Modules supersinguliers et valeurs spéciales de fonctions L sur corps quadratiques imaginaires

David Marcil - McGill University

Abstract

Cet article s'inspire sur les travaux de Merel (voir [10]). Ils se concentrent tout d'abord sur l'homologie des courbes modulaires $X_0(p)$, pour p premier, pour étudier le *quotient d'enroulement* de $J_0(p)$. En utilisant les résultats de Gross (voir [7]), nous tenterons d'étudier plutôt les modules supersinguliers pour introduire des quotients similaires de $J_0(p)$. Nous analyserons en plus grand détails ces derniers pour entre autres indiquer leur relation avec le quotient de Merel. Ceci mènera vers divers résultats sur le rang analytique de courbes elliptiques de conducteur p sur des corps quadratiques imaginaires.

Notation : Tout au long de cet article, à moins d'avis contraire, $p > 3$ sera un nombre premier et $D < 0$ sera un discriminant fondamental tel que p est inerte dans $\mathcal{O}_D$, l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

1 Introduction

1.1 Courbes Modulaires et Formes Modulaires

Le sous-groupe de congruence

$$\Gamma_0(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \mod p \right\}$$

agit sur le demi-plan de Poincaré $\mathfrak{H}$ par l'intermédiaire de transformations de Mobius, ce qui engendre la surface de Riemann $Y_0(p) := \Gamma_0(p)\backslash\mathfrak{H}$. Ses points classifient, à isomorphisme près, les paires (E, C) où E est une courbe elliptique définie sur $\mathbb{C}$ et C est un de ses sous-groupes d'ordre p. On peut attacher $\mathbb{P}^1(\mathbb{Q})$ à $\mathfrak{H}$ en plongeant $\mathfrak{H}$ dans $\mathbb{C}$ naturellement. En considérant $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, on peut alors identifier $\mathbb{Q}$ avec les fractions sur l'axe réelle de $\mathbb{C}$ et ∞ comme un point à la limite de l'axe imaginaire.

Nous allons parfois écrire $+i\infty$ et $z \to +i\infty$ au lieu de $+\infty$ et $\mathrm{Im}(z) \to +\infty$ pour cette raison. Cela permet de joindre des "points à l'infini" à $Y_0(p)$ pour obtenir $X_0(p) := \Gamma_0(p)\backslash(\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}))$ qui est maintenant une courbe algébrique définie sur $\mathbb{Q}$. Elle porte le nom de *courbe modulaire de niveau p* et notons sa variété jacobienne par $J_0(p)$.

Remarque 1. Il n'est pas très difficile de comprendre le comportement de ces points à l'infini en fait. Une vérification rapide confirme que toute fraction réduite $\frac{s}{t} \in \mathbb{Q}$ tel que $(p, t) = 1$ est $\Gamma_0(p)$-équivalente à 0, et lorsque p divise t, on a que $\frac{s}{t}$ est $\Gamma_0(p)$-équivalente à ∞. Cette observation indique que $X_0(p) - Y_0(p) = \{\Gamma_0(p)0, \Gamma_0(p)\infty\}$. Les éléments de cet ensemble sont généralement appelés les *pointes de* $X_0(p)$. Ces dernières jouent un rôle important dans l'argument de Merel, mais ne seront pas particulièrement présentes dans notre cas.

Considérons aussi l'espace des fonctions holomorphes sur $\mathfrak{H}$ à valeurs complexes. On peut définir une action de $\mathrm{SL}_2(\mathbb{Z})$ sur de telles fonctions. Pour $f : \mathfrak{H} \to \mathbb{C}$ holomorphe et $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, définissons simplement $f|_\gamma := f \circ \gamma$.

Définition. Soit $k \in \mathbb{Z}_{\geq 0}$ et $f : \mathfrak{H} \to \mathbb{C}$ holomorphe. Si les conditions suivantes sont satisfaites

1. $f|_\gamma(z) = (cz+d)^k f(z)$, $\forall\, z \in \mathfrak{H}, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$,
2. $\lim\limits_{z \to +i\infty} f|_\gamma(z)$ existe, pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, et est holomorphe à $+i\infty$

on dit que f est une *forme modulaire de poids k et niveau p.* Le $\mathbb{C}$-espace vectoriel construit avec ces fonctions est dénoté par $M_k(p)$. En contrôlant le comportement de $f|_\gamma$ à l'infini sur tout $\mathrm{SL}_2(\mathbb{Z})$, on peut considérer f comme une fonction holomorphe sur $\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Étant donné que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(p)$, on obtient que $f(z+1) = f(z)$. On peut donc performer un changement de variable $z \mapsto q = e^{2\pi i z}$ et voir f (ou même $f|\gamma$ en général pour $\gamma \in \mathrm{SL}_2(\mathbb{Z})$) comme une fonction de q. Cette transformation envoie $\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ sur $\{z \in \mathbb{C} : |z| < 1 \text{ ou } z = e^{2\pi i \frac{s}{t}}, \text{ où } \frac{s}{t} \in \mathbb{Q}\}$ et plus précisément, envoie $i\infty$ à l'origine de ce disque. Pour cette raison, le développement de Fourier $f(z) = \sum_{n \geq 0} a_n q^n$, où $a_n \in \mathbb{C}$, de f autour de $q = 0$ est souvent appelé le *développement de f à l'infini.*

Bien évidemment, $a_0 = \lim\limits_{z \to +i\infty} f(z)$ et on peut s'intéresser aux cas où $a_0 = 0$. Si cette limite s'annihile aussi pour $f|_\gamma$, pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, on dit alors que f est un *forme parabolique de poids k et niveau p.* L'espace des formes paraboliques de poids k et niveau p est classiquement indiqué par $S_k(p)$.

Dans les sections futures, nous allons principalement nous concentrer sur $S_2(p)$. Notons que les éléments de $S_2(p)$ ne sont pas des fonctions sur $X_0(p)$. En effet, par définition, $f \in S_2(p)$ n'est pas invariant sous $\Gamma_0(p)$. Cependant, on observe aisément que

$$\frac{d}{dz}\gamma(z) = \frac{d}{dz}\frac{az+b}{cz+d} = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{ad-bc}{(cz+d)^2} = \frac{1}{(cz+d)^2} \ , \ \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$$

Et donc $d\gamma(z) = (cz+d)^{-2} dz$, ce qui prouve que le différentiel $f dz$ est invariant sous $\Gamma_0(p)$ et donc est bien défini sur la courbe modulaire $X_0(p)$. Cela indique déjà l'existence d'une connection plus profonde entre $S_2(p)$ et $X_0(p)$, et donc entre $S_2(p)$ et les courbes elliptiques sur $\mathbb{C}$. Nous revisiterons ce lien au cours de ce document.

1.2 Module Supersingulier

Soit g le genre de $X_0(p)$. Il est bien connu qu'il existe $g+1$ classes d'isomorphisme de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$. Considérons des représentants $E_0, \ldots, E_g$ pour chacune de ces classes.

Définition. Le *module supersingulier de niveau p* est défini comme étant le $\mathbb{Z}$-module libre

$$\mathcal{P} := \bigoplus_{i=0}^{g} \mathbb{Z}[E_i]$$

et notons sa partie de degré 0 par

$$\mathcal{P}^0 := \left\{ \sum_{i=0}^{n} m_i [E_i] \in \mathcal{P} \ : \ \sum_{i=0}^{n} m_i = 0 \right\}$$

Pour un anneau A, nous noterons $\mathcal{P}_A := \mathcal{P} \otimes A$ pour étendre le domaine des coefficients de $\mathcal{P}$. Dans ce cas, $\mathcal{P}_A^0$ réfère encore à la partie de degré 0 de ce A-module libre. De plus, notons $w_i := \dfrac{\#\mathrm{Aut}(E_i)}{2}$ pour définir le produit scalaire

$$\langle E_i, E_j \rangle := \begin{cases} w_i & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

sur $\mathcal{P}$. En définissant $\mathrm{Eis} := \sum_{i=0}^{g} \frac{1}{w_i}[E_i]$, on obtient la décomposition orthogonale $\mathcal{P} = \mathbb{Z}\mathrm{Eis} \oplus \mathcal{P}^0$. Cette forme bilinéaire et cette décomposition s'étendent naturellement sur $\mathcal{P}_A$ pour tout anneau A.

Remarque 2. Lorsque le produit tensoriel à considérer est évident et d'une importance moindre, nous l'omettrons de la notation, ce que nous avons fait exactement en écrivant $\mathcal{P} = \mathbb{Z}\mathrm{Eis} \oplus \mathcal{P}^0$. En charactéristique $p > 3$, il est bien connu que $\prod_i w_i$ est égal au dénominateur exact de $\frac{p-1}{12} = \frac{\eta}{\delta}$, voir [7]. Il faut donc inverser δ pour pouvoir considérer Eis et formuler $\mathcal{P}_Z = Z\mathrm{Eis} \oplus \mathcal{P}_Z^0$, où $Z = \mathbb{Z}[\frac{1}{\delta}]$. Cependant, cela alourdit la notation inutilement, d'où notre abus.

