

N^o d'ordre : 2628.

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

PAR **Christophe DELAUNAY**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

Formes modulaires et invariants de courbes elliptiques définies sur \mathbb{Q}

Soutenue le 13 décembre 2002

Après avis de :

MM	J. CREMONA	Professeur	University of Nottingham	Rapporteurs
	N. ELKIES	Professeur	Harvard University	
	D. ZAGIER	Professeur	Max-Planck-Institut für Math. et Collège de France	

Devant la commission d'examen formée de :

MM	J. M. COUVEIGNES	Professeur	Université Toulouse II	Président
	E. KOWALSKI	Professeur	Université Bordeaux I	Rapporteur
	H. COHEN	Professeur	Université Bordeaux I	Directeur de thèse
	J. CREMONA	Professeur	University of Nottingham	Examineur
	M. OLIVIER	Professeur	Université Bordeaux I	Directeur de thèse
	D. ZAGIER	Professeur	Max-Planck-Institut für Math. et Collège de France	Examineur

C'est un plaisir de pouvoir exprimer ici ma gratitude envers toutes les personnes qui ont contribué de façon directe ou indirecte à l'élaboration de ce travail.

Tout d'abord, je remercie mes deux directeurs de thèse, Henri Cohen et Michel Olivier. Ils m'ont laissé une grande liberté dans mes activités de recherche tout en me donnant, avec disponibilité, les moyens nécessaires aussi bien scientifiques que matériels. Je suis sensible aux nombreux conseils et commentaires qu'ils m'ont donnés tout au long de ces années.

Je remercie les professeurs John Cremona, Noam Elkies et Don Zagier, qui ont tous les trois accepté de rapporter cette thèse, pourtant rédigée en français. Je suis heureux d'avoir pu bénéficier, lors de nos échanges, de leurs remarques toujours très constructives.

Je suis, de plus, enchanté de la présence de John Cremona et de Don Zagier parmi les membres du jury.

Jean-Marc Couveignes, par l'intérêt qu'il m'a porté et par les questions qu'il m'a posées, a motivé une grande partie de ces travaux. Je l'en remercie chaleureusement et je suis flatté qu'il ait présidé ce jury.

Je remercie aussi Emmanuel Kowalski pour sa grande disponibilité, ses conseils et ses remarques. Je suis très heureux de sa participation au jury.

Je remercie, plus généralement, tous les chercheurs qui m'ont aidé ou qui ont eu la gentillesse de me consacrer du temps. J'exprime toute ma reconnaissance envers les membres du laboratoire A2X pour leur accueil chaleureux et propice au travail.

Par l'intermédiaire de Véronique Saint-Martin, je remercie tout le personnel non-chercheur dont le travail est indispensable au bon fonctionnement de l'institut.

Bien sûr, je remercie tous mes amis doctorants ou déjà docteurs dont la liste ne cesse de s'allonger et qui est trop longue pour être donnée ici de façon exhaustive. En vrac : Christophe, David, Jean-Christophe, Olivier, Sébastien, Stéphane, ... J'ai une pensée toute particulière pour Bill, Samy et Sylvain qui m'ont beaucoup apporté tout au long de cette thèse.

Je remercie ma compagne de tous les jours, Florence, pour les joies qu'elle m'apporte et pour tout le soutien qu'elle m'a donné durant ce long travail. Le hasard a voulu que ma soutenance ait lieu le jour même de son anniversaire.

Je remercie, bien sûr, ma famille, mes proches et surtout mes formidables parents pour leurs encouragements et pour toutes ces choses qu'ils m'ont données sans compter.

Je remercie également Frédéric, mon cher ami d'enfance et Francois pour toutes ces compétitions amicales qui nous rassemblent si souvent.

Pour terminer, je voudrais présenter mes excuses à toutes les personnes que j'ai oubliées de citer ici. J'espère qu'elles me le pardonneront un jour...

Table des matières

Remerciements	3
Table des Matières	3
Introduction	9
L'espace $X_0(N)$	10
Formes Modulaires	11
Courbes Elliptiques Modulaires	13
Revêtement Modulaire	15
Description de φ	15
Calcul de φ aux pointes	16
Calcul de φ en $\tau \in \mathbb{H}$	16
Plan de la thèse	17
I Points de Heegner	19
I.1 Définitions et propriétés	19
I.1.1 Points de Heegner	19
I.1.2 Premières propriétés	20
I.2 Formules de Gross-Zagier	23
I.2.1 Tordues quadratiques	23
I.2.2 Le cas classique	24
I.2.3 Le cas général	25
I.3 Calculs explicites des points de Heegner	26
I.3.1 Méthode	26
I.3.2 Exemples	28
1 Un générateur compliqué	28
2 Un conducteur élevé	29
3 Un groupe III non trivial	29
4 Nombres congruents	30
I.4 Autour des cubiques de Sylvester	31

II Degré du revêtement modulaire	35
II.1 Introduction	35
II.2 Utilisation des “M-symboles”	36
II.2.1 Notations	36
II.2.2 Formule pour le produit scalaire	37
II.3 Utilisation des séries L	39
II.3.1 Le carré symétrique imprimitif	39
II.3.2 Le carré symétrique primitif	41
II.3.3 Calcul de $L(\mathcal{P}^2 f, s)$	43
II.3.4 Ordres de grandeurs	46
III Points de ramification du revêtement modulaire	51
III.1 Points critiques et points de ramification	51
III.1.1 Définitions et motivations	51
1 Contexte général	51
2 Cas du revêtement modulaire	52
III.1.2 Localisation des zéros de f	53
III.1.3 Factorisation par les opérateurs d’Atkin-Lehner	58
III.1.4 Cas d’une courbe de rang 2	65
III.2 Développement de Fourier aux pointes	66
III.2.1 Motivations et notations	66
III.2.2 Pointes unitaires	68
III.2.3 Pointes non unitaires	71
IV Heuristiques sur les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q}	79
IV.1 Motivations et notations	79
IV.2 Groupes de type S	82
IV.3 Séries de Dirichlet et moyennes	85
IV.3.1 Deux séries de Dirichlet	85
IV.3.2 Moyennes	88
IV.3.3 Moyennes sur les p -rangs	92
IV.4 L’assertion fondamentale	94
IV.4.1 Cas du rang 0	95
IV.4.2 Cas du rang 1	95
V Vérification numérique des conjectures de Deligne	99
V.1 Séries L et puissances symétriques	99
V.1.1 Définition et propriétés	99
V.1.2 Conjectures de Deligne	101
V.2 Vérification Numérique des conjectures de Deligne	103
V.2.1 Détermination de la série L	103
V.2.2 Normalisation de c_+ et c_-	105

V.2.3	Exemple	107
V.2.4	“Grandes” puissances symétriques	108
1	Poids 4	108
2	Poids 6	109
3	Poids 8	109
A	Calcul des séries L : méthode alternative	111
A.1	Les fonctions K_j	112
A.2	Relations linéaires	114
B	Résultats numériques concernant la courbe elliptique de conducteur	
	N=389	119
B.1	Liste des points critiques	120
B.2	Le polynôme $P_1(X)$	121
B.3	Les antécédents du points $2G_1$	122
C	Conjecture de Deligne : valeurs numériques	123
C.1	Poids 2	123
C.2	Poids 4	125
C.3	Poids 6	127
C.4	Poids 8	128
C.5	Poids 10	129
	Bibliographie	131
	Résumé	135

Introduction

Les courbes elliptiques représentent un vaste sujet d'étude en théorie des nombres et l'aspect calculatoire y joue un rôle non négligeable. Ce sont, par exemple, des expériences numériques qui ont amené Birch et Swinnerton-Dyer à formuler leur célèbre conjecture. Le théorème de Gross-Zagier, quant à lui, a été motivé en partie par les nombreux calculs de Birch et Stephens sur les points de Heegner. Depuis quelques années, de nombreux algorithmes apparaissent et permettent d'étudier de plus en plus les objets mathématiques attachés aux courbes elliptiques. Dans cette thèse, nous nous intéresserons principalement à l'aspect explicite du revêtement modulaire. Il s'agit du lien qui existe entre :

- Une courbe elliptique définie sur \mathbb{Q} de conducteur N .
- La courbe modulaire $X_0(N)$; cet espace s'interprète de façon géométrique ou analytique. Dans la plupart des cas, nous utiliserons la version analytique qui est mieux adaptée pour les calculs.

Ce lien est une application entre ces deux espaces appelée application de Weil, ou bien revêtement modulaire. Elle est donnée par une forme modulaire de poids 2 et de niveau N . L'existence automatique de cette application a longtemps été conjecturale puisque c'est une forme équivalente de la fameuse conjecture de Taniyama-Weil selon laquelle toute courbe elliptique définie sur \mathbb{Q} est modulaire. Cette conjecture démontrée en toute généralité par les récents travaux de [Wiles], [Taylor-Wiles], [Breuil etc.] a donc finalement succombé aux recherches intensives et profondes de nombreux mathématiciens. Ceci a des conséquences importantes en théorie des nombres. Une des plus célèbres est sans doute la preuve du grand théorème de Fermat : pour $n \geq 3$, l'équation $a^n + b^n = c^n$ n'a pas de solutions entières non triviales. Il a fallu plus de trois siècles pour en donner une démonstration et il est fort probable qu'aucune marge ne soit assez large pour la contenir ! La description concrète de l'application de Weil est possible et va nous permettre non seulement de résoudre des problèmes de théorie des nombres mais aussi de pouvoir l'étudier de façon explicite.

Dans un premier temps, nous allons faire quelques rappels succincts sur les trois objets centraux que nous utiliserons.

L'espace $X_0(N)$

Soit N un entier naturel. D'un point de vue géométrique, l'espace $X_0(N)$ est la compactification de l'espace $Y_0(N)$ qui classe, à isomorphisme près, les couples de courbes elliptiques (E, E') munie d'une isogénie $\iota : E \rightarrow E'$ de degré N . De façon analytique, une courbe elliptique E est le quotient de \mathbb{C} par un réseau Λ . On peut toujours considérer le couple (E, E') comme étant de la forme :

$$(E \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), E' \simeq \mathbb{C}/(\mathbb{Z} + \tau N\mathbb{Z})) ,$$

avec τ convenable appartenant au demi-plan de Poincaré \mathbb{H} . Deux nombres τ et τ' donnent lieu au même point de $X_0(N)$ si et seulement si ils sont équivalents modulo $\Gamma_0(N)$ i.e. :

$$\tau = M\tau' = \frac{a\tau + b}{c\tau + d} \quad \text{où} \quad M \in \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) , \quad N \mid c \right\} .$$

Ainsi, on obtient la version analytique de $X_0(N)$:

$$X_0(N) = \overline{\mathbb{H}}/\Gamma_0(N) \quad \text{avec} \quad \overline{\mathbb{H}} = \mathbb{H} \cup \{\infty\} \cup \mathbb{Q}.$$

La surjection canonique $\pi : \overline{\mathbb{H}} \rightarrow X_0(N)$ permet de définir des cartes locales et de munir $X_0(N)$ d'une structure de surface de Riemann compacte (cf. [Shimura 1]).

Les pointes de $X_0(N)$ sont les points provenant de $\{\infty\} \cup \mathbb{Q}$, elles sont en nombre fini et il y en a :

$$\nu_\infty = \sum_{d \mid N} \phi(\text{pgcd}(d, N/d)) ,$$

où ϕ est la fonction indicatrice d'Euler. Comme système de représentants de ces pointes dans $X_0(N)$, on choisit l'ensemble des $\frac{a}{b} \in \mathbb{P}_1(\mathbb{Q})$ tels que :

- Le dénominateur b parcourt l'ensemble des diviseurs positifs de N .
- Si $t = \text{pgcd}(b, N/b)$ alors pour chaque $0 \leq a_0 < t$ avec $\text{pgcd}(a_0, t) = 1$, on fixe un nombre $a \equiv a_0 \pmod{N/b}$ avec $\text{pgcd}(a, b) = 1$ (un tel choix est toujours possible).

Il n'est pas difficile, quoiqu'un peu technique, de décrire un procédé qui calcule une matrice $M \in \Gamma_0(N)$ telle que $MP = P'$ si P et P' sont deux pointes équivalentes.

Si $P = \frac{a}{b} \in X_0(N)$ est une pointe et $\Gamma_0(N)_P$ le stabilisateur de P dans $\Gamma_0(N)$ et si de plus, $M \in SL_2(\mathbb{Z})$ est telle que $MP = \infty$, alors il existe un nombre entier positif h vérifiant :

$$M\Gamma_0(N)_PM^{-1} = \left\{ \pm \begin{pmatrix} 1 & nh \\ 0 & 1 \end{pmatrix} , \quad n \in \mathbb{Z} \right\} . \quad (1)$$

Le nombre h s'appelle la largeur de la pointe et on a :

$$h = \frac{N}{\text{pgcd}(N, b^2)} .$$

Les éléments elliptiques d'ordre 2 (resp. d'ordre 3) de $X_0(N)$ sont les points fixes de \mathbb{H} par les matrices elliptiques d'ordre 2 (resp. ordre 3) de $\Gamma_0(N)$. Ils sont faciles à déterminer et il y en a ν_2 (resp. ν_3) où :

$$\begin{aligned} \nu_2 &= \begin{cases} 0 & \text{si } 4 \mid N \\ \prod_{p \mid N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{sinon} \end{cases}, \\ \text{et } \nu_3 &= \begin{cases} 0 & \text{si } 9 \mid N \\ \prod_{p \mid N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{sinon} \end{cases}. \end{aligned}$$

Enfin, on note μ l'indice de $\Gamma_0(N)$ dans $SL_2(\mathbb{Z})$ de sorte que :

$$\mu = N \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

Soit $\mathbb{P}_1(\mathbb{Z}/N\mathbb{Z})$ l'ensemble défini par :

$$\mathbb{P}_1(\mathbb{Z}/N\mathbb{Z}) = \{(c, d) \mid \text{pgcd}(c, d) = 1\} / \sim,$$

où \sim est la relation d'équivalence $(c, d) \sim (c', d') \Leftrightarrow cd' \equiv c'd \pmod{N}$. Les éléments (c, d) sont les "M-symboles" et ils permettent entre autre de donner un système complet de représentants de $SL_2(\mathbb{Z})$ modulo $\Gamma_0(N)$ en associant à $(c, d) \in \mathbb{P}_1(\mathbb{Z}/N\mathbb{Z})$ la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ où a et b sont des entiers vérifiant $ad - bc = 1$.

Formes Modulaires

Soit k un entier. Pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ ayant un déterminant positif, on définit l'opérateur $|_M$ qui agit sur les fonctions $f : \mathbb{H} \rightarrow \mathbb{C}$ par :

$$f|_M(\tau) = \det(M)^{k/2} (c\tau + d)^{-k} f(M\tau).$$

Une forme modulaire de poids k sur $\Gamma_0(N)$ est une fonction f sur \mathbb{H} telle que :

1. $f(\tau)$ est holomorphe.
2. $f|_M(\tau) = f(\tau)$ pour toute matrice $M \in \Gamma_0(N)$.
3. $f(\tau)$ est holomorphe aux pointes.

Si de plus f s'annule aux pointes, on dit que f est une forme parabolique. On note $M_k(N)$ (resp. $S_k(N)$) l'espace vectoriel de dimension finie des formes modulaires (resp. paraboliques) de poids k sur $\Gamma_0(N)$. Si χ est un caractère de Dirichlet modulo N , on peut aussi définir les formes modulaires de caractères χ en remplaçant la condition 2. ci dessus par :

$$2.' \quad f|_M(\tau) = \chi(d)f(\tau) \text{ pour toute matrice } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Si le caractère χ est non trivial, on peut éventuellement avoir des formes de poids k impair non nulles. On note $M_k(N, \chi)$ et $S_k(N, \chi)$ les espaces vectoriels correspondants.

La condition 3. signifie la propriété suivante. Soit P une pointe de largeur h et soit $M \in SL_2(\mathbb{Z})$ telle que $M\infty = P$. Alors l'égalité (1) et la condition 2. entraînent que $f|_M$ est périodique de période h . On peut donc écrire le développement de Fourier de $f|_M$:

$$f|_M(\tau) = \sum_n c(n)q^{n/h} \quad \text{avec} \quad q = e^{2i\pi\tau} . \quad (2)$$

La fonction f est holomorphe en P si $c(n) = 0$ pour tout $n < 0$. La forme modulaire f est parabolique si de plus $c(0) = 0$. Lorsque $P = \infty$ et $M = Id$, le développement (2) est très important ; on note $a(n)$ ses coefficients, i.e. :

$$f(\tau) = \sum_{n \geq 0} a(n)q^n .$$

On définit les opérateurs de Hecke sur $M_k(N)$ par :

$$T_p(f) = p^{k-1}f(p\tau) + \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) .$$

Si $Q \mid N$, on pose $Q' = \prod_{p \mid Q} p^{\text{ord}_p(N)}$ et on définit l'opérateur d'Atkin-Lehner W_Q par :

$$W_Q = \begin{pmatrix} xQ' & y \\ zN & wQ' \end{pmatrix} , \quad \det(W_Q) = Q' .$$

Remarquons que si $p^n \mid N$ alors $W_p = W_{p^2} = \dots = W_{p^n}$. A partir de maintenant, on va restreindre notre attention à l'espace des formes paraboliques $S_k(N)$. On peut montrer qu'il existe sur $S_k(N)$ une base de vecteurs propres pour tous les opérateurs de Hecke. On définit le sous espace $S_k(N)^{\text{old}}$ de $S_k(N)$ comme le sous espace engendré par les formes g du type :

$$g(d\tau) \quad \text{où } g \in S_k(M) \quad \text{avec } M \mid N, \quad M \neq N, \quad d \mid \frac{N}{M} .$$

L'espace $S_k(N)^{\text{new}}$ est alors le complémentaire orthogonal de $S_k(N)^{\text{old}}$ par rapport au produit scalaire de Petersson :

$$(f, g) = \int_{X_0(N)} f(\tau) \overline{g(\tau)} y^{k-2} dx dy , \quad \tau = x + iy .$$

Une forme $f \in S_k(N)^{\text{new}}$ qui est vecteur propre pour tous les opérateurs de Hecke est appelée "newform". Elle est qualifiée de normalisée si de plus on a $a(1) = 1$ dans son développement de Fourier à l'infini. Une newform f est aussi vecteur propre pour tous les opérateurs W_Q d'Atkin-Lehner ([Atkin-Lehner]), i.e.

$$f|_{W_Q} = \pm f .$$

Remarque : La terminologie française voudrait que nous parlions de forme primitive plutôt que de “newform”, mais nous avons volontairement conservé le terme anglo-saxon pour éviter toute confusion avec la notion de forme primitive introduite dans [Atkin-Li] et que nous utiliserons. Pour nous, une newform f est primitive si elle n’est la tordue d’aucune forme sur $\Gamma_0(N')$ avec $N' < N$.

On note $\mathcal{N}_k(N)$ l’ensemble des newforms normalisées. Si $f(\tau) = \sum_{n \geq 1} a(n)q^n \in \mathcal{N}_k(N)$ alors la série de Dirichlet $L(f, s) = \sum_n a(n)n^{-s}$ converge pour $\Re(s) > (k+1)/2$, se prolonge en une fonction entière et vérifie l’équation fonctionnelle :

$$\Lambda(f, s) = \varepsilon \Lambda(f, k-s) \quad \varepsilon = \pm 1 \quad ,$$

où $\Lambda(f, s) = (\sqrt{N}/2\pi)^s \Gamma(s) L(f, s)$. De plus, la série $L(f, s)$ se décompose en un produit de facteurs Eulériens :

$$\begin{aligned} L(f, s) &= \prod_p L_p(f, p^{-s}) \\ &= \prod_p (1 - \alpha(p)p^{-s})^{-1} (1 - \beta(p)p^{-s})^{-1} \quad . \end{aligned}$$

Avec :

$$\begin{cases} \alpha(p) + \beta(p) = a(p) \\ |\alpha(p)| = p^{k/2-1} \text{ et } \beta(p) = 0 & \text{si } p \nmid N \\ |\alpha(p)| = 0 \text{ et } \beta(p) = 0 & \text{si } p^2 \mid N \end{cases} \quad .$$

Notons que le signe ε de l’équation fonctionnelle est donnée par $f|_{W_N} = -\varepsilon f$.

