1	0.280
17 − 1	0.409
19 − 1	0.477
21 − 1	0.515
26 − 1	0.277

Courbe	γ_E
26 − 2	0.859
30 − 1	0.297
33 − 1	0.543
34 − 1	1.0578
35 − 1	0.642
37 − 2	0.745
38 − 1	0.331

Courbe	γ_E
38 − 2	1.1641
39 − 1	0.593
42 − 1	0.744
46 − 1	0.344
51 − 1	1.0792
55 − 1	1.1221
57 − 2	1.3709

Courbe	γ_E
57 − 3	0.740
58 − 2	1.4963
62 − 1	1.6094
66 − 1	0.483
66 − 2	1.0019
66 − 3	2.5998
67 − 1	1.2927

On s'attend donc, par exemple, à ce que la courbe de plus petit conducteur pour laquelle la hauteur des traces (en moyenne) soit supérieure à celle des points soit la $34A$, ce qui est illustré par la figure 9. Par contre, dans le cas de la courbe $37B$, les points sont plus petits (figure 10).

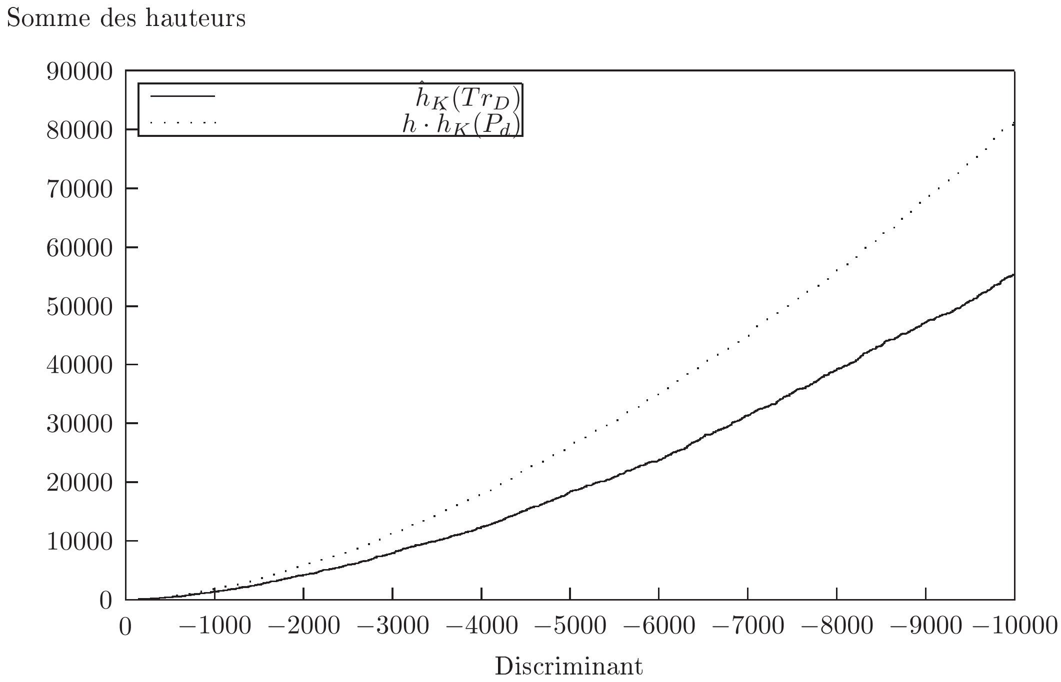

Fig. 10 – Somme des hauteur des traces et des points sur la courbe $37B$.

6 Annexes

6.1 Polynômes minimaux des points de Heegner

Je donne ici la liste, pour toutes les courbes de conducteur premier plus petit que 100, des polynômes minimaux des points de Heegner correspondant aux discriminants D listés ; ce sont tous les discriminants plus petits que 100. satisfaisant l'hypothèse de Heegner 3.2.

Ces tables sont là pour illustrer le comportement des points de Heegner, mais il n'y a aucune conclusion générale à en tirer : l'expérience a montré que le comportement des points était très irrégulier, et que déventuelles lois générales ne pouvaient s'observer que sur une quantité de valeurs beaucoup plus importante que celles données ici.