La formule de masse de Eichler indique que $\deg(\mathrm{Eis}) = \sum_{i=0}^{g} \frac{1}{w_i} = \frac{p-1}{12}$. On définit alors $\pi^0 := \mathcal{P} \twoheadrightarrow \mathcal{P}^0$ par $x \mapsto x - \frac{12}{p-1}\deg(x)\mathrm{Eis}$. L'avantage de cette projection par rapport à une autre plus naive, par exemple $x = \sum_{i=0}^{g} x_i[E_i] \mapsto \sum_{i=0}^{g}(x_i - \frac{\deg(x)}{g+1})[E_i]$, est qu'elle préserve le produit scalaire avec $\mathcal{P}^0$. Plus précisément, pour tout $x \in \mathcal{P}, y \in \mathcal{P}^0$, on voit que $\langle x, y\rangle = \langle \pi^0(x), y\rangle$.

Dans [11], Mestre énonce un important théorème qui justifie la connection entre $\mathcal{P}^0$ et $S_2(p)$. La forme suivante est une reformulation du résultat cité par Mestre pour nos besoins.

Théorème 1. *Pour tout $p > 3$ premier, il existe un isomorphisme, compatible avec l'action des opérateurs de Hecke, entre $\mathcal{P}_{\mathbb{C}}^0$ et $S_2(p)$.*

Ce théorème mentionne les *opérateurs de Hecke*, que nous introduisons dans la section subséquente. Essentiellement, ces deux espaces sont isomorphes en tant que $\mathbb{T}$-module, où $\mathbb{T}$ est l'algèbre générée par les opérateurs de Hecke.

1.3 Algèbre de Hecke

Pour $n \in \mathbb{N}$ premier à p, définissons le *n-ième opérateur de Hecke* T_n agissant sur $\mathcal{P}^0$ via

$$[E_i] \mapsto \sum_{C_n} [E_i/C_n] \ ,$$

où cette somme parcourt les sous-groupes C_n d'ordre n de E_i. De plus, notons par $E_i^{(p)}$ la courbe elliptique, unique à isomorphisme près, tel que $j(E_i^{(p)}) = j(E_i)^p$, où $j(E)$ est l'invariant j d'une courbe elliptique E. On définit alors l'*involution d'Atkin-Lehner* W_p qui agit sur $\mathcal{P}^0$ via

$$[E_i] \mapsto [E_i^{(p)}]$$

Dans [13], on démontre que ces opérateurs sont tous bien définis. En particulier, le fait que W_p est une involution vient du résultat que $j(E_i) \in \mathbb{F}_{p^2}$ pour tout $i = 0, \ldots, g$. le $\mathbb{Z}$-algèbre $\mathbb{T}$ que les opérateurs T_n et W_p engendrent est dénommé l'*algèbre de Hecke*. Notons $\mathbb{T}_A := \mathbb{T} \otimes A$.

Dans [7], on démontre que ces opérateurs sont auto-adjoints par rapport au produit scalaire $\langle \cdot, \cdot \rangle$, ils sont alors diagonalisables. En particulier, comme W_p est une involution, on peut décomposer $\mathcal{P}^0$ en deux sous-espaces $\mathcal{P}^0 = \mathcal{P}^{0,+} \oplus \mathcal{P}^{0,-}$ qui correspondent aux espaces propres de $+1$ et -1.

D'un autre côté, on peut aussi définir les opérateurs T_n par leur action sur $S_2(p)$, voir [4] et générer $\mathbb{T}$. L'énoncé du théorème 1 indique alors que $\mathcal{P}^0_{\mathbb{C}}$ et $S_2(p)$ sont isomorphes en tant que $\mathbb{T}_{\mathbb{C}}$-module. De plus, il existe même un produit scalaire $(\cdot, \cdot)$ sur $S_2(p)$, le *produit de Petersson* (voir [4]), par rapport auquel les opérateurs T_n et W_p sont aussi auto-adjoints. On obtient de nouveaux des sous-espaces propres $S_2(p)^+$ et $S_2(p)^-$ pour W_p.

1.3.1 Construction de l'algèbre de Hecke sur $\mathcal{P}^0$

L'article de Mestre [11] décrit une façon explicite pour construire ces opérateurs. Sa *Méthode des Graphes* permet d'accomplir bien plus, mais nous utiliserons principalement la partie qui calcule T_n.

Tentons tout d'abord de trouver T_2. Rappelons que nous assumons $p > 3$, alors T_2 représente la transformation linéaire qui envoie une courbe elliptique supersingulière E_i vers tous ses voisins 2-isogènes, en comptant les multiplicités.

Tout d'abord, Mestre indique comment trouver un premier invariant j supersingulier. Il suggère d'utiliser la théorie de la multiplication complexe. Cependant, les méthodes qu'il propose ne couvrent pas tous les cas possibles et si aucune d'entre elles ne s'appliquent, il faut alors chercher par force brute. Nous proposons une méthode légèrement différente. Notons que si $p \equiv 2 \bmod 3$, alors $j = 0$ est supersingulier en charactéristique p, et si $p \equiv 3 \bmod 4$, alors $j = 1728$ est supersingulier. Le seul cas restant est lorsque $p \equiv 1$ modulo 12.

Posons $m = \frac{p-1}{2}$ et définissons

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

parfois dénommé le *p-ième polynôme de Hasse*. Étant donnée que nous travaillons en charactéristique $p > 3$, toutes classes d'isomorphismes de courbes elliptiques définies sur $\bar{\mathbb{F}}_p$ possèdent une courbe définie par une équation sous la forme

$$E : y^2 = x(x-1)(x-\lambda) \ , \quad \text{où } \lambda \neq 0, 1, \lambda \in \bar{\mathbb{F}}_p$$

Dans [13], Silverman démontre que la courbe E est supersingulière exactement lorsque $H_p(\lambda) = 0$. On peut alors résoudre cette équation et utiliser la relation

$$j(E) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (\lambda - 1)^2}$$

Nous avons alors trouver un premier invariant j supersingulier j_0 et notons la classe d'isomorphismes qu'il classifie par $[E_0]$. Pour s'avoir l'image de $[E_0]$ par T_2, il suffit de résoudre le 2-ième polynôme modulaire classique. Il s'agit d'un polynôme $\Phi_2 \in \mathbb{F}_p[x, y]$ tel que (j', j'') est un zéro si et seulement s'il existe un 2-isogénie entre les courbes elliptiques E' et E'' tel que $j(E') = j'$ et $j(E'') = j''$. La plupart des langages de programmation de théorie des nombres, tel que Magma, Sage et Pari, possède une implémentation pour ces polynômes. On peut alors résoudre $\Phi_2(j_0, j')$ dans $\mathbb{F}_{p^2}$ pour trouver d'autres invariants j supersinguliers, disons $j_1, \ldots, j_k$. On peut alors recommencer avec j_1, résoudre $\Phi_2(j_1, j')$ et ainsi de suite. Mestre prouve que ce processus trouve tous les invariants j supersinguliers.

En général, voir [13], nous allons en obtenir

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & , \text{ si } p \equiv 1 \mod 12 \\ 1 & , \text{ si } p \equiv 5 \text{ ou } 7 \mod 12 \\ 2 & , \text{ si } p \equiv 11 \mod 12 \end{cases}$$

où $\lfloor x \rfloor$ représente le plus grand entier inférieur à x.

Nous avons alors tous les invariants j supersinguliers $j_0, j_1, \ldots, j_g$ et T_2. On peut ensuite trouver tout autre opérateur de Hecke T_l pour l premier, $l \neq p$, en remplacant le 2-ième polynôme modulaire classique par le l-ième. Finalement, pour calculer T_n pour $(n,p) = 1$, on utilise alors les relations

1. $T_{mn} = T_m T_n$ pour tout $m, n \geq 1$ tel que $p \not| m, n$ et $(m,n) = 1$

2. $T_{l^{e+1}} = T_{l^e} T_l - l T_{l^{e-1}}$ pour tout l premier $l \neq p$ et $e > 1$.

On peut aussi évidemment calculer W_p en identifiant les paires (j_a, j_b) tel que $j_a^p = j_b$. Le tout construit le $\mathbb{Z}$-module supersinguler $\mathcal{P}$ de niveau p et les matrices de $M_{g+1}(\mathbb{Z})$ avec lesquels l'algèbre Hecke $\mathbb{T}$ agit sur $\mathcal{P}$ par rapport à la base $[E_0], \ldots, [E_g]$.

1.3.2 Propriétés de l'algèbre de Hecke

Un fameux résultat d'Atkin et Lehner, voir [1], démontre que $\mathbb{T}_{\mathbb{C}}$ est un algèbre commutatif semi-simple, ce qui implique qu'il existe des bases pour $\mathcal{P}^0_{\mathbb{C}}$ et $S_2(p)$ consistant de vecteurs propres pour tous les opérateurs de $\mathbb{T}_{\mathbb{C}}$ simultanément.