Si ω est une forme différentielle holomorphe de $X_0(N)$, alors elle est de la forme $f(\tau)d\tau$ où f est une forme parabolique de poids 2 sur $\Gamma_0(N)$. L’application :

$$f(\tau) \longmapsto f(\tau)d\tau$$

est un isomorphisme entre $S_2(N)$ et l’espace vectoriel des formes différentielles holomorphes de $X_0(N)$. En particulier, la dimension de $S_2(N)$ est égale au genre g de $X_0(N)$ qui est donné par :

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2} \quad .$$

Courbes elliptiques Modulaires

Dans toute la suite, lorsque nous définirons une courbe elliptique E définie sur \mathbb{Q} par une équation, nous donnerons toujours le modèle minimal de Weierstrass (i.e. celui donnant le discriminant minimal). Soit donc E une courbe elliptique de conducteur N et d’équation (minimale) :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad .$$

Le théorème de Mordell-Weil nous donne la structure du groupe des points rationnels de la courbe :

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}} ,$$

où r est le rang de $E(\mathbb{Q})$ et $E(\mathbb{Q})_{\text{tors}}$ est sa partie de torsion (elle est facile à déterminer). D'un point de vue algorithmique, déterminer $E(\mathbb{Q})$, revient à trouver r générateurs indépendants de $E(\mathbb{Q})$.

Pour $p \nmid N$, on pose $a(p) = p + 1 - |E(\mathbb{F}_p)|$. On peut aussi définir des nombres $a(p)$ lorsque $p \mid N$ (dans ce cas $a(p) = \pm 1$ ou 0). On obtient alors la série L de E :

$$\begin{aligned} L(E, s) &= \prod_{p \nmid N} (1 - a(p)p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N} ((1 - a(p)p^{-s}))^{-1} \\ &= \sum_{n \geq 1} a(n)n^{-s} \quad \Re(s) > 3/2 . \end{aligned}$$

Comme toute courbe elliptique est modulaire, $L(E, s)$ est exactement la série L d'une forme modulaire $f \in \mathcal{N}_2(N)$ et ainsi, on associe naturellement à E une newform de poids 2 sur $\Gamma_0(N)$. La fonction $L(E, s)$ se prolonge donc à tout le plan complexe en une fonction entière et vérifie une équation fonctionnelle. La conjecture de Birch et Swinnerton-Dyer relie la valeur en $s = 1$ de cette série de Dirichlet à certains invariants géométriques de la courbe :

Conjecture (BSD)

$$\lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r} = \frac{R(E)\Omega c}{|E(\mathbb{Q})_{\text{tors}}|^2} |\text{III}| ,$$

où $R(E)$ est le régulateur, Ω la période réelle, c le produit des nombres de Tamagawa et III le groupe (conjecturalement fini) de Tate-Shafarevitch de E .

Cette conjecture très forte, s'inscrit en fait dans un cadre plus général. Elle a été vérifiée numériquement sur de nombreux exemples et est partiellement démontrée dans deux cas :

Cas du rang 0. Si $L(E, 1) \neq 0$, alors $r = 0$ et le groupe III est fini ([Kolyvagin], [Bump-Friedberg-Hoffstein], [Murty-Murty]). De plus, $L(E, 1)/\Omega$ est un nombre rationnel.

Cas du rang 1. Si $L(E, 1) = 0$ et $L(E, 1)' \neq 0$, alors $r = 1$ et le groupe III est fini. ([Kolyvagin], [Gross-Zagier]).

Dans le second cas, pour montrer que $E(\mathbb{Q})$ est de rang 1, Gross et Zagier construisent sur $E(\mathbb{Q})$ un point de Heegner d'ordre infini. Cette construction sera détaillée dans le chapitre I.

Une autre conséquence de la modularité de E est qu'il existe une application non constante

$\varphi : X_0(N) \rightarrow E(\mathbb{C})$ telle $\varphi(\infty) = 0$ (c'est le revêtement modulaire de E). L'image réciproque par φ de ω , la forme différentielle de Néron sur E , est une forme différentielle holomorphe de $X_0(N)$. Elle est donc de la forme $g(\tau)d\tau$ où $g \in S_2(N)$. La théorie d'Eichler-Shimura affirme que l'on a en fait (cf. [Swinerton-Dyer-Birch]) :

$$\varphi^*(\omega) = 2i\pi c_M f(\tau)d\tau ,$$

où $f(\tau)$ est la newform normalisée associée à E , et $c_M \in \mathbb{Z}$ est la constante de Manin (que l'on peut toujours supposer positive). Dans la classe d'isogénie de E , il existe une et une seule courbe, appelée courbe de Weil forte, dont le revêtement modulaire domine tous les autres ([Mazur-Swinerton-Dyer]). Pour cette courbe, la conjecture de Manin affirme que l'on a $c_M = 1$.

On peut aussi voir l'espace $X_0(N)$ comme une courbe projective lisse définie sur \mathbb{Q} . Dans ce cadre, le revêtement modulaire φ est un morphisme de courbes algébriques défini sur \mathbb{Q} . Les propriétés arithmétiques et géométriques de φ proviennent en général de cette interprétation.

Revêtement Modulaire

Description de φ

Réciproquement, supposons que $f(\tau) = \sum_n a(n)q^n$ soit une newform normalisée avec des coefficients de Fourier entiers. La forme différentielle $2i\pi c f(\tau)d\tau$, $c \in \mathbb{Z}$, étant holomorphe, l'intégrale :

$$\tilde{\phi}(\tau) = 2i\pi c \int_{\infty}^{\tau} f(z)dz$$

est indépendante du chemin choisi et définit une fonction $\tilde{\phi} : \mathbb{H} \rightarrow \mathbb{C}$. De plus, si $\gamma \in \Gamma_0(N)$, on pose :

$$\omega(\gamma) = \tilde{\phi}(\gamma\tau) - \tilde{\phi}(\tau) ,$$

la fonction $\omega(\gamma)$ ne dépend pas de τ et définit ce que l'on appelle une période de f . Un choix optimal pour τ permet de calculer rapidement $\omega(\gamma)$ ([Cremona 1]). On peut montrer que $\omega : \Gamma_0(N) \rightarrow \mathbb{C}$ est un homomorphisme de groupe. L'image $\omega(\Gamma_0(N))$ est contenu dans un réseau Λ de \mathbb{C} , et on a une application :

$$\begin{aligned} \phi : X_0(N) &\longrightarrow \mathbb{C}/\Lambda \\ \tau &\longmapsto c \sum_{n \geq 1} \frac{a(n)}{n} q^n . \end{aligned}$$

En considérant la fonction de Weierstrass associée au réseau Λ , on peut voir \mathbb{C}/Λ comme une courbe elliptique E :

$$\varphi : X_0(N) \xrightarrow{\phi} \mathbb{C}/\Lambda \xrightarrow{\wp} E(\mathbb{C}) ,$$

où l'on a noté \wp l'isomorphisme de groupe classique de \mathbb{C}/Λ dans $E(\mathbb{C})$ induit par la fonction de Weierstrass. Le calcul de \wp ne pose pas de problème (par exemple, la fonction

\wp est programmée dans le système PARI [Pari]). Avec nos hypothèses ($a(n) \in \mathbb{Z}$), on peut trouver une courbe elliptique E , définie sur \mathbb{Q} de Weil forte telle que $L(E, s) = L(f, s)$. De plus, en choisissant $c = c_M$, la constante de Manin pour E , le réseau Λ engendré par les périodes du modèle minimal de E contient $\omega(\Gamma_0(N))$ (la conjecture de Manin affirme que ces deux réseaux sont en fait égaux avec $c = 1$).

Ceci nous donne une description explicite de l'application de Weil pour E . Comme toute courbe elliptique définie sur \mathbb{Q} est modulaire, la construction ci-dessus est toujours possible.

Calcul de φ aux pointes

Soient τ dans \mathbb{H} , on note $\{\tau\}$ le symbole modulaire tel qu'il est décrit dans [Cremona 1] (C'est un élément de $H_1(X_0(N))$ et il faut voir $\{\tau\}$ comme un chemin allant de τ à ∞ sur lequel on va intégrer f). Soit α une pointe, l'opérateur de Hecke T_p agit sur les symboles modulaires et on a (cf. [Cremona 1]) :

$$T_p\{\alpha\} = \{p\alpha\} + \sum_{j=0}^{p-1} \left\{ \frac{\alpha + j}{p} \right\} . \quad (3)$$

Si $p \equiv 1 \pmod{N}$ alors les pointes $p\alpha$ et $(\alpha + j)/p$ ($j = 0, \dots, p-1$) sont toutes équivalentes à α . On peut donc trouver des matrices $M_0, M_1, \dots, M_p \in \Gamma_0(N)$ telles que :

$$\begin{aligned} M_j \alpha &= \frac{\alpha + j}{p} \quad j = 0, 1, \dots, p-1, \\ M_p \alpha &= p\alpha . \end{aligned}$$

En écrivant $\{(\alpha + j)/p\} = \{(\alpha + j)/p\} - \{\alpha\} + \{\alpha\}$, et en faisant agir f sur la formule (3), on obtient :

$$(1 + p - a(p))\phi(\alpha) = \sum_{j=0}^p \omega(M_p) .$$

Et donc $\phi(\alpha) = \frac{1}{1 + p - a(p)} \sum_{j=0}^p \omega(M_p)$ permet de définir (via \wp) la valeur de φ à la pointe α et de voir que c'est bien un point de torsion conformément au théorème de Manin-Drinfeld.

Calcul de φ en $\tau \in \mathbb{H}$

Soit $\tau \in \mathbb{H}$, comme on l'a vu pour calculer $\varphi(\tau)$, il suffit d'évaluer la série :

$$\sum_n \frac{a(n)}{n} q^n \quad q = e^{2i\pi\tau} ,$$

qui converge rapidement. Cependant, lorsque τ a une petite partie imaginaire, il faut beaucoup de termes dans la série pour avoir une bonne précision. Pour évaluer ϕ , il vaut mieux utiliser un représentant τ' de τ qui possède une partie imaginaire maximale. On peut aussi utiliser les opérateurs d'Atkin-Lehner W_Q . En effet, comme $f|_{W_Q} = \pm f$, on en déduit que :

$$\varphi = \varphi \circ W_Q + P \quad \text{où } P \in E(\mathbb{Q})_{\text{tors}} .$$

On peut facilement déterminer P et le signe ± 1 de la formule précédente (en particulier si Q est sans facteur carré, le signe est égal à $-a_Q$).

Pour calculer φ , on choisit $Q \mid N$ et W_Q tels que $W_Q\tau$ possède une partie imaginaire maximale. On calcule $\phi(W_Q\tau)$ et on en déduit $\varphi(\tau)$.

Plan de la thèse

Dans les trois premiers chapitres de cette thèse, nous nous intéressons plus particulièrement aux revêtements modulaires des courbes elliptiques.

Dans le premier chapitre, nous utiliserons la théorie des points de Heegner et le travail de Gross-Zagier pour décrire un algorithme général qui trouve des points rationnels non triviaux sur les courbes elliptiques de rang 1.

Le deuxième chapitre sera consacré au calcul du degré du revêtement modulaire. En particulier, nous y donnerons une méthode analytique rapide pour déterminer cet entier basée sur les propriétés arithmétiques du carré symétrique de la série L de la courbe elliptique. Au troisième chapitre, nous expliquerons comment on peut évaluer de façon expérimentale et étudier les points de ramification de l'application de Weil. Afin de déterminer quelles points sont des points critiques, nous étudierons le développement de Fourier des formes modulaires paraboliques aux pointes.

En se basant sur l'analogie qui existe entre les courbes elliptiques et les corps de nombres, nous ferons, dans le chapitre IV, une étude sur les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q} similaire à celle de Cohen et Lenstra sur les groupes de classes d'un corps de nombres.

L'utilisation du carré symétrique pour calculer le degré du revêtement modulaire s'insère dans le cadre général des conjectures de Deligne sur les valeurs spéciales des séries L. Dans le dernier chapitre, nous décrirons ces conjectures et expliquerons comment nous pouvons obtenir des données numériques en leur faveur.

Chapitre I

Points de Heegner

Les points de Heegner nous fournissent, dans ce chapitre, une première application concrète du revêtement modulaire associé à une courbe elliptique. La théorie des points de Heegner et l'utilisation de la version analytique de l'application de Weil vont nous permettre de calculer un point rationnel d'ordre infini sur les courbes elliptiques de rang 1 et de donner ainsi des solutions non triviales au problème Diophantien initial.

Comme nous le verrons, les points de Heegner sont attachés à des discriminants d'ordres de corps quadratiques. Il est classique, dans cette méthode, de ne considérer que des discriminants impairs et premiers avec le conducteur de la courbe (cf. [Stephens], [Green], ...) . Cependant, il est nécessaire, pour faciliter les calculs, d'avoir le plus large éventail de choix possibles. Dans ce chapitre, nous expliquerons comment construire de tels points de Heegner, y compris dans le cas où leur discriminant n'est ni impair, ni premier avec le conducteur.

I.1 Définitions et propriétés

I.1.1 Points de Heegner

Un point de Heegner est un point particulier de $X_0(N)$. Rappelons que de façon géométrique, un point de $X_0(N)$ différent d'une pointe peut-être vu comme un couple ordonné (E, E') de courbes elliptiques muni d'une isogénie $\iota : E \rightarrow E'$ de degré N . Birch définit un point de Heegner comme un couple (E, E') tel que E et E' aient multiplication complexe par le même anneau d'endomorphismes \mathcal{O} (cf. [Birch]). L'anneau \mathcal{O} est donc un ordre d'un corps quadratique imaginaire K . Le discriminant D de \mathcal{O} est de la forme $f^2 D_K$ où D_K est le discriminant du corps quadratique K et f l'indice de \mathcal{O} dans l'anneau des entiers \mathcal{O}_K de K . C'est à ce discriminant D que sont attachés nos points de Heegner. Ici, nous allons seulement considérer le cas où $f = 1$, donc le cas des discriminants fondamentaux (ceci n'est pas restrictif pour l'application que nous voulons envisager : le calcul des points rationnels sur une courbe elliptique). D'un point de vue analytique,

$\tau \in X_0(N)$ donne lieu au couple :

$$(E = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), E' = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}N\tau)) \quad .$$

Le fait que E ait multiplication complexe entraîne que τ est solution d'une équation de degré 2 à coefficients entiers :

$$A\tau^2 + B\tau + C = 0 \quad \text{avec} \quad \text{pgcd}(A, B, C) = 1 \quad \text{et} \quad \Delta(\tau) = B^2 - 4AC \quad . \quad (\text{I.1})$$

Ainsi, τ est un point de Heegner si τ et $N\tau$ satisfont tous les deux à une équation du type (I.1) avec $\Delta(\tau) = \Delta(N\tau)$. Ne considérer que des ordres maximaux signifie que $\Delta(\tau) = D_K$ est un discriminant fondamental. Si τ est un point de Heegner de discriminant D_K alors l'équation $D_K = B^2 - 4NC$ possède des solutions avec $(N, B, C) = 1$. On peut alors fixer $\beta \in \mathbb{Z}/2N\mathbb{Z}$ tel que $\beta^2 \equiv D_K \pmod{4N}$.

Le groupe des classes d'idéaux Cl_K de K est isomorphe au groupe des classes des formes quadratiques de discriminant D_K . Pour chaque classe d'idéaux $[\mathfrak{a}] \in Cl_K$, on associe le point de Heegner :

$$(\beta, [\mathfrak{a}]) = \frac{-B + \sqrt{D_K}}{2A} \pmod{\Gamma_0(N)} \in X_0(N) \quad ,$$

où (A, B, C) est une forme quadratique primitive de discriminant D_K dont la classe correspond avec $[\mathfrak{a}]$ et où $N \mid A$ et $B \equiv \beta \pmod{2N}$ (une telle forme existe toujours). L'interprétation géométrique du point de Heegner $(\beta, [\mathfrak{a}])$ est donné par le couple $(\mathbb{C}/\mathfrak{a}, \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1})$ où \mathfrak{n} désigne l'idéal primitif :

$$\mathfrak{n} = N\mathbb{Z} + \frac{\beta + \sqrt{D_K}}{2}\mathbb{Z} \quad .$$

Le choix de β fixe l'idéal primitif \mathfrak{n} et le point $(\beta, [\mathfrak{a}])$ correspond au point de Heegner $(\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])$ dans la notation utilisée par Gross (cf. [Gross]).

I.1.2 Premières propriétés

Soit E une courbe elliptique définie sur \mathbb{Q} de conducteur N . On suppose que le rang analytique de E vaut 1. Dans ce cas, le groupe de Tate-Shafarevitch III de E est fini, et le rang géométrique de E vaut 1 ([Gross-Zagier], [Kolyvagin]). On note $f(\tau) = \sum_n a(n)q^n$ la forme modulaire de poids 2 sur $\Gamma_0(N)$ associée à E et φ le revêtement modulaire comme défini dans l'introduction :

$$\varphi : X_0(N) \xrightarrow{\phi} \mathbb{C}/\Lambda \xrightarrow{\wp} E(\mathbb{C}) \quad .$$

Les hypothèses faites sur E entraînent que $L'(E, 1) \neq 0$ et que le signe ε de l'équation fonctionnelle de $\Lambda(E, s)$ est négatif, où $L(E, s)$ désigne la série L de E et $\Lambda(E, s)$ sa fonction complétée.

Les points de Heegner sont liés à un discriminant négatif (ici fondamental) vérifiant certaines conditions. Pour la suite, on se fixe un discriminant $D < 0$ tel que :

Condition 1 : D est un carré modulo $4N$.

Soit $\beta \in \mathbb{Z}/2N\mathbb{Z}$ tel que $\beta^2 \equiv D \pmod{4N}$. On note K le corps quadratique imaginaire de discriminant D , Cl son groupe de classe et $2u$ le nombre de racines de l'unité de K . De plus, on désigne par H le corps de classe de Hilbert de K . Le groupe de Galois de H sur K est isomorphe à Cl . Un isomorphisme est donné par l'application d'Artin que l'on notera λ dans la suite. Si $P = (\beta, [\mathfrak{a}]) \in X_0(N)$ est un point de Heegner, alors $\varphi(P) \in E(\mathbb{C})$ (comme tout point de $X_0(N)$!). Cependant, la théorie de la multiplication complexe permet de montrer que d'une part :

$$\varphi(P) \in E(H) \quad , \quad (\text{I.2})$$

et que d'autre part,

$$\varphi((\beta, [\mathfrak{a}]))^{\lambda([\mathfrak{b}])} = \varphi((\beta, [\mathfrak{a}\mathfrak{b}^{-1}])) \quad . \quad (\text{I.3})$$

Ces deux dernières propriétés sont par exemple des applications du théorème 4.3 de [Silverman]. Pour un contexte plus général, on pourra se référer par exemple à [Gross] et à [Shimura 1]. Les actions de la conjugaison complexe τ et de l'involution de Fricke W_N sur les points de Heegner se calculent directement :

$$\varphi((\beta, [\mathfrak{a}]))^\tau = \varphi((- \beta, [\mathfrak{a}^{-1}])) \quad , \quad (\text{I.4})$$

$$\varphi(W_N(\beta, [\mathfrak{a}])) = \varphi((- \beta, [\mathfrak{a}\mathfrak{n}^{-1}])) \quad . \quad (\text{I.5})$$

Il existe aussi une description de l'action des involutions d'Atkin-Lehner ([Gross]) mais nous ne l'utiliserons pas ici.

L'image par φ d'un point de Heegner étant algébrique, il suffit d'en calculer la trace pour obtenir un point rationnel. Pour cela posons :

$$P = \sum_{\sigma \in \text{Gal}(H/K)} \varphi((\beta, [\mathfrak{a}]))^\sigma = \sum_{[\mathfrak{b}] \in Cl} \varphi((\beta, [\mathfrak{a}\mathfrak{b}^{-1}])) \quad .$$

Les coordonnées de P appartiennent ainsi au corps quadratique K ; de plus on a :

Théorème I *Le point P appartient à $E(\mathbb{Q})$.*

Preuve :

$$P = \sum_{\sigma \in \text{Gal}(H/K)} \varphi((\beta, [\mathfrak{a}]))^\sigma = \sum_{\sigma} \varphi(W_N(\beta, [\mathfrak{a}]))^\sigma \quad .$$

En effet, l'involution de Fricke agit trivialement sur φ à cause du signe ($\varepsilon = -1$) de l'équation fonctionnelle. De plus,

$$\begin{aligned} \sum_{\sigma} \varphi(W_N(\beta, [\mathfrak{a}]))^\sigma &= \sum_{\sigma} \varphi((- \beta, [\mathfrak{a}\mathfrak{n}^{-1}]))^\sigma \\ &= \sum_{\sigma} \varphi((\beta, [\mathfrak{a}^{-1}\mathfrak{n}]))^{\sigma\tau} \\ &= P^\tau \quad . \end{aligned}$$

□

Dans cette preuve, on a utilisé en fait l'égalité plus précise suivante :

$$\varphi((\beta, [\mathbf{a}]))^\tau = \varphi((\beta, [\mathbf{a}^{-1}\mathbf{n}])) \quad .$$

De plus, on peut voir que si $[\mathbf{a}]$ correspond à la forme (A, B, C) , alors la classe $[\mathbf{a}^{-1}\mathbf{n}]$ correspond à la classe de $(A/N, -B, CN)$. Cette remarque permet de diviser le nombre d'évaluations de φ par deux ; si on a calculé $\varphi((\beta, [\mathbf{a}]))$, on reconnaît facilement la forme $(A', B', C') \simeq (A/N, -B, CN)$ et nous n'avons pas besoin d'évaluer φ au point correspondant, puisqu'il suffit de prendre le conjugué de $\varphi((\beta, [\mathbf{a}]))$.