Courbe $11A$

D	P
-7	$(-1+\sqrt{-7})+2x$
-8	$(6-\sqrt{-8})+2x$
-11	$-5+x$
-19	$(7-2\sqrt{-19})+x$
-24	$(46-17\sqrt{-24})+(4+3\sqrt{-24})x+2x^2$
-28	$(22-17\sqrt{-28})+4x$
-32	$(348-28\sqrt{-32})+(-80+7\sqrt{-32})x+4x^2$
-35	$(17-10\sqrt{-35})+(-6-6\sqrt{-35})x+x^2$
-39	$(1394-388\sqrt{-39})+(-119-223\sqrt{-39})x+(154-68\sqrt{-39})x^2$
	$+(47+3\sqrt{-39})x^3+2x^4$
-40	$(102+59\sqrt{-40})+(-68-13\sqrt{-40})x+2x^2$
-43	$(-53-4\sqrt{-43})+x$
-44	$-257-211x-59x^2+x^3$
-51	$(233-38\sqrt{-51})+(-22+6\sqrt{-51})x+x^2$
-52	$(-405-79\sqrt{-52})+(50-\sqrt{-52})x+x^2$
-55	$18181+1502x-202x^2-53x^3+x^4$
-63	$(-31722-14460\sqrt{-63})+(5739+5545\sqrt{-63})x+(-10737$
	$-519\sqrt{-63})x^2+(420-46\sqrt{-63})x^3+6x^4$
-68	$(25499-903\sqrt{-68})+(68-589\sqrt{-68})x+(244-35\sqrt{-68})x^2$
	$+(24+11\sqrt{-68})x^3+x^4$
-72	$(-15294+693\sqrt{-72})+(324-91\sqrt{-72})x+6x^2$
-76	$(575-161\sqrt{-76})+(985-41\sqrt{-76})x+(-111+8\sqrt{-76})x^2+x^3$
-79	$(-190301+19448\sqrt{-79})+(-55131-4103\sqrt{-79})x+(40465-1154\sqrt{-79})x^2$
	$+(-3207+560\sqrt{-79})x^3+(-25-22\sqrt{-79})x^4+x^5$
-83	$(5115+428\sqrt{-83})+(-1229-224\sqrt{-83})x+(113+12\sqrt{-83})x^2+x^3$
-84	$(8503+1321\sqrt{-84})+(-7852+1219\sqrt{-84})x+(1040+533\sqrt{-84})x^2$
	$+(-128-21\sqrt{-84})x^3+x^4$
-87	$(-287558+525376\sqrt{-87})+(1144392+75710\sqrt{-87})x$
	$+(-118146-25576\sqrt{-87})x^2+(-71648-9404\sqrt{-87})$
	$x^3+(13779+1237\sqrt{-87})x^4+(-483-27\sqrt{-87})x^5+2x^6$
-88	$6911-274x+x^2$
-95	$(-78013782+6005036\sqrt{-95})+(-54965182+5491290\sqrt{-95})x$
	$+(3655898+2258988\sqrt{-95})x^2+(6653098-395864\sqrt{-95})x^3$
	$+(-290004-48408\sqrt{-95})x^4+(-2086-3438\sqrt{-95})x^5$
	$+(3473+553\sqrt{-95})x^6+(-155+43\sqrt{-95})x^7+2x^8$
-96	$(-70244-1476\sqrt{-96})+(-48688-2571\sqrt{-96})x$
	$+(-8656-912\sqrt{-96})x^2+(1000+15\sqrt{-96})x^3+4x^4$
-99	$2797-274x+x^2$