Soit $f \in S_2(p)$ dans une telle base, appelé *forme de Hecke*. Il n'est pas très difficile de trouver dans la littérature des formules qui indiquent comment T_n agit sur un développement à l'infini. Si $f(z) = \sum_{n \geq 1} a_n q^n$, ces formules dévoilent que pour tout n premier à p, $T_n f = \sum_{n \geq 1} b_n q^n$ tel que $b_1 = a_n$. Cependant, comme f est une forme primitive, disons que sa valeur propre pour T_n est $\lambda_n \in \mathbb{C}$, on sait que cette série commence par $b_1 = \lambda_n a_1$, i.e. $a_n = \lambda_n a_1$. On en conclut que $a_1 \neq 0$ et donc qu'on peut normaliser f pour obtenir $a_1 = 1$. On dit alors que f est une *forme de Hecke primitive* ou tout simplement une *forme primitive*.

Remarque 3. Cette observation implique alors immédiatement que pour toute forme f, nous avons $a_n = \lambda_n$. Comme les opérateurs de Hecke T_n ont des coefficients entiers, ces valeurs propres λ_n sont des entiers algébriques. Cette remarque justifie l'attention que nous allons porter plus tard sur $\mathbb{T}_{\bar{\mathbb{Q}}}$, $\mathcal{P}^0_{\bar{\mathbb{Q}}}$ et $S_{\bar{\mathbb{Q}}} = \{ \sum_{n \geq 1} a_n q^n \in S_2(p) : a_n \in \bar{\mathbb{Q}} \}$.

L'isomorphisme du Théorème 1 peut en fait être restraint à $\mathcal{P}^0_{\bar{\mathbb{Q}}}$ et $S_{\bar{\mathbb{Q}}}$. Un résultat encore plus profond indique que ces deux espaces sont isomorphes en tant que $\mathbb{T}_{\bar{\mathbb{Q}}}$-modules libres de rang 1, voir [12]. Cela indique que pour toute forme primitive $f \in S_{\bar{\mathbb{Q}}}$, étant donné que $\mathbb{T}_{\bar{\mathbb{Q}}}$ est semi-simple, il existe un idempotent $\mathbf{1}_f \in \mathbb{T}_{\bar{\mathbb{Q}}}$ qui projette $S_{\bar{\mathbb{Q}}}$ sur la $\bar{\mathbb{Q}}$-droite engendrée par f. Puisque $\mathcal{P}^0_{\bar{\mathbb{Q}}}$ est aussi de rang 1, on obtient que $\mathbf{1}_f(\mathcal{P}^0_{\bar{\mathbb{Q}}})$ est aussi une $\bar{\mathbb{Q}}$-droite, disons une *droite de Hecke*. Pour tout $x \in \mathcal{P}^0_{\bar{\mathbb{Q}}}$, on voit aisément que $\mathbf{1}_f(x) = \dfrac{\langle x, a_f \rangle}{\langle a_f, a_f \rangle} a_f$, où a_f est un quelconque vecteur directeur de $\mathbf{1}_f(\mathcal{P}^0_{\bar{\mathbb{Q}}})$. De plus, comme les opérateurs de Hecke sont auto-adjoints, il s'en suit que les formes primitives et droites de Hecke sont perpendiculaires entre elles. Autrement dit, elles constituent des bases orthogonales pour $S_2(p)$ et $\mathcal{P}^0_{\bar{\mathbb{Q}}}$ respectivement.

2 Éléments de Gross

2.1 Définition

Dans cette section nous rappelons brièvement la définition des éléments de Gross. Cependant, pour de plus amples détails, voir [7] et [12]. Soient $R_i := \mathrm{End}(E_i)$ pour tout $i = 0, \ldots, g$. Étant donné que les courbes elliptiques $E_0, \ldots, E_g$ sont supersingulières, leurs anneaux d'endomorphismes sont des ordres maximaux dans l'algèbre de quaternions $B_{p,\infty}$ ramifiée exactement en p et à l'infini. Si $f, g : \mathcal{O}_D \hookrightarrow R_i$ sont deux plongements, on dit qu'ils sont équivalents s'il existe une unité $u \in R_i^\times$ tel que $f = ugu^{-1}$. Dans ce cas, définissons $h_i(D)$ comme étant le nombre de classes d'équivalence de plongements de $\mathcal{O}_D \hookrightarrow R_i$. Alors, le *D-ième élément de Gross* est défini comme étant

$$\gamma_D := \frac{1}{2u(D)} \sum_{i=0}^{g} h_i(D)[E_i] \in \mathcal{P}_{\mathbb{Q}}$$

où $u(D) := |\mathrm{Pic}(\mathcal{O}_D)^\times|/2$. En fait, $u(D) = 1$ pour tout D, à l'exception de $u(-3) = 3$ et $u(-4) = 2$. Nous manipulerons principalement $\gamma_D^0 := \pi^0(\gamma_D)$ ainsi que $\gamma_D^f := \mathbf{1}_f(\gamma_D^0)$.

2.2 Algorithme pour calculer γ_D

Spécifions que Gross définit en fait γ_D de façon plus formelle en utilisant l'anneau des adèles. L'interprétation ci-dessus est tout simplement plus intuitive, mais elle présente une certaine ambiguité. La confusion principale est la suivante : Dans $B_{p,\infty}$, il existe un nombre fini de classes de conjugaison d'ordres maximaux. Ces dernières sont toutes représentées dans $R_0, \ldots, R_n$, mais une même classe peut s'y retrouver plusieurs fois. Essentiellement, pour $i \neq j$, R_i et R_j sont conjugés si et seulement si E_i est isomorphe à $E_j^{(p)}$ (voir [7]). Ceci est problématique puisque, si R_i et R_j appartiennent à la même classe, tout plongement $f : \mathcal{O}_D \hookrightarrow R_i$ peut être conjugé par un certain $b \in B_{p,\infty}$ tel que $R_j = b^{-1}R_i b$ pour obtenir un plongement équivalent $b^{-1}fb : \mathcal{O}_D \hookrightarrow R_j$. Devons-nous alors compter f dans $h_i(D)$ ou dans $h_j(D)$?

Étape 1 : Trouver des bases pour $R_0, \ldots, R_g$.

Tout d'abord, il suffit de calcul un premier ordre maximal en utilisant un algorithme de Voight (voir [15]). Après réénumération, disons qu'il s'agit de R_0. Déterminons alors ses classes d'idéaux à gauche, un processus décrit dans [14], chapitre 17. Il est bien connu qu'il en existe $g + 1$ et que leurs ordres à droite sont exactement $R_0, \ldots, R_g$, à conjugation près. Alors, on peut les appeler $I_0, \ldots, I_g$ de façon à ce que l'ordre à droite de I_i soit R_i. Calculer l'ordre à droite de I_i n'est qu'un problème d'algèbre linéaire, donc ceci nous permet de trouver $R_0, \ldots, R_g$. Certains langages de programmation comme Sage et Magma sont capable d'accomplir le tout.

Étape 2 : Trouver un premier plongement $f : \mathcal{O}_D \hookrightarrow R_i$.

Ceci peut être accomplie en trouvant $b \in R_i$ tel que $b^2 = D$ puisque cela définit un plongement $\mathbb{Z}[\sqrt{D}] \hookrightarrow R_i$ par $\sqrt{D} \mapsto b$. Cependant, si $D \equiv 1 \bmod 4$, on doit aussi vérifier que $\frac{b+1}{2} \in R_i$ pour s'assurer que ce plongement s'étend à $\mathcal{O}_D$. On énumère tout d'abord les éléments dans R_0 en ordre croissant de norme. Si aucun membre de R_0 ne répond au critère $b^2 = D$, on passe alors à R_1 et ainsi de suite. Comme p est inerte dans $\mathcal{O}_D$, on peut démontrer qu'au moins un de ces ordres maximaux contient un tel b. Après réénumération, on peut assumer qu'il s'agit de R_0.

Étape 3 : Calculer $h_i(D)$.

Nous expliquons enfin comment régler la problématique mentionnée précédemment. L'idée est de travailler avec les idéaux à gauche $I_0, \ldots, I_g$ de R_0 plutôt qu'avec les ordres maximaux $R_0, \ldots, R_g$ directement. En effet, si deux ordres R_i et R_j sont conjugés, les idéaux correspondants I_i et I_j ne le sont pas par contre, ce qui permet de les distinguer. Soit $\mathrm{Pic}(\mathcal{O}_D) = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$, où h est le nombre de classes de $\mathcal{O}_D$. Pour tout $k = 1, \ldots h$, on observe que $R_0 f(\mathfrak{a}_k)$ est un idéal à gauche de R_0. Donc, $R_0 f(\mathfrak{a}_k)$ est représenté par une unique classe d'idéaux à gauche de R_0, disons I_{i_k}. Son ordre à droite est donc conjugée à R_{i_k}. Étant donné que $\mathcal{O}_D$ agit par sur la droite de $\mathfrak{a}_k$, il s'en suit que $f(\mathcal{O}_D)$ agit sur la droite de $R_0 f(\mathfrak{a}_k)$, autrement dit que $f(\mathcal{O}_D)$ est contenu dans R_{i_k}, à conjugaison près. Ceci induit un nouveau plongement $f_{\mathfrak{a}_k} : \mathcal{O}_D \hookrightarrow R_{i_k}$. Gross démontre que $f_{\mathfrak{a}_1}, \ldots, f_{\mathfrak{a}_h}$ sont tous non-équivalents. Notons $l_i(D)$ le nombre de plongements $\mathcal{O}_D \hookrightarrow R_i$ trouvés ainsi. Gross démontre aussi que $h_i(D) = 2l_i(D)$, ou en d'autres mots, ceci trouve la moitié des plongements et l'autre moitié correspond en fait aux mêmes plongements avec "l'orientation" inverse.