Exemple : Prenons $E : y^2 + y = x^3 - x$, la plus petite courbe (au sens du conducteur) de rang 1 sur \mathbb{Q} , on a $N = 37$. Choisissons tout d'abord $D = -7$ et $\beta = -17$. On a :

$$x = \phi\left(\frac{17 + \sqrt{-7}}{2 \times 37}\right) \approx 0.92959 + 1.22569 \times i$$

et $\wp(x) = [0.00 \dots, 0.00 \dots]$. On identifie aisément le point rationnel $[0, 0]$ qui est un générateur $E(\mathbb{Q})$.

Prenons maintenant $D = -47$ et $\beta = -29 + 4 \times N = 119$. Il y a cinq classes de formes quadratiques de discriminant -47 :

$$\begin{aligned} (3, 1, 4) &\simeq (37, \beta, 2^5 \times 3) \\ (1, 1, 12) &\simeq (3 \times 37, \beta, 2^5) \simeq (1, -\beta, 2^5 \times 3 \times 37) \quad , \\ (3, -1, 4) &\simeq (2 \times 37, \beta, 2^4 \times 3) \\ (2, 1, 6) &\simeq (4 \times 37, \beta, 2^3 \times 3) \simeq (2, -\beta, 2^4 \times 3 \times 37) \quad , \\ (2, -1, 6) &\simeq (6 \times 37, \beta, 2^4 \times 3) \simeq (6, -\beta, 2^4 \times 3 \times 37) \quad . \end{aligned}$$

On calcule alors :

$$\begin{aligned} z_1 &= \phi\left(\frac{-119 + \sqrt{-47}}{2 \times 37}\right) \approx -0.66457 - 0.51118 \times i \quad . \\ z_2 &= \phi\left(\frac{-119 + \sqrt{-47}}{4 \times 37}\right) \approx 1.10414 - 0.48955 \times i \quad . \\ z_3 &= \phi\left(\frac{-119 + \sqrt{-47}}{12 \times 37}\right) \approx 0.05045 + 1.22569 \times i \quad . \end{aligned}$$

Puis le point $x = z_1 + \overline{z_1} + z_2 + \overline{z_2} + z_3$. Enfin, $\wp(x)$ donne encore le point $[0, 0]$.

Une des principales difficultés est l'évaluation de ϕ en un point de Heegner. En effet, dans le choix de la forme quadratique (A, B, C) correspondant à la classe $[\mathbf{a}]$, N doit diviser A . Si le conducteur est grand, le point de Heegner $(\beta, [\mathbf{a}])$ a une petite partie imaginaire et il faudra beaucoup de termes dans la série pour obtenir une précision suffisante afin de pouvoir reconnaître P en tant que point rationnel de $E(\mathbb{Q})$. Ainsi, le conducteur

ne peut pas être trop grand pour les applications numériques.

Les hypothèses faites sur D entraînent que si $p \mid \text{pgcd}(D, N)$ alors p divise exactement N (si $p \neq 2$, $p \mid D$ aussi). Soit $p \mid \text{pgcd}(D, N)$, l'opérateur d'Atkin-Lehner W_p agit sur les points de Heegner, si, de plus, $f|W_p = -f$ ($= -a_p f$ car $p \mid N$) alors $\varphi \circ W_p = -\varphi + Q$ où Q est un point de torsion de $E(\mathbb{Q})$. Cette dernière hypothèse implique alors que le point P que nous obtenons est forcément un point de torsion. Ceci donne lieu à une restriction supplémentaire sur D :

Condition 2 : Si $p \mid \text{pgcd}(D, N)$ alors W_p agit trivialement sur f (i.e. $a_p = -1$).

Cette condition est bien sûr vide si D et N sont premiers entre eux mais elle est absolument indispensable dans le cas général.

I.2 Formules de Gross-Zagier

I.2.1 Tordues quadratiques

Soit E une courbe elliptique définie sur \mathbb{Q} , de conducteur N , et soit ε le signe de l'équation fonctionnelle de la série L de E . On note $f = \sum_n a_n q^n$ la forme modulaire de poids 2 sur $\Gamma_0(N)$ associée à E . On a $f|_{W_N} = -\varepsilon f$. Enfin, on se donne $D < 0$ un discriminant qui soit un carré modulo $4N$. On définit alors l'ensemble S par :

$$S = \{p \text{ premier tel que } p \mid \text{pgcd}(D, N) \text{ et } a_p = 1\} .$$

On considère f_D la tordue de f par le caractère quadratique $\left(\frac{D}{\cdot}\right)$:

$$f_D = \sum_{n \geq 1} a_n \left(\frac{D}{n}\right) q^n .$$

Comme on l'a vu plus haut, $p \mid D \Rightarrow p^2 \nmid N$, on en déduit que la forme f est p -primitive pour tout $p \mid D$ (primitive au sens d'Atkin et Li [Atkin-Li]) . Ainsi, f_D est une newform de poids 2 sur $\Gamma_0(N_D)$ avec $N_D = ND^2/\text{pgcd}(D, N)$. De plus, les résultats de [Atkin-Li] permettent de montrer que l'on a :

$$f_D|_{W_{N_D}} = \varepsilon (-1)^{|S|} f_D .$$

Soit E_D la courbe elliptique définie sur \mathbb{Q} tordue de E par D (i.e. E et E_D sont isomorphes sur $\mathbb{Q}(\sqrt{D})$ mais pas sur \mathbb{Q}). La forme modulaire associée à E_D est alors précisément la forme f_D (grâce à la primitivité de f , ceci ne serait *pas vrai* en général si f n'était pas p -primitive). Le signe de l'équation fonctionnelle de la série L de E_D est donc $\varepsilon_D = -\varepsilon (-1)^{|S|}$; si $\varepsilon_D = 1$ on a :

$$L(E_D, 1) = 2 \sum_{n \geq 1} a_n \left(\frac{D}{n}\right) \exp \left(\frac{-2\pi n}{\sqrt{ND^2/\text{pgcd}(D, N)}} \right) . \quad (\text{I.6})$$

I.2.2 Le cas classique

Revenons à notre étude. En particulier, E est une courbe elliptique de rang 1 sur \mathbb{Q} (donc $\varepsilon = -1$), de conducteur N et D est un discriminant négatif vérifiant les conditions 1 et 2 (dans un premier temps, on va, en fait, se restreindre au cas classique des discriminants impairs et premiers avec le conducteur). Le point P est un point rationnel (“de Heegner”) associé à D et un β convenable. Le groupe de Mordeil-Weil est engendré par un seul élément G (modulo la torsion), et le point P que nous calculons est un multiple de ce point i.e. :

$$P = \ell G \pmod{E(\mathbb{Q})_{\text{tors}}} \text{ pour un certain } \ell \in \mathbb{Z}.$$

Cependant, le point G est plus facile à reconnaître (en tant que point rationnel) que le point P lui-même, du moins quand ℓ est grand. Il est donc important de pouvoir déterminer à l’avance la valeur de ℓ ou du moins l’un de ses facteurs. Les formules “à la Gross-Zagier” vont nous permettre d’obtenir des informations de ce type. Pour cela posons :

$$L_D = 2^r L(E_D, 1) ,$$

où r est le nombre de facteurs premiers distincts divisant $\text{pgcd}(D, N)$.

Remarques : 1) La condition 2 sur le discriminant affirme en fait que l’ensemble S est vide. Le signe ε_D de l’équation fonctionnelle de la série L de E_D est donc égal à $\varepsilon_D = -\varepsilon = 1$. On peut alors calculer L_D en utilisant la série (I.6) qui converge rapidement.

2) Nous avons placé le facteur 2^r dans la série définissant L_D afin d’harmoniser les formules ; il est justifié dans [Gross]. En particulier, ce facteur disparaît lorsque D et N sont premiers entre eux.

Proposition I.2.1 (Sous BSD) *Si $D < -4$ et $\text{pgcd}(D, 2N) = 1$ alors :*

$$\frac{\ell^2}{|\text{III}|} = \frac{\sqrt{|D|} c \Omega}{4 \text{Vol}(E) |E(\mathbb{Q})_{\text{tors}}|^2} L_D ,$$

où c (resp. Ω) est le produit des nombres de Tamagawa (resp. la période réelle) de E .

Preuve : Sous les hypothèses de la proposition, la formule de Gross-Zagier [Gross-Zagier] affirme que :

$$h(P) = \frac{\sqrt{|D|}}{4 \text{Vol}(E)} L'(E, 1) L_D , \tag{I.7}$$

où h est la fonction hauteur canonique de $E(\mathbb{Q})$. On remplace dans cette formule $L'(E, 1)$ par sa valeur prédite dans la conjecture de Birch et Swinnerton-Dyer (le régulateur est ici $h(G)$). \square

I.2.3 Le cas général

Nous voulons avoir le plus de choix possibles parmi les discriminants afin de garder celui qui conduit aux classes (A, B, C) donnant des points $\tau \in \mathbb{H}$ ayant des parties imaginaires maximales. Il faudrait donc limiter (au moins conjecturalement) les restrictions que nous avons faites sur D dans la proposition I.2.1. Dans [Hayashi], l'auteur généralise le travail de Gross et de Zagier et conjecture que la formule (I.7) est valable dans un contexte plus général, incluant le cas de tous les discriminants fondamentaux vérifiant les conditions 1 et 2. En reproduisant le raisonnement précédent, nous sommes naturellement amenés à faire la conjecture générale suivante :

Conjecture I.2.2 *Avec les notations précédentes, en particulier D est un carré modulo $4N$ et pour tout $p \mid \text{pgcd}(N, D)$ le p -ième coefficient de Fourier de f est égal à -1 , on a :*

$$\frac{\ell^2}{|\text{III}|} = \frac{\sqrt{|D|} c \Omega u^2}{4 \text{Vol}(E) |E(\mathbb{Q})_{\text{tors}}|^2} L_D ,$$

où $2u$ désigne le nombre de racines de l'unité de K .

Rappelons que $u = 1$ sauf dans les cas $D = -3$ et $D = -4$ pour lesquels on a $u = 3$ et $u = 2$ respectivement. Ce nombre u n'a pas besoin d'apparaître dans la proposition I.2.1. La conjecture I.2.2 a été vérifiée sur de nombreux exemples, et elle est justifiée par [Gross], [Gross-Zagier], [Hayashi] et par la conjecture de Birch et Swinnerton-Dyer. Comme nous l'avons vu, pour les applications numériques, le conducteur N ne doit pas être trop grand. Comme, en outre, le rang de la courbe elliptique est 1, on s'attend à ce que l'ordre du groupe de Tate-Shafarevitch III de E soit petit et souvent trivial ou à la rigueur, que $|\text{III}|$ soit éventuellement grand mais que le point rationnel ait une petite hauteur et soit donc facile à trouver. La conjecture (I.2.2) nous donne alors une très bonne approximation de ℓ dans les cas où l'utilisation de la méthode des points de Heegner est justifiée. Elle donne aussi une condition supplémentaire sur D pour obtenir un point d'ordre infini. Puisque l'on doit avoir $\ell \neq 0$:

Condition 3 : $L_D \neq 0$.

Dans l'exemple de la partie précédente, l'évaluation numérique du membre de droite de la formule de la conjecture (I.2.2) donne (comme attendu) $\ell^2/|\text{III}| = 1$ pour les deux discriminants choisis.

Remarques : 1) Dans la proposition I.2.1 et la conjecture I.2.2, seule une information sur ℓ^2 est donnée. On en déduit ℓ au signe près, mais cela n'a pas d'importance car si G engendre $E(\mathbb{Q})$, $-G$ l'engendre aussi. Si l'on se fixe un générateur et que l'on fait varier les discriminants, on obtient alors une suite de nombres bien définis $(\ell) = (\ell_D)_D$. Dans [Gross-Kohnen-Zagier], on montre que ces nombres sont en fait les coefficients d'une forme de Jacobi associée à f .

2) Le nombre $\ell^2/|\text{III}|$ peut-il ne pas être entier ? Bien sûr, cela ne peut pas se produire si $|\text{III}| = 1$. Mais si III n'est pas trivial, peut-on trouver un discriminant D tel que $\ell^2/|\text{III}| \notin \mathbb{Z}$? Dans un premier temps, on peut penser que oui, car le groupe III reste fixe alors que le nombre ℓ varie avec le discriminant. Nous avons effectué plusieurs calculs concernant cette question en considérant des courbes elliptiques de rang 1 ayant un groupe de Tate-Shafarevitch non trivial (sous BSD). De telles courbes apparaissent, par exemple, dans les tables de Cremona ([Cremona 1]), ([Cremona 3]) ou parmi les courbes elliptiques associées aux “simplest cubic fields” ([Delaunay-Duquesne]). Nous avons donc utilisé abondamment la conjecture I.2.2 sur ces courbes. Cependant nous n'avons trouvé aucun cas mettant en évidence une valeur non entière de $\ell^2/|\text{III}|$ (même lorsque le sous groupe de torsion de $E(\mathbb{Q})$ n'est pas trivial).

Dans la dernière partie de ce chapitre, nous montrerons (sous BSD) que $\ell^2/|\text{III}|$ est toujours entier pour une certaine famille de courbes elliptiques (corollaire I.4.1).

3) Lorsque l'ensemble S n'est pas vide, la condition 2 n'est pas vérifiée et le point obtenu est de torsion. Cependant, on peut évaluer le membre de droite de la formule de la conjecture I.2.2 à chaque fois que L_D correspond (à 2^r près) à la valeur en $s = 1$ de la série L de E_D (i.e. dès que $-\varepsilon(-1)^{|S|} = 1$ où ε est le signe de l'équation fonctionnelle de E). En remplaçant L_D par sa valeur donnée par la conjecture BSD, on remarque alors que le membre de droite de la formule de la conjecture I.2.2 est un nombre rationnel. Ce n'est pas toujours un entier. Prenons par exemple la courbe elliptique E d'équation $y^2 + y = x^3 + x^2 - 7x + 5$, de conducteur $N = 91 = 7 \times 13$ et vérifiant $a_7 = a_{13} = 1$. Si $D = -91$, les calculs numériques donnent :

$$\frac{\sqrt{|D|} c \Omega}{4 \text{Vol}(E) |E(\mathbb{Q})_{\text{tors}}|^2} L_D \approx 1.77777777 \approx \frac{16}{9} .$$

On peut aussi donner des exemples pour lesquels la valeur trouvée n'est pas un carré rationnel (prendre par exemple $E : y^2 + y = x^3 + x^2 - 10x + 10$ de conducteur $N = 123$ et $D = -123$).

I.3 Calculs explicites des points de Heegner

I.3.1 Méthode

Pour obtenir un point rationnel par la méthode des points de Heegner, on doit faire des évaluations de la fonction φ . Pour cela, il faut au préalable avoir déterminé la constante de Manin c_M associée à E . Si la courbe est de Weil forte, la conjecture de Manin affirme que $c_M = 1$. On fait alors les calculs en supposant que la conjecture est valide, et on vérifie à la fin que l'on a bien obtenu un point rationnel d'ordre infini. Comment savoir, et que faire, si la courbe n'est pas de Weil forte ? En fait, nul besoin de répondre à ces questions. En effet, notre seul but est de produire un point rationnel non trivial sur $E(\mathbb{Q})$. On effectue donc tous les calculs en supposant que $c_M = 1$ et sans se soucier de savoir si E est de Weil forte ou non. En pratique, on obtient le résultat attendu, et on justifie cette

méthode par le fait que la constante de Manin est (conjecturalement) *très souvent égale* à 1. Ceci s'explique en étudiant le revêtement modulaire de $X_1(N)$ sur E (et non plus $X_0(N)$) et en considérant une conjecture due à Stevens (cf. [Stevens]). Cette conjecture prédit que l'analogue de la courbe de Weil forte pour le $X_1(N)$ -revêtement est la courbe ayant un volume maximal dans sa classe d'isogénie et que toutes les $X_1(N)$ -constantes de Manin sont égales à 1. Si ceci est vérifié, et si la courbe de Weil forte (pour $X_0(N)$) est la courbe ayant un volume maximal, (i.e. si les notions de courbes fortes coïncident pour $X_0(N)$ et $X_1(N)$, ce qui est très fréquent) alors toutes les $X_0(N)$ -constantes de Manin sont aussi égales à 1 ([Watkins]). Quoiqu'il en soit, si la méthode échoue à cause d'une "mauvaise" constante de Manin, on peut multiplier P par le degré de l'isogénie qui lie la courbe E avec la courbe de Weil forte de sa classe. On sait qu'il n'y a qu'un nombre fini (et *très restreint*) de valeurs possibles.

La stratégie pour calculer un point rationnel par la méthode des points de Heegner est maintenant claire :

- On cherche $D < 0$ discriminant fondamental vérifiant les conditions 1, 2 et 3. En vérifiant la condition 3, on stocke la valeur m^2 qui est donnée par le membre de droite de la formule de la conjecture (I.2.2). On fixe $\beta \in \mathbb{Z}/2N\mathbb{Z}$ tel que $D \equiv \beta^2 \pmod{4N}$.
- On trouve tous les représentants des classes des formes binaires quadratiques de discriminant D de la forme (A, B, C) avec $N \mid A$ et $B \equiv \beta \pmod{2N}$ et A le plus petit possible.
- Pour chaque (A, B, C) , on calcule $\phi\left((-B + \sqrt{D})/2A\right) \in \mathbb{C}$. On n'évalue la série qu'une seule fois pour la classe (A, B, C) et la classe correspondant à son conjugué. On obtient alors $z = \sum_{(A, B, C)} \phi\left((-B + \sqrt{D})/2A\right) \in \mathbb{C}/\Lambda$.
- Au moins un des points $z_\lambda = z/m + \lambda$ où λ est un des m^2 points de m -torsion de \mathbb{C}/Λ correspond à un point rationnel. On essaie de reconnaître les coordonnées rationnelles de $\wp(z_\lambda)$. Si on échoue, on change de z_λ .

Dans la dernière étape, on ne teste que les points z_λ qui s'envoient dans la partie réelle de $E(\mathbb{C})$; cela ne fait plus que m ou $2m$ possibilités.

Plusieurs raisons peuvent rendre la méthode infructueuse. Tout d'abord, le point que l'on cherche a une grande hauteur et la valeur de z_λ n'est alors pas assez précise pour déterminer quel point rationnel lui correspond. Ceci peut avoir lieu entre autre si le groupe de Tate-Shafarevitch de E n'est pas trivial. On a alors $m \neq \pm\ell$, et le point que l'on veut obtenir est un multiple du générateur. Pour palier ce problème, on peut, par exemple, diviser z_λ par des petits facteurs. Ensuite, la constante de Manin associée à E n'est pas égale à 1. Ce cas est certes rare, mais peut se produire. Il faut alors modifier la méthode comme nous l'avons déjà expliqué, une difficulté étant aussi de pouvoir deviner que l'échec provient bien de cette cause.