Courbe 17B

D	P
-4	$(2-\sqrt{-4})+x$
-8	$\sqrt{-8}+2x$
-15	$(4-\sqrt{-15})+3x+x^2$
-16	$(-12+\sqrt{-16})+4x$
-19	$(3-\sqrt{-19})+x$
-32	$(64-5\sqrt{-32})+(16-5\sqrt{-32})x+4x^2$
-35	$(6-2\sqrt{-35})+(-1+\sqrt{-35})x+x^2$
-36	$-26\sqrt{-36}+(42-\sqrt{-36})x+6x^2$
-43	$-2\sqrt{-43}+x$
-47	$(1470-32\sqrt{-47})+(273-57\sqrt{-47})x+(-102+4\sqrt{-47})x^2+(-41+9\sqrt{-47})x^3+(-6+2\sqrt{-47})x^4+2x^5$
-51	$32-14x+x^2$
-52	$(-32+10\sqrt{-52})+(-14-5\sqrt{-52})x+2x^2$
-55	$(-28-13\sqrt{-55})+(-157-\sqrt{-55})x+(-27-13\sqrt{-55})x^2+(14-\sqrt{-55})x^3+x^4$
-59	$(24-8\sqrt{-59})+(4-8\sqrt{-59})x+(-10-2\sqrt{-59})x^2+x^3$
-60	$(22-12\sqrt{-60})+(8+3\sqrt{-60})x+2x^2$
-64	$(-440+9\sqrt{-64})+(-144-16\sqrt{-64})x+8x^2$
-67	$(-25-\sqrt{-67})+x$
-68	$344+124x+22x^2-28x^3+x^4$
-72	$(-348-30\sqrt{-72})+(54-5\sqrt{-72})x+3x^2$
-76	$(-64-26\sqrt{-76})+(122-5\sqrt{-76})x+(-20+4\sqrt{-76})x^2+2x^3$
-83	$(240-32\sqrt{-83})+(-16-4\sqrt{-83})x+(18+2\sqrt{-83})x^2+x^3$
-84	$(800+296\sqrt{-84})+(840-48\sqrt{-84})x+(-212-16\sqrt{-84})x^2+(-42+3\sqrt{-84})x^3+2x^4$
-87	$(17224-330\sqrt{-87})+(-8656-324\sqrt{-87})x+(-4445+261\sqrt{-87})x^2$
	$+(-1310-102\sqrt{-87})x^3+(-385-27\sqrt{-87})x^4+(44-6\sqrt{-87})x^5+2x^6$
-100	$(-1850+56\sqrt{-100})+(70-22\sqrt{-100})x+5x^2$

Courbe 19A

D	P
-3	$(-3+3\sqrt{-3})+2x$
-8	$(2+\sqrt{-8})+2x$
-12	$(10-\sqrt{-12})+4x$
-15	$(-13+3\sqrt{-15})+(-3+\sqrt{-15})x+2x^2$
-19	$-5+x$
-27	$(9-2\sqrt{-27})+3x$
-31	$-11+(4-3\sqrt{-31})x+4x^2+x^3$
-32	$(-12-8\sqrt{-32})+(-8+5\sqrt{-32})x+4x^2$
-40	$(-46+3\sqrt{-40})-3\sqrt{-40}x+2x^2$
-48	$(116-29\sqrt{-48})+(-72+10\sqrt{-48})x+8x^2$
-51	$(-13-5\sqrt{-51})+(3-3\sqrt{-51})x+2x^2$
-52	$(-5-3\sqrt{-52})+9x+x^2$
-56	$(330-11\sqrt{-56})+(194-16\sqrt{-56})x+(-44+2\sqrt{-56})x^2+(-22+\sqrt{-56})x^3+2x^4$
-59	$(11-15\sqrt{-59})-2x+(9+3\sqrt{-59})x^2+2x^3$
-60	$(142+\sqrt{-60})+(-22-5\sqrt{-60})x+4x^2$
-67	$(-19-3\sqrt{-67})+2x$
-71	$(-5742+1540\sqrt{-71})+(-8420+88\sqrt{-71})x+(-2052-604\sqrt{-71})x^2+(871-27\sqrt{-71})x^3$
	$+(-156+26\sqrt{-71})x^4+(-109-19\sqrt{-71})x^5+(26-2\sqrt{-71})x^6+2x^7$
-72	$(159+23\sqrt{-72})+(-57-4\sqrt{-72})x+3x^2$
-75	$(65-22\sqrt{-75})+(-90-2\sqrt{-75})x+5x^2$
-76	$-87-77x-15x^2+x^3$
-79	$-246+(-1201-99\sqrt{-79})x+(238-48\sqrt{-79})x^2+(124+18\sqrt{-79})x^3+(-5+3\sqrt{-79})x^4+2x^5$
-84	$(181+20\sqrt{-84})+(-343+2\sqrt{-84})x+(56-11\sqrt{-84})x^2+(11+\sqrt{-84})x^3+x^4$
-88	$(-174-9\sqrt{-88})+(32-3\sqrt{-88})x+2x^2$
-91	$(125-9\sqrt{-91})+(-45+3\sqrt{-91})x+2x^2$
-95	$34261+17998x+8366x^2-1891x^3+468x^4+163x^5-136x^6-21x^7+x^8$