Étape 4 : Calculer γ_D.

Il suffit de trouver la correspondence explicite $E_i \longleftrightarrow R_i$. Jusqu'à maintenant nous n'avons qu'utiliser la relation théorique $R_i = \mathrm{End}(E_i)$. Par contre, ayant un ordre maximal R de $B_{p,\infty}$ en main, comment peut-on trouver la classe d'isomorphismes de courbes elliptiques $[E]$ tel que $R = \mathrm{End}(E)$? Chevyrev et Galbraith (voir Algorithme 2 de [3]) ont trouvé un moyen concret de performer cette tâche. Une fois accomplie, on trouve finalement

$$\gamma_D = \frac{1}{2u(D)} \sum_{i=0}^{g} h_i(D)[E_i] = \frac{1}{u(D)} \sum_{i=0}^{g} l_i(D)[E_i]$$

Table 1: Éléments de Gross pour divers premiers p et discriminants D

p	$j(E_0), \ldots, j(E_g)$	Détails	D	γ_D
11	0, 1728	–	-3	[0, 1/3]
			-20	[1, 1]
			-47	[3, 2]
53	0, -7, -3, $28 \pm 9\alpha$	$\alpha^2 = 2$	-8	[0, 0, 1, 0, 0]
			-23	[0, 1, 0, 1, 1]
			-35	[0, 0, 0, 1, 1]
73	56, 9, $39 \pm 36\alpha$, $8 \pm 11\alpha$	$\alpha^2 = -11$	-104	[2, 0, 1, 1, 1, 1]
			-167	[3, 2, 2, 2, 1, 1]
			-271	[3, 2, 1, 1, 2, 2]
251	-29, 101, -19, 64, 4, 35, $79 \pm 95\alpha$, 24, -66, $30 \pm 2\alpha$, 44, $-85 \pm 52\alpha$ $-73 \pm 71\alpha$, -38, -112, -52, 0, 30	$\alpha^2 = 57$	-260	[1, 1, 2, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]

Malgré l'allure plus ou moins compliquée de cet algorithme , on peut tout de même prouver que pour toute paire (i,j) tel que $E_i^{(p)} \cong E_j$, on a $l_i(D) = l_j(D)$. Autrement dit, si $i \neq j$ et R_i et R_j sont conjugés, alors les plongements qui causaient problèmes plus haut se divisent en deux parties égales dans les coefficients de $[E_i]$ et $[E_j]$. Par définition de l'involution d'Atkin-Lehner, cela signifie que $W_p\gamma_D = \gamma_D$. On sait alors que $\gamma_D \in \mathcal{P}^{0,+}$.

2.3 Valeurs spéciales de fonctions L sur des corps quadratiques imaginaires

Soit $f(z) = \sum_{n\geq 1} a_n q^n \in S_2(p)$. On définit la *fonction L de f* comme la série de Dirichlet

$$L(f,s) := \sum_{n\geq 1} a_n n^{-s}$$

Pour plus de détails sur la convergence et la continuation analytique de cette fonction, voir [4]. Ce qui nous importe principalement est que pour toute forme primitive f, $L(f,s)$ possède un développement en produit eulerien

$$L(f,s) = \prod_{p \text{ premier}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

et est holomorphe près de $s = 1$.

Dans [7], Gross donne une connection profonde entre $L(f,1)$ et les éléments de Gross. Soit ε_D le caractère de Dirichlet définit par le symbole de Kronecker $\left(\frac{D}{\cdot}\right)$. On peut "tordre" $f(z) = \sum_{n\geq 1} a_n q^n \in S_2(p)$ par ε_D pour obtenir $f \otimes \varepsilon_D := \sum_{n\geq 1} \varepsilon_D(n) a_n q^n \in S_2(p)$.

En fait, il démontre que pour toute forme primitive $f \in S_2(p)$,

$$L(f,1)L(f\otimes\varepsilon_D,1) = c_{f,D}\langle \gamma_D^f, \gamma_D^f\rangle \tag{1}$$

où $c_{f,D} \in \mathbb{C}$ est une constante non nulle. Ces fonctions partagent un lien important avec les courbes elliptiques. Soit E, une courbe elliptique définie sur $\mathbb{Q}$, de conducteur N_E (voir [4] pour la définition d'un conducteur). Alors, E possède une équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , \ a_i \in \mathbb{Z}$$

non singulière.

On peut alors réduire les coefficients a_i modulo p, pour divers p premier. On définit $N_p(E) := p + 1 - \#E(\mathbb{F}_p)$. En comptant $\#E(\mathbb{F}_p)$, il ne faut pas négliger le point à l'infini et si la réduction de E modulo p est singulière, on ne considère que les points non-singuliers.

Théorème 2 (Wiles)**.** *Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N_E. Il existe une unique forme primitive $f_E(z) = \sum_{n\geq 1} a_n q^n \in S_2(N_E)$ tel que $a_p = N_p(E)$ pour tout p premier.*

Il s'agit içi du fameux théorème de Wiles qui implique entre autres le dernier théorème de Fermat. La fonction L de f_E nous apporte divers informations sur $E/\mathbb{Q}$ et c'est ce sur quoi la conjecture de Birch et Swinnerton-Dyer (BSD) porte. L'énoncé complet de cette conjecture requiert beaucoup plus de notions que ce que nous avons introduit jusqu'à présent, mais de façon (très) simplifié, elle affirme que $E(\mathbb{Q})$ est fini si et seulement si $L(f_E,1) \neq 0$. L'ordre à laquelle $L(f_E,s)$ s'annihile en $s = 1$ porte le nom de *rang analytique de E* et donc cette conjecture affirme que

$E(\mathbb{Q})$ est fini exactement lorsque le rang analytique de E est nul. L'article de Zagier [16] présente une excellente introduction à BSD et explique les travaux de Gross et Zagier visant à prouver cette conjecture. L'énoncé complet n'a toujours pas été démontré, malgré des progrès importants dans les dernières décennies, mais divers résultats partiels/connexes sont connus (voir [16]).

Remarque 4. Le théorème de Wiles ne traite que des forme primitive à coefficients entiers. En général, les autres formes primitives ayant leurs coefficients dans des extensions de $\mathbb{Q}$ sont plutôt en relation avec des *variétés abéliennes* qui peuvent être perçues comme des généralisations de courbes elliptiques. Ces structures algébriques possèdent aussi une fonction L dont la valeur en $s = 1$ semble encore être connectée avec le nombre de points rationnels qu'elles détiennent. Par conséquent, même si pour plusieurs nombres premiers p, il n'existe aucune courbe elliptique sur $\mathbb{Q}$ de conducteur p, les formes primitives de $S_2(p)$ sont tout de même intéressantes.

Rappelons que toute forme primitive $f \in S_2(p)$ fait partie d'un certain sous-espace $S_2(p)^{\pm}$ où le signe exact du $\pm$ dépend de la valeur propre de f pour W_p. Dans [4], on prouve que la fonction L de f satisfait l'équation fonctionnel

$$p^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s) = \pm p^{(2-s)/2}(2\pi)^{-(2-s)}\Gamma(2-s)L(f,2-s)$$

On voit alors immédiatement qu'en $s = 1$, cette équation devient $L(f,1) = \pm L(f,1)$ et donc, selon BSD, les seules courbes elliptiques E de conducteur p ayant un nombre fini de points rationnels ont $f_E \in S_2(p)^+$. Le vecteur associé dans $\mathcal{P}^0_{\mathbb{Q}}$ est alors aussi situé dans $\mathcal{P}^{0,+}_{\mathbb{Q}}$.

On peut généraliser la fonction $L(f_E, K, s)$ pour des courbes elliptiques E définies sur des corps de nombres K. Dans ce cas, la valeur de $L(f_E, K, s)$ en $s = 1$ est reliée à la cardinalité de $E(K)$. En particulier, on a $L(f_E, \mathbb{Q}(\sqrt{D}), s) = L(f_E, s)L(f_E \otimes \varepsilon_D, s)$. Alors, la formule de Gross (1) énoncée ci-dessus indique que $E(\mathbb{Q}(\sqrt{D}))$ est fini si et seulement si $\langle \gamma_D^f, \gamma_D^f \rangle \neq 0$. Étant donné que le produit scalaire $\langle \cdot, \cdot \rangle$ est défini positif, on a que $\langle \gamma_D^f, \gamma_D^f \rangle = 0$ exactement lorsque $\gamma_D^f = 0$, soit que γ_D^0 est orthogonal à la $\mathbb{Q}$-droite $\mathbf{1}_f(\mathcal{P}^0_{\mathbb{Q}})$.