I.3.2 Exemples

1 Un générateur compliqué

On considère la courbe E d'équation :

$$y^2 + y = x^3 + 164211x - 41113287 .$$

Cette courbe possède un générateur assez compliqué mais les calculs effectués avec le système PARI ([Pari]) n'ont demandé que quelques secondes pour trouver un point rationnel. Le conducteur de la courbe vaut $N = 4923 = 3^2 \times 547$. Le discriminant de cette courbe est assez élevé par rapport au conducteur ($\Delta = -3^{32}547$). Le programme `mwrank` de Cremona ([mwrank]), qui effectue une "2-descente", a besoin de quelques minutes pour trouver un point rationnel, avec un peu plus de temps il termine le calcul complet du rang (≈ 1 heure). Les premiers discriminants fondamentaux vérifiant les conditions 1, 2 et 3 sont :

$$D = -8, -20, -23, -59, -68, -71, -95, \dots$$

Les choix des discriminants $D = -8$ et $D = -20$ permettent de trouver un point rationnel sur $E(\mathbb{Q})$ avec une seule évaluation de la fonction ϕ ; les corps $\mathbb{Q}(\sqrt{-8})$ et $\mathbb{Q}(\sqrt{-20})$ ont pour nombre de classes 1 et 2 respectivement (pour $D = -20$, on effectue une évaluation de ϕ , l'autre étant donnée par le conjugué). Tous les autres discriminants ont un nombre de classes ≥ 3 , et au moins deux évaluations de ϕ sont nécessaires.

Pour $D = -8$ on a :

$$\begin{aligned} \frac{\ell^2}{|\text{III}|} &= 36 . \\ z &= \phi\left(\frac{1808 + \sqrt{-8}}{2N}\right) \\ &\approx 0.1154390726583146567871334976 \pmod{\Lambda} . \\ P &= \wp(z/6 + 3\omega_1/6) \\ &\approx [315.5912778716686408188261015, 6491.224486509555864274073430] . \end{aligned}$$

Nous gardons les conventions utilisées par le système PARI. Le réseau Λ est engendré par ω_1 et ω_2 donnés par la 15-ème et 16-ème composante du vecteur produit par la commande `ellinit` de PARI. En utilisant le développement en fractions continues de l'approximation de P , on trouve le point :

$$P = \left[\frac{66371371729}{14502^2}, \frac{19797499059399917}{14502^3} \right] .$$

La hauteur canonique de ce point est ≈ 25.6 . Bien sûr, il est beaucoup plus difficile d'obtenir le point $6P$ directement.

Pour $D = -20$, on a $\ell^2/|\text{III}| = 4$ et :

$$\begin{aligned} z &= 2\Re\left(\phi\left(\frac{2254 + \sqrt{-20}}{2N}\right)\right) \\ &\approx 0.03847969088610488559571364511 \pmod{\Lambda} . \end{aligned}$$

On obtient le même point qu'avec $D = -8$, en évaluant $\wp(z/2 + \omega_1/2)$.

2 Un conducteur élevé

On prend :

$$E : y^2 + xy = x^3 - 66 .$$

Le conducteur $N = 1881726 = 2 \times 3 \times 7 \times 11 \times 4073$ de E est assez grand. Les calculs ont demandé quelques minutes pour obtenir un point rationnel d'ordre infini. Le programme **mwrnk** termine le calcul du rang complet en un temps équivalent. On choisit $D = -167$ qui semble être le discriminant le plus raisonnable vérifiant les conditions 1, 2 et 3 ; on a $\ell^2/|\text{III}| = 16$. On prend $\beta = -1305835$, ainsi $(\beta^2 - D)/4N = 2^2 \times 3^2 \times 7 \times 29 \times 31$ a beaucoup de petits facteurs. Les 11 classes de formes quadratiques sont les suivantes (chaque ligne donnant une classe et celle correspondant au conjugué) :

$$\begin{aligned} (N, \beta, 226548), (36N, \beta, 6293) &\rightarrow x_1 = \frac{-\beta + \sqrt{-167}}{2N} \\ (2N, \beta, 113274), (18N, \beta, 12586) &\rightarrow x_2 = \frac{-\beta + \sqrt{-167}}{4N} \\ (3N, \beta, 75516), (12N, \beta, 18879) &\rightarrow x_3 = \frac{-\beta + \sqrt{-167}}{6N} \\ (4N, \beta, 56637), (9N, \beta, 25172) &\rightarrow x_4 = \frac{-\beta + \sqrt{-167}}{8N} \\ (7N, \beta, 32364), (31N, \beta, 7308) &\rightarrow x_5 = \frac{-\beta + \sqrt{-167}}{14N} \\ (6N, \beta, 37758) &\rightarrow x_6 = \frac{-\beta + \sqrt{-167}}{12N} \end{aligned}$$

On évalue les $\phi(x_j)$, en “remontant” leur partie imaginaire grâce aux involutions d’Atkin-Lehner (nous avons eu besoin, ici, d’un peu moins de 3×10^6 coefficients a_n pour obtenir une précision suffisante). Finalement, on a :

$$\begin{aligned} z &= 2\Re(\phi(x_1)) + 2\Re(\phi(x_2)) + 2\Re(\phi(x_3)) + 2\Re(\phi(x_4)) + 2\Re(\phi(x_5)) + \phi(x_6) \\ &\approx 1.184181477996882205289921841 \pmod{\Lambda} \end{aligned}$$

Enfin, on calcule $\wp(z/4)$, et on reconnaît le point :

$$P = \left[\frac{76941655}{2598^2}, \frac{-767173503469}{2598^3} \right]$$

de hauteur ≈ 18.4 .

3 Un groupe III non trivial

On prend pour E la courbe elliptique d’équation :

$$y^2 + xy + y = x^3 + x^2 - 24752x - 1509184 .$$

Le conducteur vaut $N = 4641 = 3 \times 7 \times 13 \times 17$. Les discriminants vérifiant les conditions 1, 2 et 3 sont $D = -35, -251, -276, \dots$. On choisit bien sûr $D = -35$. On voit ici que le choix d'un discriminant non premier avec le conducteur peut éventuellement conduire à des calculs plus simples. On a $\ell^2/|\text{III}| = 4$. Il faut deux évaluations de ϕ , aux points :

$$x_1 = \frac{973 + \sqrt{-35}}{2N} \quad \text{et} \quad x_2 = \frac{973 + \sqrt{-35}}{6N} .$$

Les calculs montrent que $\phi(x_1) = \phi(x_2) \approx 0.090514828921 \pmod{\mathbb{C}/\Lambda}$ et que :

$$\varphi(x_1) = P = \left[\frac{43817777521}{239630400}, \frac{-1629520793942221}{3709478592000} \right] .$$

Ce point P est compliqué par rapport au générateur $G = [415, 7532]$ de $E(\mathbb{Q})$ (on a $P = 2G$). Le groupe de Tate-Shafarevitch est ici non trivial ($|\text{III}| = 4$), et nous a empêchés d'obtenir le point G directement.

4 Nombres congruents

En arithmétique, il y a deux exemples classiques que l'on considère de façon presque systématique ; il s'agit des nombres congruents et des cubiques de Sylvester. Le dernier sera étudié dans la dernière partie de ce chapitre. Pour les nombres congruents, le problème se ramène à trouver des solutions non triviales (si il y en a) de :

$$E_n : y^2 = x^3 - n^2x ,$$

où n est un entier positif. Le groupe de torsion de $E_n(\mathbb{Q})$ est d'ordre 4 et est engendré par les deux points d'ordre 2 :

$$P_1 = [0, 0] \quad \text{et} \quad P_2 = [n, 0] .$$

Toutes les courbes E_n sont isomorphes à E_1 sur le corps quadratiques $\mathbb{Q}(\sqrt{-n})$. Cette remarque peut-être utilisée pour adaptée la méthode des points de Heegner et la rendre plus efficace ici ([Elkies]). Cependant, notre méthode générale suffit pour traiter quelques exemples un "peu compliqués". Prenons le cas du nombre congruent $n = 157$ qui a été résolu par Zagier. On pose :

$$E : y^2 = x^3 - 157^2x .$$

Le conducteur de E vaut $N = 788768 = 2^5 \times 157^2$. On choisit $D = -39$ et $\beta = 1275547$. On a $\ell^2/|\text{III}| = 16$. Les 4 classes de formes quadratiques de discriminant -39 nous donnent :

$$\begin{aligned} (2, -1, 5) &\simeq (N, \beta, 2^2 \times 13 \times 47 \times 211) &\rightarrow x_1 &= \frac{-\beta + \sqrt{-39}}{2N} \\ (1, 1, 10) &\simeq (1, -\beta, N \times 2^2 \times 13 \times 47 \times 211) \\ (3, 3, 4) &\simeq (2N, \beta, 2 \times 13 \times 47 \times 211) &\rightarrow x_2 &= \frac{-\beta + \sqrt{-39}}{4N} \\ (2, 1, 5) &\simeq (2, -\beta, N \times 2 \times 13 \times 47 \times 211) \end{aligned}$$

On calcule :

$$\begin{aligned} z &= 2\Re(\phi(x_1) + \phi(x_2)) \\ &\approx 0.0109890348711178289 \pmod{\Lambda} . \end{aligned}$$

Enfin :

$$\wp(z/4 + \omega_1/4) \approx [344.9966583246897399073, -5706.0151727629419113686] .$$

On reconnaît le point rationnel :

$$P = \left[\frac{95732359354501581258364453}{277487787329244632169121}, -\frac{834062764128948944072857085701103222940}{146172545791721526568155259438196081} \right]$$

dont la hauteur est ≈ 54.6 .

Voici, à titre d'illustration, quelques exemples de nombres congruents qui donnent lieu à des solutions compliquées. Il s'agit des nombres $n < 300$ pour lesquels les points rationnels sur E_n , que nous avons obtenu par la méthode des points de Heegner, ont une hauteur canonique > 50 .

$$\mathbf{n} = \mathbf{263} \quad \begin{aligned} D &= -7, & \beta &= 1156427, & \ell^2/|\mathbf{III}| &= 4, & h(P) &\approx 77.18 \quad . \end{aligned}$$

$$P = \left[\frac{635157351902093570142252875888959728}{2196589972531420851340521356470969}, \frac{210381207436022030091563782998604894373879276352542940}{102949323009915282279135918676339558881595324993453} \right]$$

$$\mathbf{n} = \mathbf{269} \quad \begin{aligned} D &= -23, & \beta &= 91757, & \ell^2/|\mathbf{III}| &= 4, & h(P) &\approx 55.94 \quad . \end{aligned}$$

$$P = \left[-\frac{6841040196454710370084}{7337019259262265405625}, \frac{163241434041607239531794865751725714}{628462673537642088275144318078125} \right]$$

$$\mathbf{n} = \mathbf{277} \quad \begin{aligned} D &= -23, & \beta &= 541421, & \ell^2/|\mathbf{III}| &= 4, & h(P) &\approx 71.81 \quad . \end{aligned}$$

$$P = \left[-\frac{283607850589557281956}{8710577587017625225}, \frac{46255397525091345186771750200178}{25708126615432888593541097125} \right]$$

$$\mathbf{n} = \mathbf{293} \quad \begin{aligned} D &= -15, & \beta &= 1758375, & \ell^2/|\mathbf{III}| &= 36, & h(P) &\approx 58.34 \quad . \end{aligned}$$

$$P = \left[\frac{8927685581941938308484876237}{940689989494724882336641}, \frac{843143046416468063727201118843951115152020}{912367451766133915174366598344714561} \right]$$

I.4 Autour des cubiques de Sylvester

Dans ce paragraphe, nous étudions directement quelques propriétés arithmétiques de $\ell^2/|\mathbf{III}|$ pour une famille classique de courbes elliptiques et pour des discriminants impairs et premiers avec le conducteur (cette condition est automatique pour nos courbes). Pour

cela, nous utilisons la formule de la proposition I.2.1 et nous supposons donc dans toute cette partie la validité de la conjecture BSD.

Soit m un entier positif sans facteur cubique et non divisible par 9 (cette dernière restriction est faite pour éviter d'alourdir les calculs). On considère la courbe elliptique $x^3 + y^3 = m$ (cubique de Sylvester). Une transformation birationnelle permet d'obtenir le modèle minimal :

$$\begin{aligned} E : y^2 &= x^3 - 27 \left(\frac{m}{2} \right)^2 & \text{si } m \text{ est pair} , \\ E : y^2 + y &= x^3 - \frac{27m^2 + 1}{4} & \text{si } m \text{ est impair} . \end{aligned}$$

On aura aussi besoin pour la suite de connaître les facteurs premiers de m . On décompose m sous la forme :

$$m = 3^\alpha \prod_{j=1}^s p_j^{\beta_j} \prod_{j=1}^t q_j^{\gamma_j} \quad \text{avec } p_j \equiv 1 \pmod{3} \text{ et } q_j \equiv 2 \pmod{3} .$$

Les hypothèses faites sur m impliquent que $\alpha = 0$ ou 1 et que $1 \leq \beta_j, \gamma_j \leq 2$. Les algorithmes classiques sur les courbes elliptiques ([Cohen 1]) permettent de calculer les invariants de E :

$$\begin{aligned} \Omega &= \frac{\Gamma(1/3)^3}{2\pi\sqrt{3}} m^{-\frac{1}{3}} , \\ \text{Vol}(E) &= \frac{\Gamma(1/3)^6}{8\pi^2\sqrt{3}} m^{-\frac{2}{3}} , \end{aligned}$$

où Γ désigne la fonction d'Euler ($\Gamma(1/3) = 2.67893\dots$). De plus, le conducteur N , le produit c des nombres de Tamagawa de E et le signe ε de l'équation fonctionnelle sont donnés par les formules suivantes :

- Si $m \equiv \pm 1 \pmod{9}$ alors $N = 3^3 m^2$, $c = 3^{s+1}$ et $\varepsilon = (-1)^t$;
- Si $m \equiv \pm 2 \pmod{9}$ alors $N = 3^2 m^2$, $c = 2 \times 3^s$ et $\varepsilon = -(-1)^t$;
- Si $m \equiv \pm 4 \pmod{9}$ alors $N = 3^3 m^2$, $c = 3^s$ et $\varepsilon = -(-1)^t$;
- Si $\alpha = 1$ alors $N = 3^3 m^2$, $c = 3^s$ et $\varepsilon = (-1)^t$.

On suppose de plus que le rang de $E(\mathbb{Q})$ vaut 1.

Soit $D < 0$ un discriminant fondamental impair, premier avec N et tel que D est un carré modulo $4N$. On pose $d = |D|$. On considère la courbe elliptique E_D tordue de E par D . On écrit c' , N' , Ω' pour les invariants classiques associés à E_D . On a :

$$\begin{aligned} N' &= Nd^2 , \\ \Omega' &= \frac{\sqrt{3}}{\sqrt{d}} \Omega . \end{aligned}$$

La proposition I.2.1 affirme que l'on a :

$$\frac{\ell^2}{|\text{III}|} = \frac{\sqrt{d} c \Omega}{4 \text{Vol}(E)} L(E_D, 1) ,$$

car la courbe E (tout comme E_D) est sans torsion. En remplaçant $L(E_D, 1)$ par sa valeur prédite dans la conjecture BSD, on obtient :

$$\frac{\ell^2}{|\text{III}|} = \frac{c \times c'}{2} S' , \quad (\text{I.8})$$

où $S' = |\text{III}'|$ si $L(E, D, 1) \neq 0$ et $S' = 0$ sinon. On en déduit :

Corollaire I.4.1 (sous BSD) $\frac{\ell^2}{|\text{III}|}$ est toujours un entier.

Preuve : En effet, le groupe III est fini, son ordre est un carré parfait et le dénominateur de $\ell^2/|\text{III}|$ ne peut donc pas être égal à 2. \square

Proposition I.4.2 La valuation 3-adique de $c \times c'$ est donnée par :

$$\text{ord}_3(c \times c') = \begin{cases} 2s+2 & \text{si } m \equiv \pm 1 \pmod{9} \\ 2s & \text{sinon.} \end{cases}$$

Preuve : On utilise l'algorithme de Tate pour déterminer la valeur de c' . Pour cela, on note $r(n, p)$ le nombre de solutions de l'équation $X^3 + n = 0$ dans $\mathbb{Z}/p\mathbb{Z}$ et on définit $f(m, d)$ par :

$$\begin{aligned} f(m, d) &= \prod_{p|d} \left(1 + r\left(\left(\frac{m}{2}\right)^2, p\right) \right) \quad \text{si } m \text{ est pair} , \\ f(m, d) &= \prod_{p|d} (1 + r(2m^2, p)) \quad \text{si } m \text{ est impair} . \end{aligned}$$

On obtient alors :

- Si $m \equiv \pm 1 \pmod{9}$ alors $c' = 3^{s+1} f(m, d)$;
- Si $m \equiv \pm 2 \pmod{9}$ alors $c' = 3^s \times 2 f(m, d)$;
- Si $m \equiv \pm 4 \pmod{9}$ alors $c' = 3^s f(m, d)$;
- Si $\alpha = 1$ alors $c' = 3^s f(m, d)$.

Et on conclut en remarquant que $\text{pgcd}(f(m, d), 3) = 1$. \square

La proposition I.4.2 montre en particulier que $\frac{c \times c'}{2}$ est un multiple de 9 si et seulement si l'une de deux conditions suivantes est vérifiée :

- $m \equiv \pm 1 \pmod{9}$;
- Il existe dans la décomposition de m un facteur premier $p \equiv 1 \pmod{3}$ (i.e. $s > 0$).

Corollaire I.4.3 (sous BSD) Dans les deux cas précédents, $\frac{\ell^2}{|\text{III}|} \equiv 0 \pmod{9}$.

Ainsi le point de Heegner associé à D est un multiple de 3 fois le générateur. Nous allons maintenant expliquer pourquoi cela se produit de façon générale.

La courbe E_D admet pour équation :

$$E_D : y^2 = x^3 - k ,$$

où $k = 2^4 \times 3^3 D^3 m^2$ si m est impair et $k = 3^3 D^3 (m/2)^2$ si m est pair. Dans les deux cas, k est sans puissance 6-ème (car D est impair, premier avec 3 et m). On peut alors utiliser les résultats de [Satgé]. On note \widetilde{E}_D la courbe d'équation $y^2 = x^3 + k/27$. Les courbes E_D et \widetilde{E}_D sont 3-isogènes par une isogénie λ décrite dans la définition 1.1 de [Satgé]. On désigne par $d_3(S)$ la dimension sur $\mathbb{Z}/3\mathbb{Z}$ de l'espace vectoriel $S_\lambda(E_D, \mathbb{Q})$ (la λ -partie du groupe de Selmer de E_D). Une application directe de la proposition 1.17 de [Satgé] permet d'obtenir la minoration suivante :

$$d_3(S) \geq t + \alpha \quad (-1 \text{ si } m \equiv \pm 1 \pmod{9}) . \quad (\text{I.9})$$

On en déduit le :

Théorème II (sous BSD) *Avec les notations précédentes, le nombre $\frac{\ell^2}{|\text{III}|}$ est un entier divisible par 9.*

Preuve : On sait déjà que $\ell^2/|\text{III}|$ est un entier et le théorème est montré si $m \equiv \pm 1 \pmod{9}$ ou si $s > 0$. Dans les autres cas, on peut supposer que le rang de la courbe E_D sur \mathbb{Q} est nul (sinon $L(E_D, 1) = 0$ et $\ell = 0$), ainsi $S_\lambda(E_D, \mathbb{Q}) \simeq \text{III}(E_D, \mathbb{Q})[\lambda]$. Comme $d_3(S) > 0$ (par I.9), on en déduit que la 3-partie de III' n'est pas triviale, et donc que S' est divisible par 9. La formule (I.8) permet alors de conclure. \square

Remarque : On peut obtenir bien plus que le théorème II. Par exemple, si $m = 42$, alors la formule (I.9) donne $d_3(S) \geq 2$ et $c \times c'$ est aussi divisible par 9. Dans ce cas là, on a donc $\ell^2 \equiv 0 \pmod{81}$ (III est trivial ici) et ℓ est toujours divisible par 9.

Cette partie a permis d'illustrer que ℓ est en fait lié au groupe de Tate-Shafarevitch de E_D . Par (I.9), on voit que ce nombre peut être rendu aussi grand que l'on veut. D'où l'intérêt de le connaître à l'avance pour trouver plus facilement le point rationnel que l'on recherche.

Chapitre II

Degré du revêtement modulaire

Le but principal de cette partie est d'expliquer comment l'on peut calculer le degré du revêtement modulaire φ d'une courbe elliptique E . Il est important de connaître ce nombre, noté $\deg(\varphi)$, pour étudier explicitement l'application de Weil. De plus, une méthode efficace pour calculer $\deg(\varphi)$ est utile pour pouvoir vérifier les conjectures qui lui sont reliées.