Courbe $37A$

D	P
-3	$1+x$
-4	$-1+x$
-7	0
-11	0
-12	$-1+x$
-16	$1+x$
-27	$-2+x$
-28	$-2+x$
-36	$-2-2x+x^2$
-40	$2+x^2$
-44	$-2+2x^2+x^3$
-47	$1-2x+x^2+x^3-x^4+x^5$
-48	$1-4x+x^2$
-63	$-3-6x+3x^3+x^4$
-64	$3+2x+x^2$
-67	$-6+x$
-71	$1-5x+8x^2-x^3-10x^4+9x^5-2x^6+x^7$
-75	$6-3x+x^2$
-83	$4+10x+5x^2+x^3$
-84	$-12+12x+10x^2-10x^3+x^4$
-95	$7-5x+x^2-4x^3-10x^4+13x^5+7x^6-5x^7+x^8$
-99	$3-12x+x^2$
-100	$21-2x+x^2$

Courbe $37B$

D	P
-3	$(377+87\sqrt{-3})+98x$
-4	$(72-2\sqrt{-4})+25x$
-7	$(27+\sqrt{-7})+8x$
-11	$(65+5\sqrt{-11})+18x$
-12	$(10-\sqrt{-12})+4x$
-16	$(8+\sqrt{-16})+2x$
-27	$(15-\sqrt{-27})+6x$
-28	$(-50-43\sqrt{-28})+64x$
-36	$(-168-3\sqrt{-36})+(-18-4\sqrt{-36})x+6x^2$
-40	$(7238+307\sqrt{-40})+(4798+46\sqrt{-40})x+722x^2$
-44	$(1604+252\sqrt{-44})+(1546+147\sqrt{-44})x+(474+21\sqrt{-44})x^2+44x^3$
-47	$(54714+4268\sqrt{-47})+(75364+3614\sqrt{-47})x+(42217+1001\sqrt{-47})x^2$
	$+(11987+97\sqrt{-47})x^3+(1700+2\sqrt{-47})x^4+94x^5$
-48	$(8644-1047\sqrt{-48})+(6952-294\sqrt{-48})x+1352x^2$
-63	$(24862416+2283318\sqrt{-63})+(23215518+1803866\sqrt{-63})x+(8590851+470019\sqrt{-63})x^2$
	$+(1468494+44338\sqrt{-63})x^3+96774x^4$
-64	$(4500+2012\sqrt{-64})+(5024+455\sqrt{-64})x+578x^2$
-67	$(1485-527\sqrt{-67})+1682x$
-71	$(7214466490-200441112\sqrt{-71})+(16361443360-580351246\sqrt{-71})x+(16085344815-609672213\sqrt{-71})x^2$
	$+(8784173941-314794383\sqrt{-71})x^3+(2853420721-86414357\sqrt{-71})x^4$
	$+(548114237-12130547\sqrt{-71})x^5+(57415528-686906\sqrt{-71})x^6+2522258x^7$
-75	$(-20+36\sqrt{-75})+(105-\sqrt{-75})x+10x^2$
-83	$(54172+6108\sqrt{-83})+(45305+2501\sqrt{-83})x+(12598+278\sqrt{-83})x^2+1058x^3$
-84	$(148552-26571\sqrt{-84})+(125554-18577\sqrt{-84})x+(64944-5683\sqrt{-84})x^2+(21580-836\sqrt{-84})x^3+2738x^4$
-95	$(10796807022+7606925932\sqrt{-95})+(19767314638+11676631040\sqrt{-95})x+(17146552142+6975024072\sqrt{-95})x^2$
	$+(9954601617+1873581593\sqrt{-95})x^3+(4150626869+121133743\sqrt{-95})x^4$
	$+(1153472928-49632236\sqrt{-95})x^5+(190040712-11217378\sqrt{-95})x^6+(15664922-703352\sqrt{-95})x^7+425042x^8$
-99	$(-276-68\sqrt{-99})+(99-21\sqrt{-99})x+54x^2$
-100	$(515+23\sqrt{-100})+(725-30\sqrt{-100})x+125x^2$