Remarque 5. En jumelant toutes ses observations, on découvre alors qu'une compréhension approfondie du positionnement de γ_D^0 dans $\mathcal{P}^{0,+}_{\mathbb{Q}}$ peut indiquer exactement les courbes elliptiques de conducteurs p ayant un nombre fini de points rationnels, mais un nombre infini de points définis sur $\mathbb{Q}(\sqrt{D})$. La section suivante est motivé exactement par ce sujet.

3 Quotients de Gross $\mathbf{J_D}$ de $\mathbf{J_0(p)}$

3.1 Groupe de Mordell-Weil de $\mathbf{J_D}$

Considérons l'homorphisme de $\mathbb{T}$-modules $\mathbb{T} \to \mathcal{P}^0_{\mathbb{Q}}$ qui à t associe à $t\gamma^0_D$ et notons son noyau par I_D. Soit $I_D J_0(p)$ la sous-variété abélienne de $J_0(p)$ engendrée par $\{tx \ : \ t \in I_D, x \in J_0(p)\}$. Le quotient de $J_0(p)$ par cette sous variété $J_D := J_0(p)/I_D J_0(p)$ est une variété abélienne sur $\mathbb{Q}$ et sera dénommé le *D-ième quotient de Gross.*

Étant donné que $\mathbb{T}$ est un anneau commutatif, on remarque immédiatement que I_D est exactement l'idéal de $\mathbb{T}$ qui annihile $\mathbb{T}\gamma^0_D$, le sous-espace de $\mathcal{P}^0_{\mathbb{Q}}$ engendré par $\{t\gamma^0_D : t \in \mathbb{T}\}$. De plus, $\mathbb{T}$ est semi-simple, alors on peut considérer I_0 l'idéal supplémentaire de I_D, soit l'idéal de $\mathbb{T}$ tel que I_0 projette $\mathcal{P}^0_{\mathbb{Q}}$ sur $\mathbb{T}\gamma^0_D$ et qui est maximal pour cette charactéristique. Alors par définition, on observe que $\mathbb{T} = I_0 \oplus I_D$ et que $I_0 I_D = I_D I_0 = 0$.

Étant donné que $S_2(p)$ est aussi un $\mathbb{T}$-module, on peut aussi considérer les sous-espaces $I_0 S_2(p)$ et $I_D S_2(p)$ engendrés par $\{tf : t \in I_0, \ f \in S_2(p)\}$ et $\{tf : t \in I_D, \ f \in S_2(p)\}$ respectivement.

Lemme 1. *Soit p premier, $D < 0$ un discriminant fondamental tel que p est inerte dans $\mathcal{O}_D$ et $I_0 S_2(p)$, $I_D S_2(p)$ comme ci-dessus. Le sous-espace $I_0 S_2(p)$ (resp. $I_D S_2(p)$) est engendré exactement par les formes primitives f de $S_2(p)$ tel que $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$ (resp. $L(f, \mathbb{Q}(\sqrt{D}), 1) = 0$).*

Démonstration. Soit $f \in S_2(p)$ une forme primitive et a_f un vecteur directeur de la $\bar{\mathbb{Q}}$-droite $\mathbf{1}_f(\mathcal{P}^0_{\bar{\mathbb{Q}}})$. Indiquons la valeur propre de f (et par le fait même, de a_f) pour un opérateur $t \in T$ par $\lambda_{f,t} \in \bar{\mathbb{Q}}$.

Supposons que $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$. Dans ce cas, comme nous l'avons mentionné précédemment, l'équation (1) implique que $\langle a_f, \gamma^0_D \rangle \neq 0$. On voit immédiatement que pour tout $t \in I_D$, $\langle t a_f, \gamma^0_D \rangle = \langle a_f, t\gamma^0_D \rangle = \langle a_f, 0 \rangle = 0$. De plus, étant donné que $\mathbb{T} = I_0 \oplus I_D$, on peut décomposer $\mathrm{Id} \in \mathbb{T}$ en tant que $\mathrm{Id} = \mathrm{Id}_0 + \mathrm{Id}_D$, où $\mathrm{Id}_0 \in I_0$ et $\mathrm{Id}_D \in I_D$. On obtient alors $0 \neq \langle a_f, \gamma^0_D \rangle = \langle \mathrm{Id}_0 a_f, \gamma^0_D \rangle + \langle \mathrm{Id}_D a_f, \gamma^0_D \rangle = \langle \mathrm{Id}_0 a_f, \gamma^0_D \rangle$ et donc que $\lambda_{f,\mathrm{Id}_0} a_f = \mathrm{Id}_0 a_f \neq 0$. Alors $\lambda_{f,\mathrm{Id}_0} \neq 0$, ce qui implique que $f = (\lambda_{f,\mathrm{Id}_0})^{-1} \mathrm{Id}_0 f \in I_0 S_2(p)$.

D'un autre côté, supposons que f est une forme primitive de $I_0 S_2(p)$ et donc que $a_f \in I_0 \mathcal{P}^0_{\bar{\mathbb{Q}}}$. Par constuction, puisque $I_D I_0 = I_0 I_D = \{0\}$, il est alors évident que a_f est annihilé par tout $t \in I_D$. Autrement dit, par rapport à la décomposition orthogonale $\mathcal{P}^0_{\bar{\mathbb{Q}}} = \mathbb{T}_{\bar{\mathbb{Q}}}\gamma^0_D \oplus I_D \mathcal{P}^0_{\bar{\mathbb{Q}}}$, on sait que a_f est perpendiculaire au deuxième terme.

Par contre, a_f est évidemment non nul, donc a_f ne peut être perpendiculaire au premier terme aussi, i.e. il existe $t \in \mathbb{T}_{\bar{\mathbb{Q}}}$ tel que $\langle t\gamma^0_D, a_f \rangle \neq 0$. On en conclut alors que $\langle t\gamma^0_D, a_f \rangle = \langle \gamma^0_D, t a_f \rangle = \langle \gamma^0_D, \lambda_{f,t} a_f \rangle = \lambda_{f,t} \langle \gamma^0_D, a_f \rangle$ et donc $\langle \gamma^0_D, a_f \rangle \neq 0$, i.e. $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$. Le tout confirme que $I_0 S_2(p)$ est engendré exactement par les formes primitives f tel que $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$.

Finalement, en utilisant le fait que $\mathbb{T} = I_0 \oplus I_D$ et que $I_D I_0 = I_0 I_D = 0$, on vérifie aisément que $S_2(p)$ se partage en somme directe $I_0 S_2(p) \oplus I_D S_2(p)$ où cette décomposition est orthogonale. Étant donné que pour toutes les formes primitives de $S_2(p)$ sont perpendiculaires entre elles et forment une base de $S_2(p)$, on obtient que toutes les autres formes primitives tel que $L(f, \mathbb{Q}(\sqrt{D}), 1) = 0$ engendrent exactement $I_D S_2(p)$, ce qui conclut la démonstration. $\square$

Proposition 1. *Le groupe de Mordell-Weil sur $\mathbb{Q}(\sqrt{D})$ de $\mathrm{J_D}$ est fini.*

Démonstration. Comme $\mathbb{T}$ est semi-simple, on peut décomposer I_0 en sous-$\mathbb{T}$-modules irréductibles, disons $I_0 = \oplus_{k=1}^{r} I_{0,k}$. On peut alors définir $I_{D,k} := I_D \oplus \left(\bigoplus_{l \neq k} I_{0,k}\right)$ et $J_{D,k} := J_0(p)/I_{D,k}J_0(p)$. On a alors naturellement l'isogénie $J_D \to \prod_{k=1}^{r} J_{D,k}$. Comme cette isogénie est définie sur $\mathbb{Q}$, on voit que $J_D(\mathbb{Q}(\sqrt{D}))$ est fini si chacun des $J_{D,k}(\mathbb{Q}(\sqrt{D}))$ est fini.

On peut alors utiliser les travaux de Kolyvagin et Logachev [9] (basé sur les résultats de Gross et Zagier [8]) qui démontre que si $L(J_{D,k}, \mathbb{Q}(\sqrt{D}), 1) = 0$, alors $J_{D,k}(\mathbb{Q}(\sqrt{D}))$ est fini. De plus, les travaux de Carayol [2] prouve que $L(J_{D,k}, \mathbb{Q}(\sqrt{D}), s) = \prod L(f, \mathbb{Q}(\sqrt{D}), s)$, où f parcout les formes primitives de $I_{0,k}S_2(p)$.