II.1 Introduction

Rappelons quelques faits classiques sur les surfaces de Riemann compactes. Soient X et X' deux surfaces de Riemann compactes et $\varphi : X \rightarrow X'$ une application holomorphe entre ces deux espaces. La fonction φ est alors soit constante soit surjective. Dans le dernier cas, il existe un nombre entier positif d tel que pour tout $z' \in X'$ sauf un nombre fini, on a :

$$|\varphi^{-1}(\{z'\})| = d .$$

Cet entier est appelé le degré de φ et est noté $\deg(\varphi)$. De plus pour tout $z' \in X'$ l'inégalité :

$$|\varphi^{-1}(\{z'\})| \leq d$$

a lieu. Les points $z' \in X'$ pour lesquels l'inégalité est stricte sont des points particuliers de X' , appelés points de ramification de φ . Ils formeront un des principaux objets d'étude du prochain chapitre.

Le cas qui nous intéresse ici est :

$$X = X_0(N) \xrightarrow{\varphi} E(\mathbb{C}) = X' ,$$

où E est une courbe elliptique définie sur \mathbb{Q} de conducteur N et φ le revêtement modulaire. On parle alors de degré modulaire de E . Ce nombre $\deg(\varphi)$ joue un rôle d'une grande importance en théorie des nombres. Par exemple, on conjecture que $\deg(\varphi)$ ne peut pas être trop élevé (la conjecture précise est : $\log(\deg(\varphi)) = O(\log(N))$). Cette conjecture a

une conséquence arithmétique très forte puisqu'elle entraîne une des formes de la conjecture abc. Soit f la newform normalisée de poids 2 sur $\Gamma_0(N)$ associée à E de sorte que l'on a : $\varphi^*(\omega) = 2i\pi c_M f(\tau)d\tau$ où ω est l'unique (à multiplication par un scalaire près) forme différentielle invariante de E et c_M la constante de Manin (que l'on peut supposer positive). Le degré modulaire est lié à la norme de Petersson de f car (cf. [Zagier]) :

$$\deg(\varphi) = \frac{4\pi^2 c_M^2 \|f\|^2}{\text{Vol}(E)} . \quad (\text{II.1})$$

On voit que le calcul de $\deg(\varphi)$ se ramène à celui de $\|f\|$. Dans [Zagier], Zagier donne un procédé explicite pour évaluer $\|f\|$ dans le cas général d'un sous-groupe de congruence Γ . Cremona traduit la méthode de Zagier dans le langage des “M-symboles” ([Cremona 2]) ; ce qui lui évite d'avoir à utiliser un domaine fondamental explicite pour $X_0(N)$, et lui permet de calculer numériquement les degrés modulaires de toutes les courbes elliptiques de conducteur $N \leq 5000$. Ces méthodes sont plutôt géométriques, et deviennent longues lorsque le conducteur est grand.

Dans le paragraphe II.2, nous expliquerons comment on généralise le travail de Cremona pour obtenir une formule directe sur le produit scalaire (de Petersson) de deux formes modulaires f_1 et f_2 . Pour cela, nous utiliserons les outils et les notations de [Cremona 2]. Dans le paragraphe II.3, nous donnerons une méthode plus rapide qui calcule $\|f\|$ en utilisant les propriétés de la série L du carré symétrique de E .

II.2 Utilisation des “M-symboles”

II.2.1 Notations

Soient f_1 et f_2 deux formes modulaires de poids 2 sur $\Gamma_0(N)$. Comme nous l'avons déjà vu dans l'introduction, les applications :

$$\begin{aligned} \varphi_r : \mathbb{H} &\longrightarrow \mathbb{C} & (r = 1, 2) \\ \tau &\longmapsto 2i\pi \int_{\infty}^{\tau} f_r(z)dz \end{aligned} ,$$

sont bien définies car la valeur de l'intégrale ne dépend pas du chemin choisi. De plus, si $\gamma \in \Gamma_0(N)$, alors :

$$\omega_r(\gamma) = \varphi_r(\gamma\tau) - \varphi_r(\tau)$$

est indépendant de τ et ω_r définit un homomorphisme de groupe $\omega_r : \Gamma_0(N) \rightarrow \mathbb{C}$ dont le noyau contient toutes les matrices elliptiques et paraboliques de $\Gamma_0(N)$.

Comme dans [Cremona 2], on choisit \mathcal{S} un système de représentants à droite pour $\Gamma_0(N)$ dans $SL_2(\mathbb{Z})$ tel que :

$$\gamma \in \mathcal{S} \Rightarrow \gamma ST \in \mathcal{S} \quad \text{où } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

Un tel choix est toujours possible si $\Gamma_0(N)$ ne contient pas d'élément elliptique. Dans la suite, nous allons oublier ces éléments elliptiques car étant dans le noyau de ω_1 et ω_2 , leurs

contributions n’apportent rien, ni dans les calculs que nous allons faire, ni dans la formule du théorème III. On note \mathcal{F}_N un domaine fondamental de $X_0(N)$ tel qu’il est décrit dans [Cremona 2], si bien que sa frontière est formée par les (γ) pour $\gamma \in \mathcal{S}$ où (γ) désigne la géodésique $\{\gamma(0), \gamma(\infty)\}$. On note que $(\gamma) = -(\gamma S)$.

Pour $\gamma \in \mathcal{S}$, γS est équivalente à une matrice dans \mathcal{S} . Notons γ^* cette matrice ; il existe ainsi une matrice $s(\gamma) \in \Gamma_0(N)$ tel que $\gamma S = s(\gamma)\gamma^*$. L’application $*$: $\mathcal{S} \rightarrow \mathcal{S}$ est une involution.

De même, il existe $t(\gamma) \in \Gamma_0(N)$ et $\tau(\gamma) \in \mathcal{S}$ telles que $\gamma T = t(\gamma)\tau(\gamma)$. On s’intéresse aux τ -orbites dans \mathcal{S} . Si $\gamma_1 \in \mathcal{S}$ est un point de base, alors $\gamma_1, \gamma_2 = \tau(\gamma_1), \dots, \gamma_k = \tau(\gamma_{k-1})$ est une orbite complète de longueur k . Bien sûr, k dépend de l’orbite, et nous devrions écrire k_{γ_1} (la longueur de l’orbite est en fait égale à la largeur de la pointe $\gamma_1(\infty) = \gamma_j(\infty)$ dans $X_0(N)$), mais pour alléger l’écriture nous omettrons d’indiquer cette dépendance dans la suite (le contexte étant suffisamment clair). On a (cf. [Cremona 2]) :

$$\sum_{j=1}^k \omega_r(t(\gamma_j)) = 0 ; \quad (II.2)$$

$$s(\gamma TS) = t(\gamma) . \quad (II.3)$$

II.2.2 Formule pour le produit scalaire

Avec les outils de la partie précédente, le produit scalaire de Petersson de f_1 et de f_2 peut s’écrire à l’aide d’une somme finie, facilement calculable. Le théorème suivant est une reformulation du théorème I de [Zagier].

Théorème III *Avec les notations précédentes :*

$$(f_1, f_2) = \frac{i}{16\pi^2} \sum_{\tau\text{-orbites}} \sum_{1 \leq j < i \leq k} \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} - \omega_1(t(\gamma_i)) \overline{\omega_2(t(\gamma_j))} .$$

Preuve : On a :

$$\begin{aligned} (f_1, f_2) &= \frac{i}{2} \int_{\mathcal{F}_N} f_1(z) f_2(z) dz \wedge \overline{dz} \\ &= \frac{1}{4\pi} \int_{\mathcal{F}_N} d \left(\varphi_1(z) \overline{f_2(z)} dz \right) \\ &= \frac{1}{4\pi} \int_{\partial \mathcal{F}_N} \varphi_1(z) \overline{f_2(z)} dz \\ &= \frac{1}{4\pi} \sum_{\gamma \in \mathcal{S}} \int_{(\gamma)} \varphi_1(z) \overline{f_2(z)} dz \\ &= \frac{1}{8\pi} \sum_{\gamma \in \mathcal{S}} \left(\int_{(\gamma)} \varphi_1(z) \overline{f_2(z)} dz + \int_{(\gamma^*)} \varphi_1(z) \overline{f_2(z)} dz \right) . \end{aligned}$$

En effet, l'application $*$ est une involution. La $\Gamma_0(N)$ -invariance de $f_2(z)dz$ nous donne :

$$\begin{aligned}
(f_1, f_2) &= \frac{1}{8\pi} \sum_{\gamma} \int_{(\gamma)} (\varphi_1(z) - \varphi_1(s(\gamma)z)) \overline{f_2(z)} dz \\
&= \frac{-1}{8\pi} \sum_{\gamma} \omega_1(s(\gamma)) \int_{(\gamma)} \overline{f_2(z)} dz \\
&= \frac{-i}{16\pi^2} \sum_{\gamma} \omega_1(s(\gamma)) \left(\overline{\varphi_2(\gamma(\infty)) - \varphi_2(\gamma(0))} \right) \\
&= \frac{-i}{16\pi^2} \sum_{\gamma} \omega_1(s(\gamma)) \overline{\varphi_2(\gamma(\infty))} + \frac{i}{16\pi^2} \sum_{\gamma} \omega_1(s(\gamma)) \overline{\varphi_2(\gamma(0))} .
\end{aligned}$$

Dans la première somme, on effectue le changement de variables $\gamma \leftrightarrow \gamma^*$. On utilise que :

- d'une part $\omega_1(s(\gamma^*)) = -\omega_1(s(\gamma))$;
- et d'autre part $\varphi_2(\gamma^*(\infty)) = \varphi(s(\gamma)^{-1}\gamma(0)) = \varphi_2(\gamma(0)) - \omega_2(s(\gamma))$.

On obtient alors :

$$(f_1, f_2) = \frac{i}{16\pi^2} \left(2 \sum_{\gamma} \omega_1(s(\gamma)) \overline{\varphi_2(\gamma(0))} - \sum_{\gamma} \omega_1(s(\gamma)) \overline{\omega_2(s(\gamma))} \right) .$$

Or,

$$\begin{aligned}
\sum_{\gamma} \omega_1(s(\gamma)) \overline{\varphi_2(\gamma(0))} &= \sum_{\gamma} \omega_1(s(\gamma TS)) \overline{\varphi_2(\gamma(\infty))} \\
&= \sum_{\gamma} \omega_1(t(\gamma)) \overline{\varphi_2(\gamma(\infty))} \\
&= \sum_{\tau\text{-orbites}} \sum_{j=1}^k \omega_1(t(\gamma_j)) \overline{\varphi_2(\gamma_j(\infty))} \\
&= \sum_{\text{orbites}} \sum_{j=1}^k \omega_1(t(\gamma_j)) \left(\overline{\varphi_2(\gamma_j(\infty)) - \varphi_2(\gamma_1(\infty))} \right) \\
&= \sum_{\text{orbites}} \sum_{j=1}^k \sum_{i=1}^{j-1} \omega_1(t(\gamma_j)) \left(\overline{\varphi_2(\gamma_{i+1}(\infty)) - \varphi_2(\gamma_i(\infty))} \right) \\
&= - \sum_{\text{orbites}} \sum_{j=1}^k \sum_{i=1}^{j-1} \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} .
\end{aligned}$$

Dans cette suite d'égalités, on a utilisé la formule (II.2). La formule (II.3) nous donne :

$$\begin{aligned} \sum_{\gamma} \omega_1(s(\gamma)) \overline{\omega_2(s(\gamma))} &= \sum_{\gamma} \omega_1(t(\gamma)) \overline{\omega_2(t(\gamma))} \\ &= \sum_{\text{orbites}} \sum_{j=1}^k \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_j))} . \end{aligned}$$

Finalement :

$$\begin{aligned} (f_1, f_2) &= \frac{-i}{16\pi^2} \sum_{\text{orbites}} \left(2 \sum_{j=1}^k \sum_{i=1}^{j-1} \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} + \sum_{j=1}^k \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_j))} \right) \\ &= \frac{-i}{16\pi^2} \sum_{\text{orbites}} \left(\sum_{j=1}^k \sum_{i=1}^j \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} - \sum_{j=1}^k \sum_{i=j}^k \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} \right) \\ &= \frac{-i}{16\pi^2} \sum_{\text{orbites}} \left(\sum_{j=1}^k \sum_{i=1}^j \omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} - \sum_{j=1}^k \sum_{i=j}^k \omega_1(t(\gamma_i)) \overline{\omega_2(t(\gamma_j))} \right) \\ &= \frac{i}{16\pi^2} \sum_{\text{orbites}} \left(\sum_{j=1}^k \sum_{i=j+1}^k \left(\omega_1(t(\gamma_j)) \overline{\omega_2(t(\gamma_i))} - \omega_1(t(\gamma_i)) \overline{\omega_2(t(\gamma_j))} \right) \right) . \end{aligned}$$

Et le théorème est montré. \square

Corollaire II.2.1 *Avec les notations précédentes :*

$$\|f_1\|^2 = \frac{-1}{8\pi^2} \sum_{\tau\text{-orbites}} \sum_{1 \leq j < i \leq k} \Im m \left(\omega_1(t(\gamma_j)) \overline{\omega_1(t(\gamma_i))} \right) .$$

Preuve : On prend $f_2 = f_1$ dans le théorème. \square

Dans [Cremona 2], on utilise la formule du corollaire pour calculer $\|f\|^2$ et en déduire de nombreux degrés modulaires. Cela fournit une méthode assez efficace. Cependant lorsque le conducteur est grand, la détermination de \mathcal{S} et le calcul des périodes $\omega(\gamma)$ prennent beaucoup de temps.

II.3 Utilisation des séries L

II.3.1 Le carré symétrique imprimitif

Revenons aux notations de II.1 ; E est donc une courbe elliptique définie sur \mathbb{Q} , de conducteur N et f est la forme modulaire associée à E . On cherche à calculer $\|f\|^2$. Le développement de Fourier de f à l'infini est de la forme :

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n , \quad q = e^{2i\pi\tau} .$$

La série de Hasse-Weil de E , $L(E, s)$ est égale à la série L de f ; en d'autres termes, nous avons :

$$L(E, s) = L(f, s) = \sum_n a_n n^{-s} .$$

Cette série possède un développement en produit Eulérien :

$$L(E, s) = \prod_p L_p(E, p^{-s})^{-1} ,$$

où $L_p(E, X) = (1 - \alpha_p X)(1 - \beta_p X)$, avec $\alpha_p + \beta_p = a_p$ et :

$$\begin{aligned} |\alpha_p| &= |\beta_p| = \sqrt{p} \quad , \text{ si } p \nmid N \quad . \\ \beta_p &= 0 \text{ et } \alpha_p = \pm 1 \quad (\text{resp. } \alpha_p = 0) \text{ si } p \parallel N \quad (\text{resp. si } p^2 \mid N) \quad . \end{aligned}$$

Ce produit Eulérien permet de définir le carré symétrique imprimitif de $L(f, s)$, on pose :

$$L(\mathcal{I}^2 f, s) = \prod_p (1 - \alpha_p^2 p^{-s})^{-1} (1 - \alpha_p \beta_p p^{-s})^{-1} (1 - \beta_p^2 p^{-s})^{-1} \quad , \quad (\text{II.4})$$

$$= \frac{\zeta_N(2s-2)}{\zeta_N(s-1)} \sum_{n=1}^{\infty} \frac{a_n^2}{n^s} \quad , \quad \Re(s) > 2 \quad . \quad (\text{II.5})$$

Ici, la fonction ζ_N désigne la fonction ζ de Riemann dans laquelle on a enlevé les facteurs Eulériens des nombres premiers p divisant le conducteur N ; c'est-à-dire :

$$\zeta_N(s) = \sum_{\text{pgcd}(n, N)=1} n^{-s} .$$

Il a été établi par Shimura et indépendamment par Zagier que la fonction $L(\mathcal{I}^2 f, s)$ se prolonge en une fonction holomorphe sur tout le plan complexe. La méthode de Rankin permet en outre d'obtenir (cf. [Shimura 2]) :

$$\|f\|^2 = \frac{N}{8\pi^3} L(\mathcal{I}^2 f, 2) \quad .$$

Ainsi, il ne reste plus qu'à évaluer la fonction $L(\mathcal{I}^2 f, s)$ en $s = 2$. Mais tout d'abord, on observe que le carré symétrique imprimitif n'est quasiment pas modifié lorsqu'on remplace E par une de ses tordues quadratiques.

Théorème IV *Soit E' une courbe elliptique tordue quadratique de E de conducteur N' avec $\text{ord}_p(N') \leq \text{ord}_p(N)$ pour tout p premier, et avec $L(E', s) = \sum_n a'_n n^{-s}$. On pose $N = MD_1^2 D_2^2 2^k$ et $N' = MD_2^2 2^\lambda$ où M , D_1 et D_2 sont impairs, D_1 et D_2 sont sans*

facteur carré et où $\lambda \leq k$. On a :

$$\begin{aligned} \|f\|^2 &= \|f'\|_{\sim}^2 \frac{1}{D_1} \prod_{p|D_1} (p-1)(p+1-a'_p)(p+1+a'_p) \\ &\times \frac{1}{D_2} \prod_{p|D_2} (p-1)(p+1) \\ &\times \begin{cases} 2^{k-3}(3-a'_2)(3+a'_2) & \text{si } \lambda = 0, k \geq 4 \\ 2^{k-3} \times 3 & \text{si } \lambda = 1, k \neq \lambda \\ 2^{k-\lambda} & \text{si } 2 \leq \lambda \leq k \text{ ou si } \lambda = k \end{cases} . \end{aligned}$$

Le symbole $\|\cdot\|_{\sim}$ signifie que l'on prend la norme dans le bon espace (ici dans $X_0(N')$).

Preuve : Prenons E' une courbe elliptique tordue de E par un caractère de conducteur premier $p \geq 5$. Supposons que $\text{ord}_p(N') < \text{ord}_p(N)$ (sinon il ne se passe rien). Pour tous les nombres premiers $q \neq p$, les facteurs Eulériens $L_q(\mathcal{I}^2 f, X)$ et $L_q(\mathcal{I}^2 f', X)$ sont les mêmes car le caractère quadratique est tué en prenant les carrés. On sait que $p^2 | N$, donc $a_p = 0$ et $L_p(\mathcal{I}^2 f, X) = 1$.

Si $\text{pgcd}(N', p) = 1$, on a alors :

$$L(\mathcal{I}^2 f, s) = L(\mathcal{I}^2 f', s) \times (1 - \alpha_p'^2 p^{-s})(1 - pp^{-s})(1 - \beta_p'^2 p^{-s}) .$$

En prenant $s = 2$, on obtient :

$$\|f\|^2 = \|f'\|_{\sim}^2 \frac{(p-1)(p+1-a'_p)(p+1+a'_p)}{p} .$$

Si $\text{pgcd}(N', p) = p$ alors $L_p(\mathcal{I}^2 f', X) = 1 - X$ et :

$$L(\mathcal{I}^2 f, s) = L(\mathcal{I}^2 f', s)(1 - p^{-s}) .$$

Ainsi $\|f\|_N^2 = \|f'\|_{\sim}^2 (p-1)(p+1)/p$. Les cas $p = 2$ et 3 , se traitent par un raisonnement similaire. Le théorème se montre ensuite en récapitulant pour tous les nombres premiers, les égalités que l'on vient d'établir. \square

Grâce à ce théorème, on peut facilement obtenir une relation entre $\deg(\varphi)$ et $\deg(\varphi')$. Il permet aussi de restreindre notre étude aux courbes elliptiques qui ne sont pas des tordues quadratiques d'une courbe elliptique de conducteur plus petit.

II.3.2 Le carré symétrique primitif

Nous supposons dans toute cette partie que E a un conducteur minimal parmi la famille de ses tordues quadratiques.

Le carré symétrique imprimitif a un inconvénient majeur ; il ne possède pas d'équation

fonctionnelle traditionnelle. Il est donc difficile de trouver une méthode directe pour évaluer cette fonction en un point. Pour palier ce défaut, il faut corriger certains facteurs Eulériens de cette série L et définir le carré symétrique primitif :

$$L(\mathcal{P}^2 f, s) = L(\mathcal{I}^2 f, s) \prod_{p(*)} L_p(\mathcal{P}^2 f, p^{-s})^{-1} ,$$

où le produit $(*)$ porte sur l'ensemble fini des nombres premiers pour lesquels $p^2 \mid N$. En donnant les bons facteurs Eulériens pour $L(\mathcal{P}^2 f, s)$, nous allons en même temps définir un nombre entier positif B qui nous servira dans la suite.

Si $p^2 \nmid N$, on sait déjà que $L_p(\mathcal{P}^2 f, X) = L_p(\mathcal{I}^2 f, X)$, de plus on a $\text{ord}_p(B) = \text{ord}_p(N)$. Supposons maintenant que $p^2 \mid N$.