Courbe $43A$

D	P
-3	$-1+x$
-7	0
-8	0
-12	$1+x$
-19	$1+x$
-20	$1+x^2$
-27	$-1+x$
-28	$-2+x$
-32	$2+2x+x^2$
-39	$1-x-x^2-x^3+x^4$
-43	$-2+x$
-48	$1+x^2$
-51	$-2-3x+x^2$
-55	$1-x+5x^2-x^3+x^4$
-63	$-3-6x+3x^3+x^4$
-71	$1+x+3x^2+x^3+2x^5+2x^6+x^7$
-72	$3-6x+x^2$
-75	$6+3x+x^2$
-76	$-3+x+3x^2+x^3$
-80	$1-2x+4x^2-2x^3+x^4$
-88	$12-2x+x^2$
-91	$3-8x+x^2$

Courbe $53A$

D	P
-4	$-1+x$
-7	0
-11	0
-15	$1-x+x^2$
-16	$-1+x$
-24	$1-x+x^2$
-28	$-2+x$
-36	$1+x+x^2$
-40	$2+x^2$
-43	$-2+x$
-44	$-2+4x-4x^2+x^3$
-47	$-1+3x-3x^2+2x^3-x^4+x^5$
-52	$-1-3x+x^2$
-59	$-2+5x-3x^2+x^3$
-60	$1+x+x^2$
-63	$3-6x+6x^2-3x^3+x^4$
-64	$1+2x+x^2$
-68	$2-4x+7x^2-5x^3+x^4$
-91	$3-5x+x^2$
-95	$1-x+4x^2-4x^3+10x^4-11x^5+12x^6-5x^7+x^8$
-96	$3-6x+7x^2-2x^3+x^4$
-99	$3+3x+x^2$
-100	$6-2x+x^2$

Courbe $61A$

D	P
-3	$1+x$
-4	0
-12	$-1+x$
-15	$-1+x+x^2$
-16	0
-19	$-1+x$
-20	$-1+x+x^2$
-27	$1+x$
-36	$-3+x^2$
-39	$1+x-x^2+x^3+x^4$
-47	$1-2x+2x^2-x^3+x^5$
-48	$-3+x^2$
-52	$-3-x+x^2$
-56	$1-x+x^3+x^4$
-60	$1-3x+x^2$
-64	$4+4x+x^2$
-75	$1-3x+x^2$
-76	$-3+x+3x^2+x^3$
-80	$-1+x^2+x^4$
-83	$1+2x-2x^2+x^3$
-88	$3-x+x^2$
-95	$1-x-4x^2+6x^3+3x^4-7x^5-x^6+3x^7+x^8$
-100	$5-5x+x^2$

Courbe $67A$

D	P
-3	$5+x$
-7	$11+4x$
-8	$5+2x$
-11	$3+x$
-12	$7+3x$
-20	$29+24x+5x^2$
-27	$5+x$
-28	0
-31	$571+534x+145x^2+9x^3$
-32	$9+6x+2x^2$
-43	$19+9x$
-44	$199+233x+89x^2+11x^3$
-48	$149+122x+25x^2$
-51	$89+38x+x^2$
-52	$85+66x+13x^2$
-63	$2305+2924x+1242x^2+179x^3+x^4$
-67	0
-72	$313+218x+25x^2$
-75	$265+195x+36x^2$
-79	$941+197x-339x^2-79x^3+34x^4+9x^5$
-80	$4253+3490x+836x^2+110x^3+25x^4$
-87	$17681+43193x+41798x^2+20260x^3+5092x^4+608x^5+25x^6$
-95	$6575645+19574860x+25388573x^2+18755667x^3+8644547x^4+2551452x^5+472640x^6+50506x^7+2401x^8$
-99	$75+75x+16x^2$