En jumelant ces deux résultats, on trouve alors que $J_D(\mathbb{Q}(\sqrt{D}))$ est fini si $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$ pour toute forme primitive $f \in \oplus_{k=1}^{r} I_{0,k}S_2(p) = I_0S_2(p)$. Le lemme 1 indique exactement que cette dernière condition est vraie, ce qui conclut la démonstration. □

Cette proposition est sensiblement différentes des autres résultats que nous allons prouver ci-dessous. Cependant, il s'agit d'un élément clé de la preuve de Merel. Dans son article, il démontre que la proposition précédente implique l'énoncé suivant.

Théorème 3. *Soit $d > 1$ un entier, p un nombre premier et $D < 0$ un discriminant fondamental tel que p est inerte dans $\mathcal{O}_D$. Si $T_1\gamma_D^0, \ldots, T_d\gamma_D^0$ sont linéairement indépendants dans $\mathcal{P}_{\mathbb{Q}}^0$ et que $p \geq d^{3d^2}$, alors il n'existe aucune courbe elliptique E, définie sur un corps de nombres K de degré d, possédant un point de torsion $P \in E(K)$ d'ordre p.*

Dans son article, Merel travaille en fait avec un énoncé quelque peu différent, mais sa preuve peut aisément être adaptée à notre situation. Il prouve aussi, en utilisant les travaux de Faltings et Frey (voir [5], [6]), que ce théorème implique qu'il existe une borne $b(d) \geq 1$ tel que pour toute courbe elliptique E/K, où K est un corps de nombre de degré d, si $P \in E(K)$ est un point de torsion, alors l'ordre de P est au plus $b(d)$. Autrement dit, trouver une borne pour les points d'ordre premier suffit pour prouver l'existence d'une borne pour tous les points de torsion.

Pour établir l'indépendance linéaire de $T_1\gamma_D^0$, …, $T_d\gamma_D^0$, il est alors essentiel de comprendre le comportement de γ_D^0 sous l'action de $\mathbb{T}$. Malgré le fait que la section suivante ne parvient pas à déterminer ce comportement, elle étudie la structure de J_D pour essayer d'établir une meilleur compréhension de la situation. Par le fait même, on y découvre certains résultats sur le rang analytique sur $\mathbb{Q}(\sqrt{D})$ des courbes elliptiques.

3.2 Propriétés de $\mathbf{J_D}$

Dans la section précédente, on a démontré que $J_D(\mathbb{Q}(\sqrt{D}))$ est fini en utilisant le fait que $I_0S_2(p)$ ne contient que des formes primitives f tel que $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$. En fait, étant donné que $I_0S_2(p)$ contient toutes les formes primitives satisfaisant cette propriété, on a que J_D est le plus large quotient de $J_0(p)$ ayant un nombre fini de points sur $\mathbb{Q}(\sqrt{D})$. En comparaison, dans [10], Merel parvient à construire un différent quotient, appelé le *quotient d'enroulement*, qui est essentiellement le plus large ayant un nombre fini de points définis sur $\mathbb{Q}$. Il substitue $I_0S_2(p)$ par le sous-espace vectoriel de $S_2(p)$ contenant exactement les formes primitives $f \in S_2(p)$ tel que $L(f, 1) \neq 0$.

Évidemment, puisque $J_D(\mathbb{Q}(\sqrt{D}))$ est fini, il s'en suit que $J_D(\mathbb{Q})$ est aussi fini. En théorie, cela porte à croire que la dimension, en tant que variété sur $\mathbb{Q}$, du quotient d'enroulement est plus élevé que celle J_D. Par contre, en réalité, il semblerait que pour un nombre considérable de discriminants D, J_D est identique au quotient de Merel. Pour voir cela, il suffit de remarquer que pour certains discriminants D, $L(f, 1) \neq 0$ si et seulement si $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$. Tentons d'analyser les données suivantes rapidement.

Table 2: Valeurs de $\langle \gamma_D^f, \gamma_D^f \rangle$ pour toutes les formes primitives $f \in S_2(73)$ et divers discriminants D.

Développement à l'infini de f	D	$\langle \gamma_D^f, \gamma_D^f \rangle$
$f_1 := q + q^2 + \ldots$	-424	$2/3$
	-427	0
	-431	$3/2$
	-443	$1/6$
$f_2 := q - \frac{t^3+3t^2-8t-12}{4}q^2 + \ldots$	-424	$-(17t^3 + 51t^2 - 136t - 300)/78$
	-427	$-(2t^3 + 6t^2 - 16t - 46)/39$
	-431	0
	-443	$(6t^3 + 18t^2 - 48t - 300)/39$
$f_3 := q + \frac{t^3+3t^2-8t-8}{4}q^2 + \ldots$	-424	$(17t^3 + 51t^2 - 136t - 40)/78$
	-427	$(2t^3 + 6t^2 - 16t + 6)/39$
	-431	0
	-443	$-(6t^3 + 18t^2 - 48t - 112)/39$
$f_4 := q - \frac{t^3+3t^2-4t}{4}q^2 + \ldots$	-424	0
	-427	0
	-431	0
	-443	0
$f_5 := q + \frac{t^3+3t^2-4t-12}{4}q^2 + \ldots$	-424	0
	-427	0
	-431	0
	-443	0

Note : Le polynôme minimal de t sur $\mathbb{Q}$ est $X^4 + 4X^3 - 3X^2 - 14X - 4$

Rappelons que $L(f, \mathbb{Q}(\sqrt{D}), 1) = L(f,1)L(f \otimes \varepsilon_D, 1)$. Il est bien connu que les fonctions L des deux dernières formes primitives f_4 et f_5 indiquer sur ce tableau s'annulent en $s = 1$, ce qui explique qu'en général, on aura toujours $\langle \gamma_D^{f_4}, \gamma_D^{f_4} \rangle = \langle \gamma_D^{f_5}, \gamma_D^{f_5} \rangle = 0$. D'un autre côté, les trois autres formes primitives f_1, f_2 et f_3 ont chacunes au moins un discriminant D tel que $\langle \gamma_D^{f_i}, \gamma_D^{f_i} \rangle \neq 0$, donc $L(f_1, 1)$, $L(f_2, 1)$ et $L(f_3, 1)$ sont tous non nuls. Dans [10], Merel considère alors exactement le sous-espace engendré par ces trois formes paraboliques. Par contre, dans notre cas, si on prend $D = -431$, le tableau ci-dessus indique que $L(f_1, \mathbb{Q}(\sqrt{-431}), 1) \neq 0$ alors que pour f_2 et f_3, leurs fonctions L sur $\mathbb{Q}(\sqrt{-431})$ sont nulles. Par conséquent, J_{-431} est strictement plus petit que le quotient d'enroulement. Le même raisonnement s'applique pour $D = -427$.

D'un autre côté, posons $D = -424$ (ou même $D = -443$). On voit que $L(f_i, \mathbb{Q}(\sqrt{-424}), 1) \neq 0$ pour $i = 1, 2, 3$. Dans ce cas, on obtient que $L(f, 1) \neq 0$ si et seulement si $L(f, \mathbb{Q}(\sqrt{-424}), 1) \neq 0$ et, comme mentionné auparavant, cela montre que J_{-424} est identique au quotient d'enroulement. Cela n'a rien de particulier à ces deux discriminants ni au cas $p = 73$. Le tableau ci-dessus ne présente que ces quatres cas, mais en calculant ces quantités pour tous discriminants $-100\ 000 < D < 0$, on voit aisément que la majorité des cas se comporte comme $D = -424$ et -443. L'auteur encourage aussi le lecteur à construire le même tableau que ci-dessus pour d'autres nombres premiers. On remarque aisément qu'il y a plusieurs discriminants pour lesquels $\langle \gamma_D^f, \gamma_D^f \rangle \neq 0$ pour toute forme primitive tel que $L(f, 1) \neq 0$. Ces derniers commentaires ne tentent pas de constituer une preuve rigoureuse, mais plutôt une observation immédiate.

Remarque 6. Notons que si p n'est pas inerte dans $\mathcal{O}_D$, on peut prouver que $L(f \otimes \varepsilon_D, 1) = 0$. Par conséquent, pour toute forme primitive f, $L(f, \mathbb{Q}(\sqrt{D}), 1)) = 0$ même si possiblement, certaines d'entre elles ont $L(f, 1) \neq 0$. Pour ces discriminants D, on obtient donc que J_D est trivial. En terme de distribution, il est connu que p est inerte dans environ 50% des discriminants fondamentaux, alors environ la moitié des quotients J_D sont triviaux et l'autre moitié est plus intéressante. La discussion du paragraphe précédent tente de convaincre que, pour un nombre considérable de discriminants D dans la seconde moitié, J_D est identique au quotient d'enroulement de Merel. Malgré le fait que nous n'avons pas d'énoncer précis décrivant l'existence d'un tel disciminant, nous pouvons tout de même prouver les résultats suivants.

Proposition 2. *Soit p premier et $D < 0$, un discriminant fondamental tel que p est inerte dans $\mathcal{O}_D$. Le D-ième quotient de Gross J_D est non-trivial si et seulement si $\gamma_D^0 \neq 0$, soit que γ_D n'est pas un multiple de* Eis.