Pour $p \neq 2, 3$ alors $\text{ord}_p(B) = 1$ et $L_p(\mathcal{P}^2 f, X) = 1 - pX$ ou $1 + pX$ dépendant des propriétés d'une certaine extension de corps. Dans [Watkins], on peut néanmoins trouver le critère simple suivant. On a $L_p(\mathcal{P}^2 f, X) = 1 - pX$ si et seulement si l'une des conditions suivantes est vérifiée :

- $p \equiv 1 \pmod{12}$;
- $p \equiv 5 \pmod{12}$, $p^2 \mid c_6$ et $p^2 \nmid c_4$;
- $p \equiv 7 \pmod{12}$ et soit $p^2 \nmid c_6$, soit $p^2 \mid c_6$ et $p^2 \mid c_4$.

Si $p = 2$ ou 3 , les tableaux II.1 et II.2 donnent toutes les possibilités sur les facteurs Eulériens. Celles-ci se déduisent de [Coates-Schmidt], il faut cependant faire attention au cas $2^8 \mid N$ pour lequel les auteurs ont oublié deux possibilités.

$\text{ord}_2(N)$	$\text{ord}_2(B)$	$L_2(\mathcal{P}^2 f, X)$
2	1	$1 + pX$
3	2	1
5	3	1
7	4	1
8	3	$1 + pX$
	3	$1 - pX$
	4	1

TAB. II.1 – Facteurs locaux en $p = 2$

Pour $p = 2$, le seul cas ambigu est $2^8 \mid N$ pour lequel :

- si $2^9 \mid c_6$ alors $L_2(\mathcal{P}^2 f, X) = 1$;
- si $2^9 \nmid c_6$ et $c_4 \equiv \varepsilon 32 \pmod{128}$ alors $L_p(\mathcal{P}^2 f, X) = 1 + \varepsilon pX$, où $\varepsilon = \pm 1$.

$\text{ord}_3(N)$	$\text{ord}_3(B)$	$L_3(\mathcal{P}^2 f, X)$
2	1	$1 + pX$
3	2	1
4	2	$1 + pX$
	2	$1 - pX$
5	3	1

TAB. II.2 – Facteurs locaux en $p = 3$

Pour $p = 3$, $3^4 \parallel N$ est le seul cas ambigu et $L_p(\mathcal{P}^2 f, X) = 1 - pX$ si et seulement si une des deux conditions est satisfaite :

- $c_4 \equiv 27 \pmod{81}$;
- $c_4 \equiv 9 \pmod{27}$ et $c_6 \equiv \pm 108 \pmod{243}$.

On a maintenant toutes les notations et outils nécessaires pour énoncer un théorème dû à Coates et Schmidt (cf. [Coates-Schmidt]) :

Théorème V (Coates-Schmidt) *La fonction $L(\mathcal{P}^2 f, s)$ se prolonge en une fonction holomorphe sur tout le plan complexe et vérifie l'équation fonctionnelle :*

$$\Lambda(\mathcal{P}^2 f, s) = \Lambda(\mathcal{P}^2 f, 3 - s) \quad ,$$

où

$$\Lambda(\mathcal{P}^2 f, s) = \left(\frac{B}{2\pi^{3/2}} \right)^s \Gamma(s) \Gamma\left(\frac{s}{2}\right) L(\mathcal{P}^2 f, s) \quad .$$

Remarques : 1) On peut aussi définir le carré symétrique primitif dans le cas où E est tordue quadratique d'une courbe elliptique E' ayant un conducteur plus petit, on a alors $L(\mathcal{P}^2 f, s) = L(\mathcal{P}^2 f', s)$. Ce fait n'est en général pas vrai pour les carrés symétriques imprimitifs.

2) Si le conducteur N est sans facteur carré, alors $L(\mathcal{P}^2 f, s) = L(\mathcal{I}^2 f, s)$ et $B = N$. Dans ce cas, il n'y a donc pas de corrections à effectuer.

3) On associe à E un objet géométrique appelé carré symétrique de E . Grâce aux techniques de Serre (cf. [Serre]), on peut définir pour cet objet une série L qui est précisément le carré symétrique primitif que nous avons défini. C'est en fait cette série L et cet objet géométrique que Coates et Schmidt étudient dans leur article ([Coates-Schmidt]).

II.3.3 Calcul de $L(\mathcal{P}^2 f, s)$

Avec les notations précédentes, on pose :

$$\begin{aligned} C &= \frac{B}{2\pi^{3/2}} \quad , \\ \gamma(s) &= C^s \Gamma(s) \Gamma\left(\frac{s}{2}\right) \quad . \end{aligned}$$

On écrit :

$$L(\mathcal{P}^2 f, s) = \sum_{n \geq 1} b_n n^{-s} . \quad (\text{II.6})$$

La définition de $L(\mathcal{P}^2 f, s)$ permet de calculer facilement les coefficients b_n de cette série de Dirichlet. La majoration $a_p \leq 2\sqrt{p}$ pour p premier sur les coefficients de la forme f , et le développement en produit Eulérien de $L(\mathcal{P}^2 f, s)$, nous donnent $b_n < n^2$. De plus, des techniques classiques de théorie analytique des nombres sur l'équation fonctionnelle de $\Lambda(\mathcal{P}^2 f, s)$ permettent d'obtenir (cf. [Kowalski]) :

$$L(\mathcal{P}^2 f, 2) = \sum_{n \leq X} \frac{b_n}{n^2} + O(B^2 X^{-1}) . \quad (\text{II.7})$$

Cette formule implique que la série $\sum_n b_n/n^2$ converge vers $L(\mathcal{P}^2 f, 2)$. Cependant, cette méthode n'est pas très efficace pour calculer $\|f\|^2$ car la convergence est très lente.

La série $L(\mathcal{P}^2 f, s)$ vérifie une équation fonctionnelle de type classique et on peut appliquer la technique décrite dans ([Cohen 2], chapitre 10) pour évaluer $\Lambda(\mathcal{P}^2, s)$ en un point $s \in \mathbb{C}$.

Proposition II.3.1 *On a :*

$$\Lambda(\mathcal{P}^2 f, s) = \sum_{n \geq 1} \frac{b_n}{n^s} F(s, n) + \sum_{n \geq 1} \frac{b_n}{n^{3-s}} F(3-s, n) , \quad (\text{II.8})$$

où

$$F(s, x) = C^s \Gamma(s) \Gamma\left(\frac{s}{2}\right) - \int_0^x \frac{1}{2i\pi} \int_{\Re(z)=\delta} t^{-z} C^z \Gamma(z) \Gamma(z/2) dz t^{s-1} dt$$

pour tout $\delta > 0$.

La série (II.8) est rapidement convergente et donc pratique pour les calculs numériques. Plus précisément, on a :

Proposition II.3.2 *Soit $s = \sigma + it$ et $A = \frac{x}{2^{1/4}C}$ alors :*

$$|F(s, x)| \leq 7 \frac{x^\sigma}{A - \sigma A^{1/3}} e^{-\frac{3}{2} A^{2/3}} .$$

Preuve : Tout d'abord, on doit estimer les facteurs gammas. Pour cela, on utilise la formule $\Gamma(s) = \sqrt{2\pi} s^{s-1/2} e^{-s} e^{R(s)}$, où $|R(s)| \leq 1/(6|s|)$ pour obtenir les deux majorations suivantes :

$$\left| \Gamma\left(\frac{\delta + iT}{2}\right) \Gamma(\delta + iT) \right| \leq \pi 2^{\frac{\delta}{4}+1} \delta^{\frac{3\delta}{2}-1} e^{-\frac{3\delta}{2}} e^{\frac{1}{2\delta}} e^{-\frac{T^2}{2\delta}(\frac{T^2}{\delta^2}-3)} \text{ pour tout } T \leq \delta , \quad (\text{II.9})$$

$$\left| \Gamma\left(\frac{\delta + iT}{2}\right) \Gamma(\delta + iT) \right| \leq \pi 2^{\frac{\delta}{4}+1} T^{\frac{3\delta}{2}-1} e^{-\frac{3\pi T}{4}} e^{\frac{1}{2\sqrt{2}\delta} + \frac{\delta}{2}} \text{ pour tout } T > \delta . \quad (\text{II.10})$$

Ensuite, on a :

$$\begin{aligned} F(s, x) &= \gamma(s) - \int_0^x \frac{1}{2i\pi} \int_{\Re(z)=\delta} t^{-z} \gamma(z) dz t^{s-1} dt \\ &= \frac{1}{2i\pi} \int_{\Re(z)=\delta} C^z x^{s-z} \Gamma(z) \Gamma\left(\frac{z}{2}\right) \frac{dz}{z-s} . \end{aligned}$$

Et donc :

$$|F(s, x)| \leq \frac{1}{2\pi} C^\delta \frac{x^{\sigma-\delta}}{\delta-\sigma} \int_{\mathbb{R}} \left| \Gamma\left(\frac{\delta+iT}{2}\right) \Gamma(\delta+iT) \right| dT .$$

Comme $|\Gamma(z)| = |\Gamma(\bar{z})|$, il suffit de majorer l'intégrale sur $[0, +\infty]$. On pose :

$$I = \int_0^\infty \left| \Gamma\left(\frac{\delta+iT}{2}\right) \Gamma(\delta+iT) \right| dT = I_1 + I_2 \quad \text{avec :}$$

$$\begin{aligned} I_1 &= \int_0^\delta \left| \Gamma\left(\frac{\delta+iT}{2}\right) \Gamma(\delta+iT) \right| dT , \\ I_2 &= \int_\delta^\infty \left| \Gamma\left(\frac{\delta+iT}{2}\right) \Gamma(\delta+iT) \right| dT . \end{aligned}$$

Les inégalités (II.9) et (II.10) appliquées à I_1 et I_2 respectivement donnent :

$$I \leq 3.6\pi^{3/2} \delta^{\frac{3\delta-1}{2}} e^{-\frac{3\delta}{2}} 2^{\frac{\delta}{4}} .$$

En revenant à $F(s, x)$, on obtient :

$$|F(s, x)| \leq 3.6\sqrt{\pi} \frac{x^\sigma}{\delta-\sigma} \left(\frac{x}{2^{1/4}C} \right)^{-\delta} \delta^{-\frac{3\delta-1}{2}} e^{-\frac{3\delta}{2}} .$$

Cette inégalité a été établie pour tout $\delta > 0$. Le choix $\delta = \left(\frac{x}{2^{1/4}C} \right)^{2/3}$ prouve la majoration attendue. \square

Cette proposition permet, non seulement de voir que (II.8) converge rapidement, mais aussi d'évaluer l'erreur commise lorsque nous tronquons la série. Il ne nous reste plus qu'à calculer $F(s, x)$. Pour cela, on déplace la droite d'intégration $\Re(z) = \delta$ vers la gauche en faisant apparaître les contributions de tous les pôles de la fonction $t^{-z}\gamma(z)$. On obtient :

Proposition II.3.3

$$F(s, x) = \gamma(s) - \sum_{q=0}^{\infty} x^{s+2q} \left(\frac{v_{2q} - \log(x)u_{2q}}{s+2q} + \frac{u_{2q}}{(s+2q)2} + \frac{xu_{2q+1}}{s+2q+1} \right) , \quad (\text{II.11})$$

avec

$$\begin{aligned} u_{2q} &= \frac{2(-1)^q}{C^{2q}q!(2q)!} , \\ u_{2q+1} &= \frac{(-1)^q \sqrt{\pi} 2^{2q+1} q!}{(2q+1)!^2 C^{2q+1}} , \\ v_{2q} &= \frac{2(-1)^q}{C^{2q}q!(2q)!} \left(\log(C) - \frac{3}{2}\gamma + \frac{1}{2} \sum_{j=1}^q j^{-1} + \sum_{j=1}^{2q} j^{-1} \right) . \end{aligned}$$

Les termes u_q et v_{2q} se calculent récursivement et rapidement lors de l'évaluation de la série. Dans la pratique, on calcule N_0 tel que :

$$\left| \sum_{n=N_0+1}^{\infty} \frac{b(n)}{n^s} F(s, n) \right| < \varepsilon \quad \text{et} \\ \left| \sum_{n=N_0+1}^{\infty} \frac{b(n)}{n^{3-s}} F(3-s, n) \right| < \varepsilon \quad .$$

Puis, on somme les i_0 premiers termes de la série (II.11), où i_0 est le plus petit entier tel que (cf. [Tollis]) :

$$C^2 N_0^{-i_0-1/2} \left\lfloor \frac{i_0}{2} \right\rfloor! i_0! > \frac{10N_0}{\pi\varepsilon} \quad .$$

Remarque : L'évaluation de la série (II.11) pour x grand pose des problèmes numériques (du même ordre que si l'on voulait calculer $\exp(-x)$ avec x grand, en utilisant la série $\sum_n x^n/n!$). Il faut donc être très vigilant quant à son utilisation ; on peut, par exemple, doubler la précision avec laquelle nous faisons les calculs, comme le fait remarquer Tollis ([Tollis]).

Toutes ces formules nous donnent une méthode pour calculer $\Lambda(\mathcal{P}^2 f, s)$; en l'appliquant à $s = 2$, on en déduit $L(\mathcal{I}^2 f, 2)$ puis $\|f\|^2$ et enfin $\deg(\varphi)$ (par II.1). Une vérification des calculs numériques est donnée par le fait que $\deg(\varphi)$ doit être un entier.

Cette méthode est très rapide et permet de calculer de nombreux degrés modulaires en peu de temps.

Exemple : Prenons l'exemple de la courbe elliptique E de conducteur $N = 11$ et d'équation : $y^2 + y = x^3 - x^2 - 10x - 20$. Il faut environ 25 termes dans les séries (II.8) et moins de 25 termes dans la série (II.11) pour calculer $L(\mathcal{P}^2 f, 2)$ à 10^{-4} près. On obtient alors $\|f\|^2 \approx 0.0469$ et $\deg(\varphi) \approx 0.999996$. On en déduit que $\deg(\varphi) = 1$.

Remarque : Lors de la préparation de ce travail, nous avons été informé de l'existence du preprint ([Watkins]) de Watkins, où une méthode similaire (mais pas aussi détaillée) est utilisée pour calculer de nombreux et intéressants degrés modulaires.

II.3.4 Ordres de grandeurs

Dans la formule (II.1), on a exprimé $\deg(\varphi)$ en fonction de $\|f\|^2$. Un des avantages de ceci est que l'on sait majorer $\|f\|^2$. En effet, l'équation fonctionnelle de $L(\mathcal{P}^2, s)$ permet d'obtenir :

$$\|f\|^2 \ll_{\varepsilon} N^{1+\varepsilon} \quad .$$

En fait, on peut remplacer N^{ε} par une puissance convenable de $\log(N)$. On voit donc qu'une bonne estimation de $\text{Vol}(E)$ doit donner aussi une bonne estimation de $\deg(\varphi)$ (modulo la constante de Manin).

Proposition II.3.4 *Soit C un réel positif. Il existe $a \in \mathbb{R}$ et $A \in \mathbb{R}$ dépendant de C telle que :*

$$|j(E)| \leq C \implies a|\Delta_{\min}|^{-1/6} < \text{Vol}(E) < A|\Delta_{\min}|^{-1/6} ,$$

où Δ_{\min} est le discriminant minimal de E .

Preuve : En faisant un changement de variables classique de paramètres (u, r, s, t) , l'invariant j est bien sûr inchangé alors que $\text{Vol}(E)$ est multiplié par u^2 et Δ par u^{-12} . L'estimation de la proposition dépend donc pas du modèle et on peut supposer que E est donnée par $y^2 = 4x^3 - Ax - B$. En désignant par e_1, e_2 et e_3 les racines du polynôme $P(x) = 4x^3 - Ax - B$ (on a $e_1 + e_2 + e_3 = 0$) et par $v \in \mathbb{C}$ tel que $e_2 = ve_1$ (on suppose que $e_1 \neq 0$), on a $\Delta = 16e_1^6(v-1)^2(v+2)^2(2v+1)^2$ et $j = 2^8 3^3 (v^2 + v + 1)^2 (v-1)^{-2} (v+2)^{-2} (2v+1)^{-2}$. Si $\Delta > 0$, les racines e_1, e_2 et e_3 sont réelles, supposons de plus que $e_1 < e_2 < e_3$. Alors les périodes ω_1 et ω_2 de E sont données par les intégrales :

$$\omega_1 = \int_{e_1}^{e_2} \frac{dx}{\sqrt{P(x)}} \quad \text{et} \quad \omega_2 = i \int_{e_2}^{e_3} \frac{dx}{\sqrt{-P(x)}} .$$

Une estimation directe permet d'obtenir les encadrements suivants :

$$\begin{aligned} \frac{\pi}{2} \frac{1}{\sqrt{e_3 - e_1}} &\leq \omega_1 \leq \frac{\pi}{2} \frac{1}{\sqrt{e_3 - e_2}} , \\ \frac{\pi}{2} \frac{1}{\sqrt{e_3 - e_1}} &\leq \omega_2/i \leq \frac{\pi}{2} \frac{1}{\sqrt{e_2 - e_1}} . \end{aligned}$$

Et ainsi,

$$\frac{\pi^{12}}{4^6} \frac{|v-1|^2 |2v+1|^2}{|v+2|^4} \leq \text{Vol}(E)^6 |\Delta| \leq \frac{\pi^{12}}{4^6} \frac{|2v+1|^2}{|1-v||v+2|} .$$

Comme j est borné, les nombres $|1-v|$, $|v+2|$ et $|2v+1|$ sont tous minorés par un nombre strictement positif. Un calcul analogue permet de traiter le cas $\Delta < 0$. \square

En admettant la conjecture de Manin, la proposition II.3.4 nous fournit la majoration $\deg(\varphi) \ll N^{1+\varepsilon} \Delta^{1/6}$ pour les courbes elliptiques d'invariants j bornés. Dans ([Szpiro]), Szpiro propose la conjecture selon laquelle le rapport :

$$\sigma(E) = \frac{\log(|\Delta_{\min}|)}{\log(N)}$$

est borné. Le nombre $\sigma(E)$ s'appelle le rapport de Szpiro de E . On peut montrer que $\sigma(E) \geq 6$ pour une infinité de courbes. La conjecture de Szpiro permet d'obtenir des bornes polynômiales sur $\deg(\varphi)$ (toujours modulo la constante de Manin). On voit aussi qu'il existe un lien étroit entre $\sigma(E)$ et l'ordre de grandeur de $\deg(\varphi)$. En particulier, une courbe ayant un degré modulaire élevé devrait avoir un grand rapport de Szpiro. Le tableau II.3 donne la liste des 10 plus grands degrés modulaires parmi les courbes de

conducteur $N < 5000$. On note $[a_1, a_2, a_3, a_4, a_6]$ les coefficients de la courbe E de sorte que :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 .$$

$[a_1, a_2, a_3, a_4, a_6]$	N	$\deg(\varphi)$	$\sigma(E)$
$[1, 0, 0, -190366575, 325694589866937]$	3990	14857920	8.792
$[1, -1, 1, -48728476146, 4140222075962097]$	4898	13895640	5.929
$[1, -1, 1, 1082069572, 90485275778687]$	3870	8547840	8.517
$[1, -1, 0, -1037153740, 12855149477425]$	3995	3552320	6.987
$[1, 0, 1, -454511321, -1733886056644]$	4434	3046080	7.588
$[1, -1, 0, -1165563934, 15316534975252]$	4294	2847600	5.101
$[1, 0, 0, -2099919255, -37089124766487]$	3486	2709504	7.681
$[1, 0, 1, -8682871045, 311416866934832]$	3054	2356200	5.306
$[1, 1, 1, -1364688305, 19403731837775]$	4290	2322432	6.439
$[1, 0, 1, -4473924258, 115180683613556]$	4390	2234624	6.286

TAB. II.3 – Grands degrés modulaires pour $N < 5000$

En fait, ces degrés sont très grands ; la moyenne de $\deg(\varphi)$ pour toutes les courbes modulaires de conducteur < 5000 est d'environ 12000. Les rapports de Szpiro que l'on obtient sont aussi importants (en principe, le rapport de Szpiro d'une courbe est proche de 1).

Remarque : La courbe elliptique de conducteur $N = 1290$ et d'équation :

$$y^2 + xy + y = x^3 + 120229952x - 3351306510322 ,$$

pour laquelle $\deg(\varphi) = 1068480$ possède un rapport de Szpiro $\sigma(E) \approx 8.903$. C'est le plus grand rapport de Szpiro que je connais.