Courbe $73A$

D	P
-3	$(-2-57\sqrt{-3})+49x$
-4	$(-72-2\sqrt{-4})+25x$
-8	$(-2-3\sqrt{-8})+4x$
-12	$(-4+\sqrt{-12})+2x$
-16	$\sqrt{-16}+2x$
-19	$(-8+12\sqrt{-19})+25x$
-23	$(-28-3\sqrt{-23})+(33+2\sqrt{-23})x+(-12+2\sqrt{-23})x^2+x^3$
-24	$(217+14\sqrt{-24})+(-44+\sqrt{-24})x+49x^2$
-27	$(-6+\sqrt{-27})+3x$
-32	$(-14-3\sqrt{-32})+(-8+3\sqrt{-32})x+4x^2$
-35	$-4+(6-\sqrt{-35})x+x^2$
-36	$-12-2\sqrt{-36}x+3x^2$
-48	$(2-2\sqrt{-48})+(-8+\sqrt{-48})x+2x^2$
-55	$(63+6\sqrt{-55})+(-258+19\sqrt{-55})x+(-149-32\sqrt{-55})x^2+(58-9\sqrt{-55})x^3+9x^4$
-64	$(-36-12\sqrt{-64})+(-48+7\sqrt{-64})x+18x^2$
-67	$(-18-89\sqrt{-67})+361x$
-71	$(-748052-53337\sqrt{-71})+(-1160395-60922\sqrt{-71})x+(-335236-40356\sqrt{-71})x^2+(-414084-39912\sqrt{-71})$ $x^3+(-16512-13512\sqrt{-71})x^4+(27176-6384\sqrt{-71})x^5+(6560-1022\sqrt{-71})x^6+11449x^7$
-72	$(-20-256\sqrt{-72})+(-1120+104\sqrt{-72})x+361x^2$
-75	$(-20-36\sqrt{-75})+(-165+27\sqrt{-75})x+40x^2$
-76	$(144+6\sqrt{-76})+(-60-20\sqrt{-76})x+(-48+7\sqrt{-76})x^2+9x^3$
-79	$(408+9\sqrt{-79})+(95-30\sqrt{-79})x+(-80+27\sqrt{-79})x^2+(-47-6\sqrt{-79})x^3-52x^4+9x^5$
-91	$(-171+15\sqrt{-91})+(87+25\sqrt{-91})x+72x^2$
-92	$(-84608-1323\sqrt{-92})+(-75750-15554\sqrt{-92})x+(53208-8444\sqrt{-92})x^2+20402x^3$
-96	$(-270+54\sqrt{-96})+(-144-57\sqrt{-96})x+(224+26\sqrt{-96})x^2+(-96-3\sqrt{-96})x^3+18x^4$
-100	$(-385-18\sqrt{-100})+(100-45\sqrt{-100})x+125x^2$

Courbe $79A$

D	P
-3	$2+x$
-7	0
-12	0
-15	$-1+x+x^2$
-24	$1+2x+x^2$
-27	$-1+x$
-28	$2+x$
-35	$-1+x+x^2$
-39	$-1-2x+2x^2+3x^3+x^4$
-43	$-1+x$
-47	$1-x-3x^2+3x^3+4x^4+x^5$
-48	$2+2x+x^2$
-56	$1+2x+x^2+2x^3+x^4$
-59	$-1+4x+4x^2+x^3$
-60	$-1-x+x^2$
-63	$-3-6x+3x^3+x^4$
-68	$1+x^2+2x^3+x^4$
-71	$1-2x^2-3x^3+x^4+5x^5+4x^6+x^7$
-75	$-1-x+x^2$
-79	$-3+8x-3x^2-5x^3+x^4+x^5$
-91	$-3-x+x^2$
-96	$1-4x+2x^2+4x^3+x^4$

Courbe 83A

D	P
-8	0
-15	$1+x+x^2$
-19	0
-20	$1+2x+x^2$
-24	$1+x+x^2$
-32	$2+2x+x^2$
-35	$2+x+x^2$
-39	$1+2x+2x^2+x^3+x^4$
-43	$-1+x$
-47	$-1+x^2+2x^3+2x^4+x^5$
-52	$2+2x+x^2$
-55	$3+4x+4x^2+3x^3+x^4$
-56	$2+2x+3x^2+3x^3+x^4$
-60	$3+3x+x^2$
-67	$-1+x$
-71	$1+8x+18x^2+24x^3+21x^4+13x^5+5x^6+x^7$
-72	$3+3x+x^2$
-76	$-2-2x+x^3$
-79	$-1-2x-3x^2+2x^4+x^5$
-80	$1+2x^2+x^4$
-83	$-2+x-x^2+x^3$
-88	$3-x+x^2$
-91	$2+x+x^2$
-96	$1+4x+5x^2+2x^3+x^4$