Démonstration. Évidemment si $\gamma_D^0 = 0$, on a par définition $I_D = \mathbb{T}$. Il s'en suit que $I_D J_0(p) = \mathbb{T} J_0(p) = J_0(p)$ et donc notre quotient J_D équivaut $J_0(p)/I_D J_0(p) = \{0\}$, ce qui prouve une direction de notre énoncé.

D'un autre côté, supposons que $\gamma_D^0 \neq 0$. Rappelons que le Théorème 1 énonce que pour $p > 3$ premier, $\mathcal{P}_{\mathbb{C}}^0$ est isomorphe à $S_2(p)$ en tant que $\mathbb{T}_{\mathbb{C}}$-module. De plus, on peut prouver que $S_2(p)$ est isomorphe à $T_0(J_0(p))$, soit l'espace tangent de $J_0(p)$ à l'origine, en tant que $\mathbb{T}_{\mathbb{C}}$-module encore une fois. Alors, on obtient de plus les isomorphismes suivants.

$$T_0(J_D) \cong T_0(J_0(p))/I_D T_0(J_0(p)) \cong \mathcal{P}_{\mathbb{C}}^0 / I_D \mathcal{P}_{\mathbb{C}}^0$$

Il suffit alors de démontrer que $\mathcal{P}_{\mathbb{C}}^0 / I_D \mathcal{P}_{\mathbb{C}}^0 \neq \{0\}$. Il est en fait assez facile d'observer que $\gamma_D^0 \notin I_D \mathcal{P}_{\mathbb{C}}^0$. Autrement, on pourrait écrire $\gamma_D^0 = \sum_{i=1}^n t_i x_i$ pour certain $t_i \in I_D$, $x_i \in \mathcal{P}_{\mathbb{C}}^0$.

Dans ce cas, comme les opérateurs t_i sont auto-adjoints pour $\langle \cdot, \cdot \rangle$, on obtient

$$\langle \gamma_D^0, \gamma_D^0 \rangle = \sum_{i=1}^{n} \langle \gamma_D^0, t_i x_i \rangle = \sum_{i=1}^{n} \langle t_i \gamma_D^0, x_i \rangle = \sum_{i=1}^{n} \langle 0, x_i \rangle = 0$$

Par contre, comme ce produit scalaire est défini positif, cela implique que $\gamma_D^0 = 0$, contradiction. On a donc que l'espace tangent de J_D à l'origine est non-nul et donc que J_D est non-trivial. □

Corollaire 1. *Soit p et D comme ci-dessus. Si p = 5, 7 ou 13, le D-ième quotient de Gross J_D est nul pour tout D. Pour tout autre premier p, soit η l'exact numérateur de $\frac{p-1}{12}$ et h_D le nombre de classe de $\mathcal{O}_D$. Si η ne divise pas h_D, alors le D-ième quotient de Gross J_D est non-trivial.*

Démonstration. Premièrement, pour $p = 5$, 7, ou 13, on sait que $\text{genre}(X_0(p)) = 0$, et donc que $\mathcal{P}_{\mathbb{Q}}$ est uni-dimensionel. Alors, γ_D est necessairement sur la même $\mathbb{Q}$-droite que Eis, ce qui prouve notre premiere assertion.

À partir de maintenant, supposons que $p \neq 5$, 7 ou 13 et que J_D est nul. Rappelons que $\text{Eis} = \sum_{i=0}^{g} \frac{1}{w_i}[E_i]$ est de degré $\frac{p-1}{12} = \frac{\eta}{\delta}$, où δ est l'exact dénominateur de $\frac{p-1}{12}$. Alors, en utilisant la proposition précédente, on sait que $\gamma_D = \frac{12}{p-1} \deg(\gamma_D)\text{Eis} = \frac{\delta}{\eta} \deg(\gamma_D)\text{Eis}$. De plus, dans [7], Gross prouve que $\deg(\gamma_D) = \frac{1}{u(D)} h_D$, où $u(D) = \frac{|Pic(\mathcal{O}_D)^\times|}{2}$. Notons que ce fait est immédiat d'après notre description dans la section 2.2 de l'algorithme qui calcule γ_D.

Pour $D \neq -3, -4$, nous avons $u(D) = 1$ et donc $\gamma_D = \frac{\delta h_D}{\eta}\text{Eis}$ et les coefficients de γ_D sont tous entiers. Étant donné que les coefficients de Eis ont tous 1 comme numérateur et que $\gcd(\eta, \delta) = 1$, il s'en suit que η divise h_D, comme désiré.

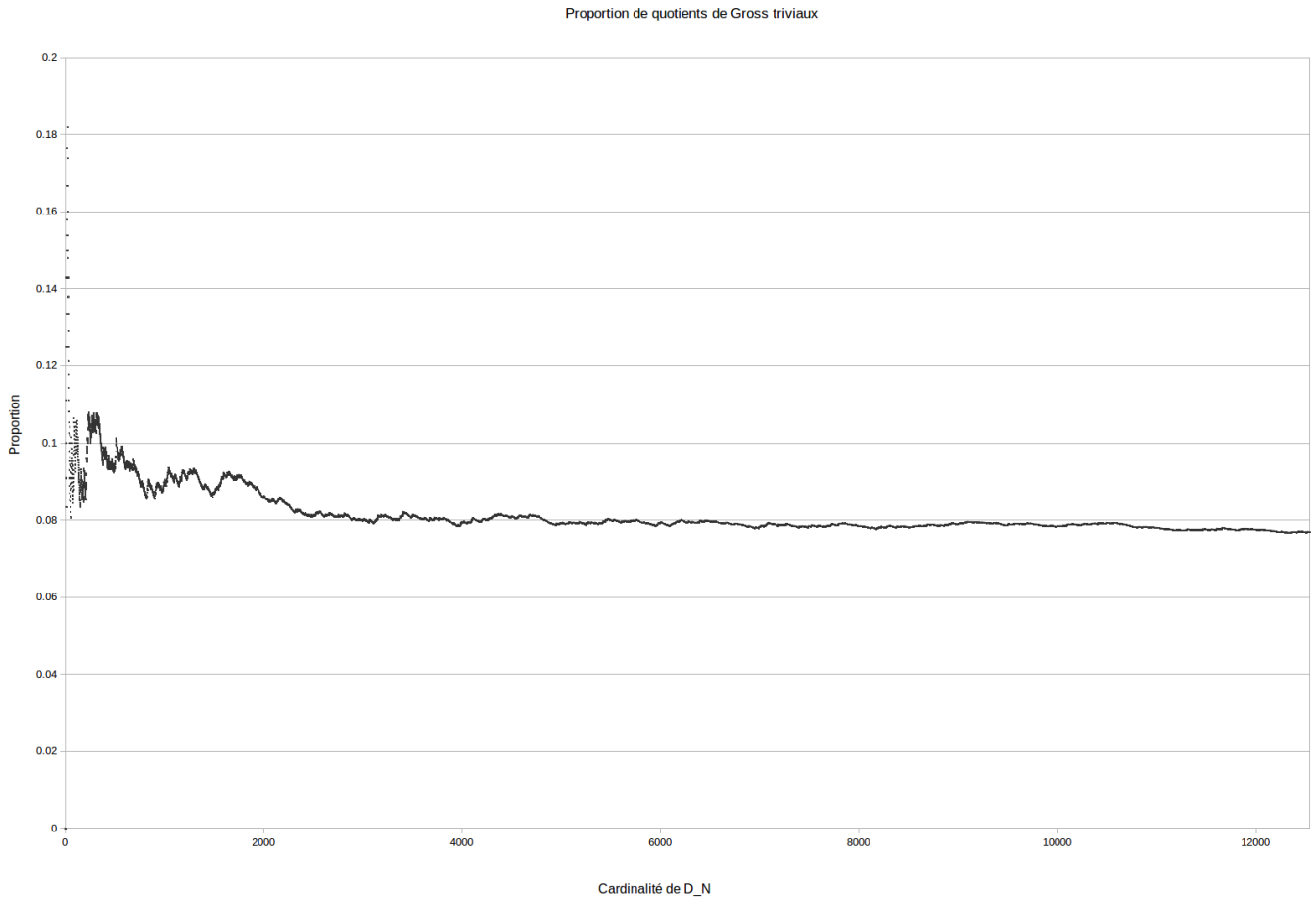
Pour $D = -3$ ou -4, on peut en fait prouver que J_D n'est jamais trivial, ce qui est en accord avec notre énoncé. Supposons que p est inerte dans $\mathcal{O}_{-3}$. Comme $u(-3) = 3$ et $h_{-3} = 1$, on trouve $\deg(\gamma_{-3}) = \frac{1}{3}$. Par construction des éléments de Gross, nous obtenons alors $\gamma_{-3} = \frac{1}{3}[E_i]$ pour un certain $i = 0, \ldots, g$. Il est cependant évident que cet élément de $\mathcal{P}_{\mathbb{Q}}$ ne se retrouve pas sur la $\mathbb{Q}$-droite engendrée par $\text{Eis} = \sum_{i=0}^{g} \frac{1}{w_i}[E_i]$ car $g \geq 2$ pour $p \neq 5$, 7 ou 13. Le cas $D = -4$ est identique, sauf que $u(-4) = 2$, ce qui termine la démonstration. □

Corollaire 2. *Soit D comme ci-dessus. Il n'existe qu'un nombre fini de nombre premiers p pour lesquels le D-ième quotient de Gross J_D de $J_0(p)$ est trivial.*

Tentons d'étudier ces résultats concrètement. Plus précisément, posons $p = 11$ et étudions le comportement des quotients de Gross de $J_0(11)$. Prenons une borne $N > 0$ et posons $\mathcal{D}_N$ l'ensemble des discriminants premiers $D < 0$ tel que p est inerte dans $\mathcal{O}_D$ et $|D| < N$. Tentons d'étudier la convergence du ratio

$$\frac{\text{Nombre de quotients } J_D \text{ triviaux pour } D \in \mathcal{D}_N}{|\mathcal{D}_N|}$$

Le graphe suivant démontre la tendance de ce ratio pour N allant de 2 à 90 000.