Lorsque le rapport de Szpiro est petit, le degré se contrôle mieux. En particulier, on a :

Proposition II.3.5 *Soit \mathcal{E} une famille de courbes elliptiques définies sur \mathbb{Q} telle que :*

- $j(E)$ est borné pour $E \in \mathcal{E}$.
- $\Delta_{\min}(E)$ est sans facteur carré.

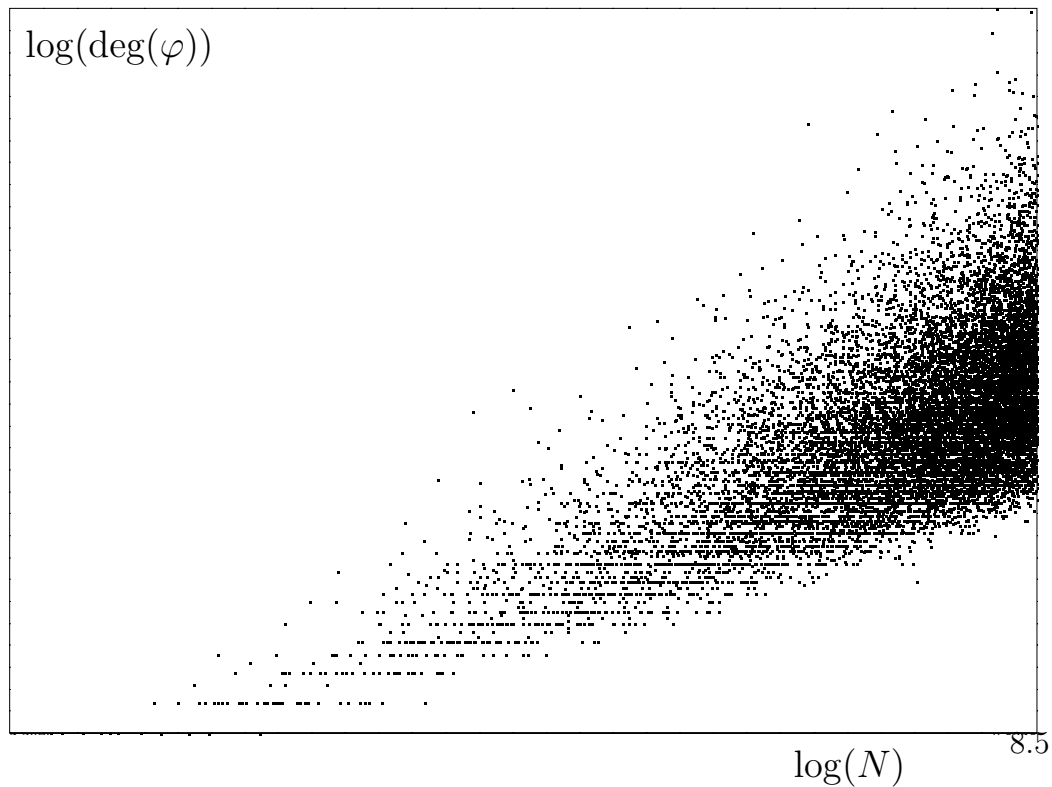
alors

$$\deg(\varphi) \ll N^{7/6} \log(N)^3 \quad (N \rightarrow +\infty) .$$

Preuve : Dans les conditions de la proposition le conducteur N de $E \in \mathcal{E}$ est égal au discriminant de E . On utilise la proposition II.3.4 et la formule (II.1). La borne supérieure provient alors de $L(\mathcal{P}^2 f, 2) \ll \log(N)^3$ et du fait que la constante de Manin est bornée lorsque le conducteur est sans facteur carré. \square

Pour visualiser graphiquement la croissance de $\deg(\varphi)$ en fonction de N , nous avons tracé, dans la figure II.1, le nuage de points de coordonnées $(\log(N), \log(\deg(\varphi)))$ correspondant aux premières courbes elliptiques de conducteur N .

13.8

FIG. II.1 – Croissance de $\deg(\varphi)$

La famille de courbes elliptiques $E_k : y^2 + xy = x^3 + k$ (avec $k(432k + 1)$ sans facteur carré) donne un exemple d'une famille infinie de courbes vérifiant les hypothèses de la proposition II.3.5. Comme Δ_{min} est sans facteur carré, le conducteur N est égal au discriminant Δ_{min} et par conséquent N est aussi sans facteur carré (la courbe est semi-stable). La famille E_k (avec $k(432k + 1)$ sans facteur carré) fournit donc une infinité de courbes elliptiques semi-stables ayant un invariant j borné.

Dans le cas où la famille \mathcal{E} est infinie, la puissance $N^{7/6}$ de la proposition II.3.5 est optimale, en effet :

Proposition II.3.6 *Soit \mathcal{E} une famille infinie de courbes elliptiques définies sur \mathbb{Q} telle que :*

- *$j(E)$ est borné pour $E \in \mathcal{E}$.*
- *E est semi-stable (i.e. N est sans facteur carré).*

alors

$$\deg(\varphi) \gg N^{7/6} \log(N) \quad (N \rightarrow +\infty) .$$

Preuve : Cette borne inférieure provient de la majoration très profonde :

$$L(\mathcal{P}^2 f, 2) \gg 1/\log(N)$$

prouvée par Goldfeld, Hoffstein et Lieman dans le cas où le conducteur N est sans facteur carré ([Goldfeld-Hoffstein-Lieman]). □

Chapitre III

Points de ramification du revêtement modulaire

Dans ce chapitre, on s'intéresse aux points de ramification du revêtement modulaire d'une courbe elliptique. En particulier, on donne une méthode numérique pour les déterminer tous. On essaie d'obtenir, de façon plus ou moins expérimentale, quelques propriétés de ces points spéciaux.

III.1 Points critiques et points de ramification

III.1.1 Définitions et motivations

1 Contexte général

Afin de fixer les notations, nous suivons [Shimura 1] dans un cadre général.

Soient X et X' deux surfaces de Riemann compactes et $\varphi : X \rightarrow X'$ une application holomorphe non constante. On fixe $z_0 \in X$ et on pose $z'_0 = \varphi(z_0) \in X'$. Si u et u' sont des paramètres locaux aux points z_0 et z'_0 qui s'annulent en z_0 et z'_0 , on peut écrire le développement de φ dans un voisinage de z_0 :

$$u'(\varphi(z)) = a_e u(z)^e + a_{e+1} u(z)^{e+1} + \cdots, a_e \neq 0.$$

L'entier positif e , qui ne dépend que de z_0 , s'appelle l'indice de ramification de φ en z_0 . Si z_0, z_1, \dots, z_h sont les antécédents par φ de z'_0 et si $e_{z_1}, e_{z_2}, \dots, e_{z_h}$ sont leur indice de ramification respectif, on a :

$$\deg(\varphi) = e_{z_1} + e_{z_2} + \cdots + e_{z_h}. \quad (\text{III.1})$$

Il y a un nombre fini de points $c \in X$ pour lesquels $e_c > 1$; ce sont les points critiques de φ . D'après (III.1), si c est un tel point alors :

$$|\{\varphi^{-1}(\varphi(c))\}| < \deg(\varphi),$$

et $\varphi(c)$ est un point de ramification de φ . Pour tous les autres points $z \in X$ on a $e_z = 1$ et $\deg(\varphi)$ correspond bien au nombre d'antécédents de $\varphi(z)$. En un sens, $\deg(\varphi)$ est toujours égal au nombre d'antécédents, comptés avec multiplicité, d'un point $z' \in X'$.

Nous aurons aussi besoin de la formule d'Hurwitz :

$$2g - 2 = \deg(\varphi) (2g' - 2) + \sum_{z \in X} (e_z - 1) , \quad (\text{III.2})$$

où g et g' sont les genres de X et de X' respectivement.

2 Cas du revêtement modulaire

Prenons E une courbe elliptique définie sur \mathbb{Q} de conducteur N . Pour simplifier l'exposé, nous allons supposer que E est une courbe de Weil forte et que la conjecture de Manin est vérifiée. Tous les exemples numériques que nous allons prendre satisferont ces hypothèses. On considère

$$\varphi : X_0(N) \rightarrow E(\mathbb{C})$$

le revêtement modulaire de E .

On note ν_2 (resp. ν_3) le nombre de points elliptiques d'ordre 2 (resp. d'ordre 3) de $X_0(N)$, ν_∞ désigne le nombre de pointes et μ est l'indice de $\Gamma_0(N)$ dans $SL_2(\mathbb{Z})$.

Le genre g de $X_0(N)$ est alors donné par (cf. [Shimura 1]) :

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2} .$$

Comme le genre de $E(\mathbb{C})$ est 1, on constate, grâce à la formule d'Hurwitz, que φ admet exactement $2g - 2$ points critiques comptés avec multiplicité. Les points critiques de φ sont les zéros de la forme différentielle holomorphe $d\varphi = 2i\pi f(z)dz$ et nous sommes donc amenés à trouver tous les zéros de f . Cependant, un zéro de f n'est pas forcément un point critique car dz possède (seulement) une partie polaire :

$$\text{Div}(dz) = - \left(\sum_{j=1}^{\nu_\infty} P_j + \frac{1}{2} \sum_{j=1}^{\nu_2} e_j + \frac{2}{3} \sum_{j=1}^{\nu_3} e'_j \right) ,$$

où les P_j sont les pointes de $X_0(N)$ et e_j (resp. e'_j) sont les points elliptiques d'ordre 2 (resp. d'ordre 3). On voit ainsi qu'un point $z \in X_0(N)$ est critique si et seulement si z est un zéro de f ne provenant pas d'un pôle de dz . Par exemple, une pointe $P \in X_0(N)$ est un point critique si et seulement si l'ordre d'annulation de f en P est ≥ 2 .

Remarque : La forme $f(z)dz$ étant une forme différentielle holomorphe, tous les pôles de dz sont compensés par des zéros de f . La forme f s'annule donc aux points elliptiques (et aux pointes!). Avec les cartes locales que nous prenons, il faut faire attention à la multiplicité d'un zéro de f en un point elliptique d'ordre 2 (resp. d'ordre 3) car elle se compte par tranche de $1/2$ (resp. de $1/3$). C'est pourquoi un zéro simple (resp. double)

de f , vue comme fonction de \mathbb{H} dans \mathbb{C} , en un point elliptique d'ordre 2 (resp. d'ordre 3) compense exactement le pôle de dz associé.

Soit $c \in X_0(N)$ un point critique, $\varphi(c)$ est donc un point de ramification ; on peut montrer que $\varphi(c)$ est un point algébrique de $E(\overline{\mathbb{Q}})$ défini sur un corps de nombres K . Le point $\text{Tr}_{K/\mathbb{Q}}(\varphi(c))$ est alors un point rationnel de $E(\mathbb{Q})$. Une question naturelle, posée par Mazur et Swinnerton-Dyer dans [Mazur-Swinnerton-Dyer], est la détermination du groupe engendré par les $\text{Tr}_{K/\mathbb{Q}}(\varphi(c))$ pour c critique. On note $E(\mathbb{Q})^{\text{crit}}$ ce sous- groupe de $E(\mathbb{Q})$. On dit qu'un point critique c est un point critique fondamental si $c \in i\mathbb{R}_+ \subseteq X_0(N)$ (cf. [Mazur-Swinnerton-Dyer]). On note $E(\mathbb{Q})^{\text{fond}}$ le sous-groupe de $E(\mathbb{Q})$ engendré par les $\text{Tr}_{K/\mathbb{Q}}(\varphi(c))$, pour c critique fondamental.

En particulier, on trouve dans [Mazur-Swinnerton-Dyer] le théorème suivant :

Théorème VI (Mazur-Swinnerton-Dyer) *Soit E une courbe elliptique définie sur \mathbb{Q} . Le rang analytique de E est inférieur ou égal au nombre de points critiques fondamentaux d'ordre impair de E . De plus, ces deux nombres ont la même parité.*

Le but de ce chapitre est de donner une étude expérimentale de ces points particuliers du revêtement modulaire. Par exemple, les premières questions et les problèmes qui se posent sont :

- Calculer tous les points critiques de φ .
- Déterminer pour un point de ramification, un corps de nombre K dans lequel il est défini.
- Étudier les groupes $E(\mathbb{Q})^{\text{crit}}$ et $E(\mathbb{Q})^{\text{fond}}$; dire si ce sont des groupes de torsion ou non, etc ...

III.1.2 Localisation des zéros de f

On pose :

$$\begin{aligned}\alpha_j &= \begin{pmatrix} 0 & -1 \\ 1 & j-1 \end{pmatrix} \quad \text{pour } j = 1, 2, \dots, N, \\ \alpha_{N+1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

Puis, on choisit des matrices $\alpha_{N+2}, \dots, \alpha_\mu$ afin d'obtenir un système de représentants à droite de $SL_2(\mathbb{Z})$ modulo $\Gamma_0(N)$ i.e. :

$$SL_2(\mathbb{Z}) = \bigcup_{j=1}^{\mu} \Gamma_0(N) \alpha_j.$$

Remarquons que si N est premier, $\mu = N + 1$, et nous n'avons pas besoin de compléter l'ensemble $\{\alpha_1, \dots, \alpha_\mu\}$ initialement défini.

Soit :

$$\mathcal{F} = \{z \in \mathbb{H}, -\frac{1}{2} < \Re(z) \leq \frac{1}{2}, |z| \geq 1\}$$

le domaine fondamental classique de $SL_2(\mathbb{Z})$. On définit alors un domaine fondamental \mathcal{F}_N de $X_0(N)$ par :

$$\mathcal{F}_N = \bigcup_{j=1}^{\mu} W_N \alpha_j \mathcal{F} ,$$

où W_N est l'involution de Fricke (cf. figure III.1, où $\rho = e^{2i\pi/3}$). Ce domaine peut ne pas être connexe (sauf si N est premier), mais cela n'a pas d'importance pour la suite.

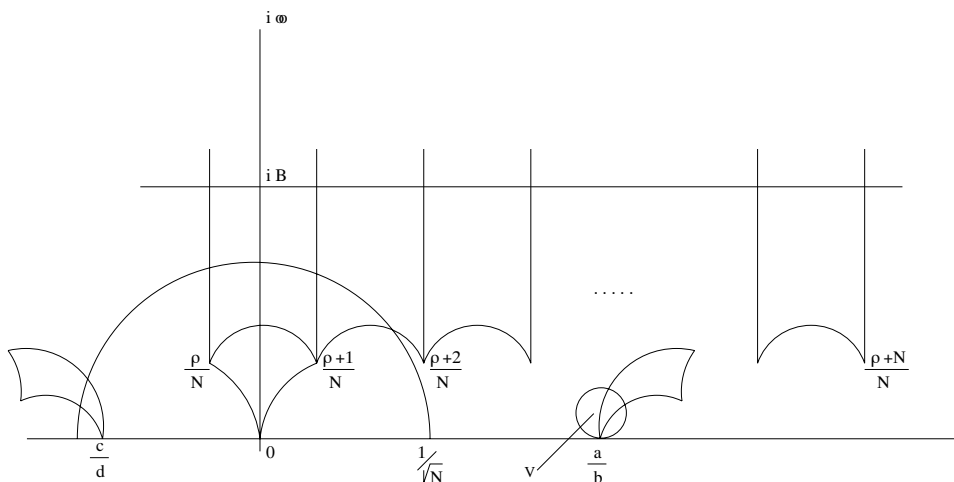


FIG. III.1 – Domaine fondamental pour $X_0(N)$

Nous recherchons tous les zéros de f dans \mathcal{F}_N . Dans un premier temps, nous voulons restreindre ce domaine.

Proposition III.1.1 *Il existe un nombre $B = B_f < 0.27$ tel que :*

$$\begin{cases} f(z) = 0 \\ \Im m(z) > B \end{cases} \implies z = i\infty .$$

Preuve : On considère la fonction :

$$\begin{aligned} g &: \mathbb{D} \longrightarrow \mathbb{D} \\ q &\longmapsto \sum_n a_n q^n . \end{aligned}$$

Sur le cercle $\{|q| = r\}$, on a :

$$\begin{aligned} |g(q) - q| &= \left| \sum_{n \geq 2} a_n q^n \right| = |q| \left| \sum_{n \geq 2} a_n q^{n-1} \right| \\ &\leq |q| \sum_{n \geq 2} |a_n| r^{n-1} . \end{aligned}$$

On pose $F(r) = \sum_{n \geq 2} |a_n| r^n$, on a $F(0) = 0$. Dès que r est assez petit, on a donc $F(r) < 1$, et, en appliquant le théorème de Rouché, on voit que le seul zéro de g dans le disque $\{|q| < r\}$ est $q = 0$. En revenant à f , on en déduit le théorème avec $B = -\log(r)/2\pi$. De plus, en majorant brutalement $|a_n|$ par $2n$, on obtient $B < 0.27$. \square

Cette majoration $B < 0.27$ est bien sûr très mauvaise et nous ne chercherons pas à l'améliorer. Dans les applications, on étudie directement la fonction F et on calcule une valeur convenable pour r . On en déduit alors une borne correcte pour B . La recherche des zéros de f au voisinage de l'infini est donc réglée. Pour les autres pointes, le problème est en général plus délicat. Cependant, certaines se traitent comme la pointe à l'infini.

Définition III.1.2 Une pointe $P = a/b \in X_0(N)$ est unitaire si $\text{pgcd}(b, N/b) = 1$.

Dans cette définition, on fait implicitement la supposition que le représentant a/b de la pointe P est tel que $\text{pgcd}(a, b) = 1$ et $b \mid N$.

La terminologie "unitaire" apparaît dans [Mazur-Swinnerton-Dyer]. Pour une pointe unitaire a/b , on peut toujours trouver un opérateur d'Atkin-Lehner W tel que $Wa/b = i\infty$ (cf. III.2.2 pour une description explicite de W). En appliquant cet opérateur W sur l'ouvert $\{\Im m(z) > B\}$, on obtient :

Corollaire III.1.3 Soit a/b une pointe unitaire, il existe un voisinage $V \subset X_0(N)$ de a/b tel que :

$$\begin{cases} f(z) = 0 \\ z \in V \end{cases} \implies z = \frac{a}{b} .$$

Il est clair que ce voisinage V est explicite dès que l'on connaît B et W .

Enfin, on remarque que :

$$f(z) = 0 \iff f(W_N z) = 0 .$$

On peut toujours choisir un élément $z' \in \{z, W_N z\}$ de sorte que $|z'| \geq 1/\sqrt{N}$. Toutes les considérations précédentes permettent de réduire considérablement le domaine de recherche des zéros de f (cf. figure III.1). On quadrille ensuite le domaine restant par des petits pavés rectangulaires R . Pour chacun d'entre eux, on évalue numériquement l'indice de zéro dans $f(R)$:

$$\text{Ind}_R = \frac{1}{2i\pi} \int_{\partial R} \frac{f'(z)}{f(z)} dz = \frac{1}{2i\pi} \int_{\partial f(R)} \frac{dz}{z} .$$

Le nombre Ind_R doit être un entier. S'il est nul R ne contient pas de zéro. Sinon, R en contient, on le partage en quatre pavés égaux et on recommence ... Lorsqu'un pavé contenant un zéro est suffisamment petit, on utilise la méthode de Newton en initialisant la récurrence en un point quelconque de ce pavé. On obtient alors les zéros de f avec la précision désirée. Il faut prêter une attention particulière aux éventuels zéros multiples qui peuvent poser quelques difficultés supplémentaires (de détection et de convergence pour la méthode de Newton).

Une fois tous les zéros de f évalués :

- On vérifie que tous les points trouvés sont bien inéquivalents modulo $\Gamma_0(N)$ (la méthode de Newton a pu créer un “saut” et trouver un zéro hors du domaine \mathcal{F}_N).
- On élimine tous ceux provenant des pôles de la forme dz .
- Il doit alors en rester $2g - 2$.

Cette méthode fonctionne assez bien dans la pratique. Par exemple, nous avons pu, en l'utilisant, déterminer numériquement tous les points critiques des revêtements modulaires des courbes de conducteurs $N \leq 100$.

Notons c_1, c_2, \dots, c_r les points critiques que l'on vient de trouver, on considère alors les points de ramification associés : $z_j = \varphi(c_j) = [x_j, y_j]$, pour $1 \leq j \leq r$. Comme les coordonnées de z_j sont algébriques, les polynômes :

$$P_1(X) = \prod_{j=1}^r (X - x_j) \quad \text{et}$$

$$P_2(X) = \prod_{j=1}^r (X - y_j)$$

sont à coefficients rationnels. Si on peut les calculer avec une précision suffisante, on reconnaît P_1 et P_2 en tant que polynômes de $\mathbb{Q}[X]$. On obtient ainsi numériquement le corps de définition des points de ramification. En outre, le fait que P_1 et P_2 aient des coefficients rationnels nous donne une vérification numérique des résultats obtenus.