Courbe 89A

D	P
-4	$1+x$
-8	0
-11	0
-16	$1+x$
-20	$-1+x+x^2$
-32	$-2+x^2$
-36	$1-x+x^2$
-39	$1+2x^2+3x^3+x^4$
-40	$-1+x+x^2$
-44	$2+2x+2x^2+x^3$
-47	$-1-x-x^2+x^3+2x^4+x^5$
-55	$-1-2x+x^3+x^4$
-64	$1-2x+x^2$
-67	$-2+x$
-68	$-2-4x+x^2+3x^3+x^4$
-71	$-1-x-2x^2-2x^3-x^4+2x^5+3x^6+x^7$
-72	$3+3x+x^2$
-79	$-1+2x+x^2+3x^3+3x^4+x^5$
-80	$-1-x^2+x^4$
-84	$1+2x+3x^2+2x^3+x^4$
-87	$1-2x+5x^2+4x^3-x^4+x^5+x^6$
-88	$-2+x^2$
-91	$4+4x+x^2$
-99	$3+3x+x^2$
-100	$1-3x+x^2$

Courbe $89B$

D	P
-4	$(-8+22\sqrt{-4})+25x$
-8	$(-2+25\sqrt{-8})+36x$
-11	$(-2+5\sqrt{-11})+9x$
-16	$\sqrt{-16}+2x$
-20	$(-16-32\sqrt{-20})+(-144+36\sqrt{-20})x+81x^2$
-32	$(2+\sqrt{-32})+(-8-\sqrt{-32})x+4x^2$
-36	$(-144+5\sqrt{-36})+(-132+20\sqrt{-36})x+24x^2$
-39	$(-365+18\sqrt{-39})+(-262+71\sqrt{-39})x+(83+44\sqrt{-39})x^2+(58+\sqrt{-39})x^3+x^4$
-40	$(-9-\sqrt{-40})+(-4+2\sqrt{-40})x+4x^2$
-44	$(44-15\sqrt{-44})+(-2-16\sqrt{-44})x+(-44-3\sqrt{-44})x^2+2x^3$
-47	$(-187224+35777\sqrt{-47})+(38707-5902\sqrt{-47})x+(73808+4029\sqrt{-47})x^2$
	$+(90639-4938\sqrt{-47})x^3+(13316+504\sqrt{-47})x^4+6889x^5$
-55	$(13951-54972\sqrt{-55})+(-128224+32166\sqrt{-55})x+(235112-6012\sqrt{-55})x^2+(-60776+12978\sqrt{-55})x^3+39601x^4$
-64	$(7452-1900\sqrt{-64})+(-20144+1775\sqrt{-64})x+10658x^2$
-67	$(-882-235\sqrt{-67})+1369x$
-68	$(-2880+845\sqrt{-68})+(-2824-424\sqrt{-68})x+(1712-405\sqrt{-68})x^2+(1844-4\sqrt{-68})x^3+200x^4$
-71	$(-3966660-545443\sqrt{-71})+(-7402519+1340114\sqrt{-71})x+(13802020+652180\sqrt{-71})x^2+(3898199-1378396\sqrt{-71})x^3$
	$+(-7307088-263408\sqrt{-71})x^4+(-581755+317220\sqrt{-71})x^5+(383812+7758\sqrt{-71})x^6+11449x^7$
-72	$(96+32\sqrt{-72})+(144+12\sqrt{-72})x+27x^2$
-79	$(8905068-1748375\sqrt{-79})+(13872877-1305754\sqrt{-79})x+(11161004-32533\sqrt{-79})x^2$
	$+(4709777+115534\sqrt{-79})x^3+(854404+14038\sqrt{-79})x^4+49729x^5$
-80	$400+(-320-60\sqrt{-80})x+(-316+24\sqrt{-80})x^2+(80+15\sqrt{-80})x^3+25x^4$
-84	$(-39232+720\sqrt{-84})+(138400-1200\sqrt{-84})x+(-58820-11811\sqrt{-84})x^2+(-20140+5160\sqrt{-84})x^3+10952x^4$
-87	$(3674371+37170\sqrt{-87})+(4730666+718765\sqrt{-87})x+(-2830299+740200\sqrt{-87})x^2$
	$+(-3317532+82530\sqrt{-87})x^3+(-652326-68720\sqrt{-87})x^4+(30166-11095\sqrt{-87})x^5+10609x^6$
-88	$(-2439-2350\sqrt{-88})+(-13900+2375\sqrt{-88})x+10609x^2$
-91	$(-45+7\sqrt{-91})+(7+7\sqrt{-91})x+8x^2$
-99	$(-3831+425\sqrt{-99})+(1800+408\sqrt{-99})x+864x^2$
-100	$(-9360+352\sqrt{-100})+(-2000-1100\sqrt{-100})x+3125x^2$