Pour $N = 90\ 000$, l'ensemble $\mathcal{D}_N$ contient 12 539 discriminants et la proportion se trouve à environ 7.688%. Ce graphique est naturellement lié à la conjecture de Goldfeld.

En effet, observons que $S_2(11)$ est uni-dimensionel, alors il n'existe qu'une unique forme parabolique primitive $f \in S_2(11)$. Alors, pour un discriminant fondamental D, J_D est trivial si et seulement si $\gamma_D^f = 0$. En utilisant la formule de Gross (1), on voit que cela se produit exactement lorsque $L(f \otimes \varepsilon_D, 1) = 0$, étant donné qu'il est bien connu que $L(f, 1) \neq 0$. La conjecture de Goldfeld prédit que 50% des torsions par des charactères quadratiques ε_D produiront des formes paraboliques $f \otimes \varepsilon_D$ dont la fonction L s'annule en $s = 1$, et l'autre 50% auront une fonction L non-nulle en $s = 1$.

Comme mentionné précédemment, il est bien connu que si p n'est pas inerte dans $\mathcal{O}_D$, alors $L(f \otimes \varepsilon_D, 1) = 0$. On sait aussi qu'en terme de distribution, p est inerte dans $\mathcal{O}_D$ pour 50% des discriminants fondamentaux. Alors, comme nous ne considérons que les discriminants D tel que p est inerte dans $\mathcal{O}_D$, la théorie indique que la probabilité qu'un de nos quotient de Gross de $J_0(11)$ soit trivial est de 0%. Il est alors surprenant d'observer un proportion aussi haute que 7.688%. On observe une proportion similaire avec $p = 37$, où le pourcentage est environ à 10% pour $N = 100\ 000$.

Cependant, plusieurs expériences similaires semblent toujours avoir une tendance plus élevée que la théorie le prédit. On raconte que Stein a eu à travailler plusieurs années pour aquérir une base de données suffisament large et observer une proportion approchant 50% en tentant de vérifier la conjecture de Goldfeld directement. Initialement, ses résultats étaient au-delà de 50% et il a fallu étudier le comportement de courbes elliptiques à conducteur incroyablement large pour que la tendance débute à diminuer.

Pour conclure, les résultats suivant donnent une interprétation des corollaires ci-dessus en termes du rang analytiques sur $\mathbb{Q}(\sqrt{D})$ de courbes elliptiques définies sur $\mathbb{Q}$.

Proposition 3. *Soit $p \neq 5$, 7 ou 13 premier et $D < 0$, un discriminant premier tel que p est inerte dans O_D. Soit η l'exact numérateur de $\frac{p-1}{12}$ et h_D le nombre de classe de $\mathcal{O}_D$. Si η ne divise pas h_D, alors il existe une forme primitive $f \in S_2(p)$ tel que $L(f, \mathbb{Q}(\sqrt{D}), 1) \neq 0$.*

Démonstration. Cet énoncé suit immédiatement en utilisant le corollaire 1, le fait que la non-trivialité de J_D implique que $I_0 S_2(p) \neq \{0\}$ et le lemme 1. □

Malheureusement, on ne peut garantir que cette forme primitive possède un dévoleppement à l'infini à coefficients entiers, donc il se peut que cette forme primitive ne soit pas associée à une courbe elliptique. Cependant, comme mentionné auparavant, ce résultat donne une condition simple pour étudier le comportement de variétés abéliennes en général sur des corps quadratiques imaginaires.

Proposition 4. *Soit p premier et $D < 0$ comme ci-dessus. Soit $E/\mathbb{Q}$ est une courbe elliptique de conducteur p et f_E est la forme parabolique associée. Si le rang analytique de E sur $\mathbb{Q}(\sqrt{D})$ est nul, alors la $\bar{\mathbb{Q}}$-droite $\mathbf{1}_{f_E}(\mathcal{P}^0_{\bar{\mathbb{Q}}})$ se retrouve dans $\mathbb{T}_{\bar{\mathbb{Q}}}\gamma^0_D$ qui est lui-même un sous-espace de $\mathcal{P}^{0,+}_{\bar{\mathbb{Q}}}$.*

Démonstration. Si $L(f_E, \mathbb{Q}(\sqrt{D}), 1) \neq 0$, alors $f_E \in I_0 S_2(p)$, i.e. a_{f_E} se retrouve dans $I_0\mathcal{P}^0_{\bar{\mathbb{Q}}} = \mathbb{T}_{\bar{\mathbb{Q}}}\gamma^0_D$, où a_{f_E} est un vecteur directeur de $\mathbf{1}_{f_E}(\mathcal{P}^0_{\bar{\mathbb{Q}}})$. Le fait que $I_0\mathcal{P}^0_{\bar{\mathbb{Q}}} = \mathbb{T}_{\bar{\mathbb{Q}}}\gamma^D_0$ est un sous-espace de $\mathcal{P}^{0,+}_{\bar{\mathbb{Q}}}$ est immédiat, en utilisant le lemme 1 et le signe de l'équation fonctionnel des fonctions L. □

Étant donné que la version de la conjecture de BSD sur des corps quadratiques imaginaires a été démontrée, cette proposition donne une condition nécessaire pour que $E(\mathbb{Q}(\sqrt{D}))$ soit fini en terme du positionnement de γ^0_D dans $\mathcal{P}^0_{\bar{\mathbb{Q}}}$. Par contre, trouver une condition suffisante semble constituer une tâche beaucoup plus subtile. De nouveau, on voit qu'une compréhension plus en profondeur de l'action de $\mathbb{T}$ sur γ^0_D est nécessaire pour aller plus loin.

Remerciements

J'aimerais remercier Prof. Henri Darmon et Dr. Jan Vonk, mes superviseurs pour ce projet, pour tout le temps qu'ils ont dévoué pour m'aider dans ma recherche et la rédaction de ce document et pour répondre à mes questions incessantes. De plus, en tant que récipiendaire d'une bourse de recherche de 1er cycle CRSNG, j'aimerais remercier Prof. Darmon, le département de mathématiques de l'université McGill et le CRSNG pour leur support financier.

References

[1] Atkin, A.O.L and Lehner, J. *Hecke operators on* $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[2] Carayol, H. *Sur les representations l-adiques associees aux formes modulaires de Hilbert. Ann. Sci. de l'ENS 19*, pages 409–468, 1986.

[3] Chevyrev, I. and Galbraith, S. D. *Constructing supersingular elliptic curves with a given endomorphism ring. LMS Journal of Computation and Mathematics*, 17:71–91, 2014.

[4] Diamond, F. and Shurman, J. *A First Course in Modular Forms.* Springer, 2000.

[5] Faltings, G. *The general case of S. Lang's conjecture. Barsotti Symposium in Algebraic Geometry*, June. 1991.

[6] Frey, G. *Curves with infinitely many points of fixed degree. Israel Journal of Mathematics*, 1994.

[7] Gross, B. H. *Heights and special values of L-series. CMS Conf. Proc. 7*, 1986.

[8] Gross, B. H. and Zagier, D. B. *Heegner points and derivatives of L-series. Invent. Math.*, 84:225–320, 1986.

[9] Kolyvagin, V. A. and Logachev, D. Y. *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. Leningrad Math. J. 1* n^0 *5*, pages 1229–1253, 1989.

[10] Merel, L. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math.*, 124(1-3):437–449, 1996.

[11] Mestre, J. F. *La méthode des graphes. Exemples et applications. Taniguchi Symp., Kyoto*, 2004.

[12] Rebolledo, M. *Module supersingulier et homologie des courbes modulaires. Journal of Number Theory*, 121:234–264, 2006.

[13] Silverman, J. H. *The Arithmetic of Elliptic Curves.* Brown University, 1986.

[14] Voight, J. *Quaternion Algebra.* À paraitre.

[15] Voight, J. *Identifying the Matrix Ring : Algorithms for Quaternion Algebras and Quadratic Forms. ArXiv e-prints*, April 2010.

[16] Zagier, D. B. *L-series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss. Notices Amer. Math. Soc. 31*, (7):739–743, 1984.