6.2 Notes sur les programmes

Les programmes qui ont servi à obtenir les données numériques détaillées dans ce rapport ont été réalisés à l'aide des langages de programmation Pari/GP et Magma. Magma a l'avantage d'un très grand nombres de fonctions implémentées en théorie des nombres et en particulier concernant les courbes elliptiques, comme par exemple le calcul de la hauteur de Néron-Tate. Pari a présenté un léger avantage de vitesse. En particulier, Pari s'est avéré nettement plus performant que Magma pour le calcul des coefficients de la série L d'une courbe elliptique ; cet avantage a été crucial pour les calculs que l'on a effectués.

En Magma est implémentée une base de données de courbes elliptiques dûe à Cremona [Cre], qui a permis de faire facilement des boucles sur toutes les courbes elliptiques de conducteur sans facteur carré plus petit que 200, par exemple.

Les principaux programmes réalisés ont servi à calculer des points de Heegner plus ou moins directement, comme décrit dans la partie 4. Les fonctionnalités élevées du langage Magma ont par exemple permis de calculer des points de Heegner sur des *ring class field* de degré 5 ou 6 sur $\mathbb{Q}(\sqrt{D})$ en tant qu'éléments de ce corps, et non simplement leurs polynômes minimaux sur $\mathbb{Q}(\sqrt{D})$, puis de calculer avec une très grande précision leur hauteur de Néron-Tate.

Cependant, on a en général plutôt calculé les hauteurs en passant par un calcul de séries L, et en utilisant la formule de Gross-Zagier. Le calcul précis des points de Heegner eux-mêmes servait alors de vérification. Pour le calcul de séries L, le package *computel* pour Pari de Tim Dorkchister s'est avéré fort utile (http ://maths.dur.ac.uk/ dma0td/computel/).

Références

[CF] J.W.S. Cassels et A. Frohlich eds, Algebraic Number Theory, Academic Press, 1967.

[Coh93] H. Cohen, A course in computational algebraic number theory, Springer-Verlag GTM 138, 1993.

[Coh00] H. Cohen, Advanced topics in computational number theory, Springer-Verlag GTM 193, 2000.

[Cre] J.E. Cremona. Elliptic Curve Data, www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html.

[Da1] H. Darmon, Rational points on modular elliptic curves, CBMS Regional Conference Series in Mathematics, 101, American Mathematical Society, 2004.

[Da2] H. Darmon et P. Green, Elliptic curves and class fields of real quadratic fields : algorithms and evidence, Experimental Mahematics 11 :1 (2002), 37-55.

[Gr84] Benedict H. Gross, Heegner Points on $X_0(N)$, Modular Forms, ed. R.A. Rankin, Halsted Press, (1984) 87-105.

[GZ] B.H. Gross et Zagier, Derivatives of L-series and the height of Heegner points, Invent. Math. 84 (1986), 225-320.

[HJLS] , Polynomial time algorithms for finding integer relations among real numbers, Siam J. Comput. 18 (1989), 859-881.

[Iw] H Iwaniec, On the order of vanishing of modular L-functions at the critical point, Séminaire de théorie des nombres de Bordeaux 6 (1990), 365-375.

[Ja] G.J. Janusz, Algebraic Number Fields 2nd Ed., American Mathematical Society, Graduate Studies in Mathematics Vol. 7, 1991.

[Mur] M. R. Murty et V. K. Murty, Derivatives of modular L-series, Annals of Mathematics 133 (1991), 447-475.

[Se] Jean-Pierre Serre, Cours d'arithmétique, Presses Universitaires de France, 1970.

[Si86] Joseph H. Silverman, The arithmetic of elliptic curves, Springer-Verlag GTM 106, 1986.

[Si94] Joseph H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer-Verlag GTM 151, 1994.

[To] E. Tollis, Zeros of Dedekind zeta functions in the critical strip, Mathematics of Computation 66 :219 (1997), 1295-1321.

[Wa] Mark Watkins, Computing the modular degree of an elliptic curve, Experimental Mathematics 11 :4 (2002).