Exemples

Dans tous les exemples que nous donnons ici, nous ne démontrons pas que les polynômes P_1 et P_2 obtenus numériquement sont exactement les polynômes définissant les points de ramification. La seule justification est que P_1 et P_2 sont très proches de polynômes à coefficients rationnels ayant des “petits” dénominateurs.

Prenons la courbe E d'équation :

$$E : y^2 + xy = x^3 - x^2 + 9x .$$

Le conducteur de cette courbe est $N = 63$. L'espace $X_0(N)$ a 8 pointes, mais ne possède pas de point elliptique. Son genre est $g = 5$. De plus, on a $\deg(\varphi) = 4$.

Nous devons donc trouver 8 points critiques. La méthode décrite ci-dessus permet de les obtenir :

$$\begin{aligned} c_1 &\approx 0.09909 + 0.01809 i ; \\ c_2 &\approx 0.15501 + 0.02831 i ; \\ c_3 &\approx 0.39953 + 0.06761 i ; \\ c_4 &\approx 0.47281 + 0.01829 i ; \\ \text{puis } c_5 &= -\overline{c_1}, \quad c_6 = -\overline{c_2}, \quad c_7 = -\overline{c_3}, \quad \text{et } c_8 = -\overline{c_4} . \end{aligned}$$

On pose $z_j = \varphi(c_j) = [x_j, y_j] \in E(K)$, et on reconnaît :

$$\begin{aligned} \prod_{j=1}^8 (X - x_j) &= (X^4 - 8X^3 + 46X^2 - 72X + 81)^2, \\ \prod_{j=1}^8 (X - y_j) &= (X^4 - 6X^3 + 111X^2 - 486X + 729)^2. \end{aligned}$$

On en déduit que les coordonnées des points de ramification de φ sont dans le corps K défini par :

$$P(X) = X^4 - 5X^2 + 7, \quad \text{disc}(P) = 2^4 \times 3^2 \times 7.$$

Les nombres $j(c_k)$ et $j(63c_k)$ sont aussi des nombres algébriques, mais leur corps de définition est bien plus difficile à reconnaître directement :

$$\begin{aligned} \prod_{k=1}^8 (X - j(c_k)) &= X^8 \\ &- 401371584648X^7 \\ &+ 177120450035027024549685X^6 \\ &- 3546960419673605771871720984X^5 \\ &+ 977351297352871386484091101055634X^4 \\ &+ \dots \end{aligned}$$

Un polynôme plus “simple” donnant le même corps est :

$$P(X) = X^8 - X^6 + 2X^2 + 1, \quad \text{disc}(P) = 2^8 \times 3^4 \times 7^2.$$

Dans cet exemple, les polynômes sont facilement reconnaissables car leurs coefficients sont (semble-t-il) entiers. Ce n'est pas toujours le cas, comme le montre l'exemple qui suit.

Prenons :

$$E : y^2 + xy = x^3 + x^2 + 4x + 5,$$

de conducteur $N = 89$. L'espace $X_0(N)$ possède 2 pointes, 2 points elliptiques d'ordre 2 (et aucun d'ordre 3), de plus $g = 7$ et $\deg(\varphi) = 5$. Les points elliptiques sont :

$$e_1 = \frac{-34 + i}{89} \quad \text{et} \quad e_2 = -\overline{e_1}.$$

Par notre méthode, nous obtenons 12 points de ramification, $(z_j = [x_j, y_j])_{1 \leq j \leq 12}$, pour φ . On a alors :

$$P_1 = \frac{1}{5^2 \times 71^4} (635292025X^{12} + 5312326784X^{11} + 37111326712X^{10} + \dots).$$

Ce polynôme a donc des coefficients assez compliqués et un grand dénominateur. Le corps donné par P_1 peut, en fait, être défini par le polynôme plus simple suivant :

$$P(X) = X^{12} - 4X^{11} + 41X^{10} - 150X^9 + 654X^8 - 1974X^7 + 5183X^6 - 11356X^5 + 22404X^4 - 30906X^3 + 43031X^2 - 34132X + 11623$$

Nous avons ainsi calculé tous les points critiques pour les revêtements modulaires des courbes elliptiques de conducteur ≤ 100 (et d'autres). Dans beaucoup d'exemples, on s'aperçoit que les points critiques sont des points de Heegner ! Dans la plupart des cas, nous pouvons donner une explication à ces phénomènes.

III.1.3 Factorisation par les opérateurs d'Atkin-Lehner

Soit W_Q ($Q \mid N$ et $\text{pgcd}(Q, N/Q) = 1$) un opérateur d'Atkin-Lehner. Puisque la forme f est une newform, c'est un vecteur propre pour W_Q et on a $f|_{W_Q} = \pm f$. En revenant à la fonction φ , on en déduit que :

$$\varphi \circ W_Q = \pm \varphi + P, \quad P \in E(\mathbb{Q})_{\text{tors}}. \quad (\text{III.3})$$

De plus, $2P = 0$ si le signe apparaissant dans la formule (III.3) est positif. Supposons que l'on ait simplement $\varphi \circ W_Q = \varphi$, alors on peut factoriser le revêtement modulaire par l'opérateur W_Q :

$$\varphi : X_0(N) \xrightarrow{\frac{\pi_Q}{2}} X_0(N)/W_Q \xrightarrow{\bar{\varphi}} E(\mathbb{C}).$$

La première flèche π_Q est l'application quotient, son degré vaut 2. On a donc $\deg(\bar{\varphi}) = \deg(\varphi)/2$. Les points fixes de W_Q dans $X_0(N)$ sont des points critiques de π_Q et donc de φ . Par la formule d'Hurwitz appliquée à π_Q , on a :

$$2g - 2 = 2(2g_Q - 2) + |\{\text{points fixes de } W_Q \text{ dans } X_0(N)\}|,$$

où g_Q est le genre de $X_0(N)/W_Q$. Pour obtenir ce nombre g_Q nous allons utiliser une formule de trace due à Skoruppa et à Zagier ([Skoruppa-Zagier]). Pour cela, nous utilisons leurs notations.

On définit une fonction $H_n(\Delta)$ pour $n \in \mathbb{N}$ et $\Delta \leq 0$.

Si $n = 1$, $H_1(\Delta) = H(|\Delta|)$ où H est la fonction nombre de classes d'Hurwitz (cf. [Cohen 1]).

Si $n \geq 2$, on écrit $\text{pgcd}(n, \Delta) = a^2b$ avec b sans facteur carré, et on pose :

$$H_n(\Delta) = \begin{cases} \left(\frac{\Delta/a^2b^2}{n/a^2b} \right) a^2b H_1\left(\frac{\Delta}{a^2b^2} \right) & \text{si } a^2b^2 \mid \Delta \\ 0 & \text{sinon.} \end{cases}$$

Pour $n \in \mathbb{N}$, on désigne par $Q(n)$ le plus grand entier dont le carré divise n , par $\sigma_0(n)$ le nombre diviseurs positifs de n et par μ la fonction de Moebius. En utilisant [Skoruppa-Zagier], on a :

Proposition III.1.4 On note $\text{Tr}(W_Q, S_2(N))$ la trace de l'opérateur W_Q dans $X_0(N)$. On a :

$$\text{Tr}(W_Q, S_2(N)) = \sum_{\substack{m \mid N \\ \mu\left(\frac{N}{m}\right) \neq 0}} \mu\left(\text{pgcd}\left(\frac{N}{m}, Q\right)\right) S(m, \text{pgcd}(m, Q)) \quad , \quad (\text{III.4})$$

où

$$\begin{aligned} S(m, n) = & -\frac{1}{2} \sum_{\substack{n' \mid n \\ n' > 4}} \left| \mu\left(\frac{n}{n'}\right) \right| H_{\frac{m}{n}}(-4n') \\ & -\frac{1}{2} \sum_{\substack{n' \mid n \\ 2 \leq n' \leq 4}} \left(\left| \mu\left(\frac{n}{n'}\right) \right| H_{\frac{m}{n}}(-4n') + 2H_{\frac{m}{n}}(n'^2 - 4n') \right) \\ & -\frac{1}{2} \left(|\mu(n)| H_{\frac{m}{n}}(-4) + 2H_{\frac{m}{n}}(-3) + 2|\mu(\text{pgcd}(4, n))| H_{\frac{m}{n}}(0) \right) \\ & -\frac{1}{2} \text{pgcd}(Q(n), 2) Q\left(\frac{m}{n}\right) \\ & + \begin{cases} \sigma_0(n) & \text{si } \frac{m}{n} \text{ est un carré} \\ 0 & \text{sinon} \end{cases} . \end{aligned}$$

Remarques : 1) Dans [Skoruppa-Zagier] (pp. 117), les auteurs ont, semble-t-il, oublié le facteur $\mu(\text{pgcd}(N/m), Q)$ dans la somme (III.4).

2) En prenant $Q = 1$, on retrouve $\text{Tr}(Id, S_2(N))$, le genre de $X_0(N)$.

On obtient, par la formule (III.4), la trace tr de l'opérateur W_Q sur l'espace $S_2(N)$. Soit \mathcal{B} une base de $S_2(N)$ formée par des vecteurs propres de W_Q . Alors, $tr = S_+ - S_-$ où S_+ (resp. S_-) désigne le nombre de formes $g \in \mathcal{B}$ telles que $g|_{W_Q} = g$ (resp. $g|_{W_Q} = -g$). Or, on a $g = S_+ + S_-$; on en déduit que $S_+ = (g + tr)/2$. De plus, S_+ est exactement le genre de $X_0(N)/W_Q$. Le nombre de points fixes de W_Q est donc :

$$|\{\text{points fixes de } W_Q \text{ dans } X_0(N)\}| = 2 - 2 \text{Tr}(W_Q, S_2(N)) \quad . \quad (\text{III.5})$$

On recherche maintenant tous les points fixes de W_Q dans $X_0(N)$. On pose :

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} \quad , \quad \det(W_Q) = Q \quad ,$$

et on veut $\tau \in \mathbb{H}$ tel que $W_Q \tau = M \tau$ pour $M \in \Gamma_0(N)$. Quitte à modifier les coefficients x, y, z et w de W_Q , on peut supposer que $M = Id$ et on a donc :

$$W_Q \tau = \tau \quad .$$

La matrice W_Q est ainsi une matrice elliptique, on peut voir que :

$$|x + w|\sqrt{Q} < 2 . \quad (\text{III.6})$$

Si $Q \neq 2, 3$ alors $x = -w$ et :

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & -Qx \end{pmatrix} \quad \det(W_Q) = Q .$$

Or $\det(W_Q) = -Q^2x^2 + yNz$ et donc $(2Qx)^2 = -4Q + 4Nyz$ et le point :

$$\tau = \frac{2xQ + \sqrt{-4Q}}{2Nz} , \quad (\text{III.7})$$

est un point fixe de W_Q (réciproquement, on vérifie facilement qu'un point fixe est de la forme (III.7)). Le point τ a précisément la forme d'un point de Heegner (en fait, c'est un point de Heegner dans un espace $X_0(N')$ pour un $N'|N$ convenable). Le procédé pour trouver tous les points fixes est le suivant :

– On cherche les solutions $\beta \pmod{2N}$ de l'équation :

$$\beta^2 \equiv -4Q \pmod{4N} \quad \text{avec } \beta \text{ de la forme } 2Qx . \quad (\text{III.8})$$

– Pour chaque β et chaque diviseur z de $(\beta^2 + 4Q)/4N$, on prend le point fixe :

$$\tau = \frac{\beta + \sqrt{-4Q}}{2Nz} . \quad (\text{III.9})$$

A chaque fois que l'on obtient un nouveau point τ , on vérifie qu'il n'est pas équivalent modulo $\Gamma_0(N)$ à un point déjà trouvé (sinon on le laisse). Lorsqu'on a épuisé tous les diviseurs z , on recommence éventuellement avec des solutions de (III.8) de la forme $\beta + 2N$ etc ... jusqu'à ce que tous les points fixes soient trouvés. On sait quand on doit s'arrêter puisque par la formule (III.5), on connaît le nombre de ces points. On va tous les obtenir de cette manière car ils sont de la forme (III.7).

Si $Q = 2$ ou 3 , on a $|x + w| = 0$ ou $|x + w| = 1$. On vient de traiter le premier cas. Pour le second, il faut légèrement modifier la méthode et tenir compte de $w = 1 - x$; essentiellement cela ne change rien. L'équation (III.8) est juste remplacée par :

$$\beta^2 - 2Q\beta \equiv 4Q \pmod{4N} \quad \text{avec } \beta \text{ de la forme } 2Qx .$$

Et les points fixes sont alors de la forme :

$$\tau = \frac{-\beta + Q + \sqrt{\Delta}}{2Nz} ,$$

où $\Delta = -4$ (resp. $\Delta = -3$) si $Q = 2$ (resp. $Q = 3$).

Dans la théorie des formes modulaires, certains opérateurs, différents des opérateurs de Hecke ou d'Atkin-Lehner, interviennent naturellement. Ils proviennent en principe de l'étude du normalisateur de $\Gamma_0(N)$ dans $SL_2(\mathbb{R})$ ([Atkin-Lehner]). On peut se servir d'eux pour obtenir des informations sur le revêtement modulaire. Si on trouve un tel opérateur \widetilde{W} , tel que $f|_{\widetilde{W}} = f$, alors, dans certains cas on peut factoriser φ :

$$\varphi : X_0(N) \longrightarrow X_0(N)/\widetilde{W} \xrightarrow{\bar{\varphi}} E(\mathbb{C}) .$$

Les points fixes de \widetilde{W} sont des points critiques et, comme précédemment, on montre que ce sont des points quadratiques dans $X_0(N)$. Cela se produit généralement lorsque $4 \mid N$; en effet, l'opérateur :

$$S_2 = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$$

agit alors par -1 sur les newforms de $S_2(N)$ (i.e. $f|_{S_2} = -f$). On peut alors utiliser S_2 pour trouver de nouveaux opérateurs à travers lesquels φ se factorise. Détaillons tout ceci à travers un exemple précis.

Nous prenons pour E la courbe d'équation :

$$E : y^2 = x^3 - 7x + 6 .$$

Le conducteur de E est $N = 80$. Le genre de $X_0(80)$ est $g = 7$ et on a $\deg(\varphi) = 4$. On doit trouver 12 points critiques pour φ .

Tout d'abord, on a :

$$\varphi \circ W_2 = \varphi ,$$

et la formule (III.5) nous apprend que le genre de $X_0(80)/W_2$ vaut 3 et que W_2 possède 4 points fixes. Par la méthode décrite ci-dessus, on obtient ces 4 points :

$$\begin{aligned} c_1 &= \frac{64 + \sqrt{-64}}{2 \times 80} & c_2 &= -\overline{c_1} , \\ c_3 &= \frac{256 + \sqrt{-64}}{2 \times 400} & c_4 &= -\overline{c_3} . \end{aligned}$$

Ensuite, on constate que l'opérateur $\widetilde{W} = (W_2 S_2)^2 W_2$ appartient au normalisateur de $\Gamma_0(N)$, que $f|_{\widetilde{W}} = f$ et que :

$$\varphi \circ \widetilde{W} = \varphi .$$

Remarque : On ne peut pas simplifier l'expression de \widetilde{W} . En effet, les opérateurs W_2 et S_2 ne commutent pas. Par contre, on peut voir que \widetilde{W} est une involution de $X_0(N)$.

On peut montrer que le genre de $X_0(80)/\widetilde{W}$ est aussi égal à 3. On a donc encore 4 points fixes à trouver pour \widetilde{W} . L'adaptation de la méthode ci-dessus permet de les déterminer :

$$\begin{aligned} c_5 &= \frac{16 + \sqrt{-64}}{2 \times 80} & c_6 &= \frac{-144 + \sqrt{-64}}{2 \times 400} , \\ c_7 &= -\overline{c_5} & c_8 &= -\overline{c_6} . \end{aligned}$$

De plus, $\deg(\varphi) = 4$ et on vient factoriser φ par deux applications de degré 2. Nous ne sommes donc pas loin d'avoir complètement décomposé φ . On considère le diagramme suivant :

$$\varphi : X_0(80) \xrightarrow[2]{\pi_2} X_0(80)/W_2 \xrightarrow[2]{\widetilde{\pi}_2} X_0(80)/(W_2, \widetilde{W}) \simeq E(\mathbb{C}) .$$

Les points critiques de π_2 sont donc c_1, c_2, c_3 et c_4 .

Dans l'espace $X_0(80)/W_2$ les points c_5 et c_6 sont équivalents de même que les points c_7 et c_8 . On note $\overline{c_5} = \pi_2(c_5) = \pi_2(c_6)$ et $\overline{c_7} = \pi_2(c_7) = \pi_2(c_8)$. Les points $\overline{c_5}$ et $\overline{c_7}$ vérifient :

$$\widetilde{W}\overline{c_5} = \overline{c_5} \quad \text{et} \quad \widetilde{W}\overline{c_7} = \overline{c_7} ,$$

(on considère ici l'action de \widetilde{W} dans $X_0(80)/W_2$) car les points c_5, c_6, c_7 et c_8 sont fixes par \widetilde{W} (dans $X_0(80)$). Ainsi, $\overline{c_5}$ et $\overline{c_7}$ sont des points critiques de $\widetilde{\pi}_2$.

Le genre de $X_0(80)/(W_2, \widetilde{W})$ est 1, l'application $\widetilde{\pi}_2$ possède donc 4 points critiques. On va voir que les 2 points critiques manquants sont des pointes de $X_0(N)/W_2$. Pour cela, on pose :

$$P_1 = \frac{1}{4} , \quad P_2 = \frac{3}{4} , \quad P_3 = \frac{1}{20} , \quad P_4 = \frac{3}{20} .$$

Ce sont des pointes différentes de $X_0(N)$.

On a $\pi_2(P_1) = \{P_1, P_2\} = \overline{P_1}$ et $\pi_2(P_3) = \{P_3, P_4\} = \overline{P_3}$. De plus, l'action de \widetilde{W} sur ces pointes est donnée par : $\widetilde{W}P_1 = P_2$ et $\widetilde{W}P_3 = P_4$. On en déduit que :

$$\widetilde{W}\overline{P_1} = \overline{P_1} \quad \text{et} \quad \widetilde{W}\overline{P_3} = \overline{P_3} .$$

Les pointes $\overline{P_1}$ et $\overline{P_3}$ sont donc bien des points critiques de $\widetilde{\pi}_2$.

Bilan, on a obtenu les 12 points critiques du revêtement modulaire :

- c_1, c_2, c_3, c_4 sont des points critiques provenant de l'action de W_2 sur $X_0(N)$.
- c_5, c_6, c_7, c_8 sont des points critiques provenant de l'action de \widetilde{W}_2 sur $X_0(N)$.
- P_1, P_2, P_3, P_4 sont des points critiques provenant de l'action de \widetilde{W} sur l'espace $X_0(80)/W_2$.

L'étude détaillée de ce revêtement modulaire est ici possible car φ peut se factoriser totalement et de façon tout à fait explicite.

Définition III.1.5 Soit E une courbe elliptique définie sur \mathbb{Q} de conducteur N et φ son revêtement modulaire. On dit que E est une courbe involutive s'il existe des opérateurs U_1, U_2, \dots, U_k appartenant au normalisateur de $\Gamma_0(N)$ dans $SL_2(\mathbb{R})$ tels que φ se factorise complètement :

$$\varphi : X_0(N) \longrightarrow X_1 \longrightarrow X_2 \cdots \longrightarrow X_k \simeq E(\mathbb{C}) ,$$

où $X_j = X_{j-1}/U_j$ et U_j est une involution de X_{j-1} .

C'est une définition plus générale que celle donnée dans [Mazur-Swinnerton-Dyer], où seules les factorisations à travers les opérateurs d'Atkin-Lehner sont envisagées. On vient donc d'établir :

Proposition III.1.6 *La courbe E d'équation $E : y^2 = x^3 - 7x + 6$ est involutive. Le revêtement modulaire associé possède 12 points critiques, 8 sont des points de Heegner et 4 sont des pointes de $X_0(80)$.*

L'exemple que nous venons de traiter nous apprend plusieurs choses :

- D'abord, l'utilisation d'autres opérateurs que ceux d'Atkin-Lehner est indispensable pour l'étude du revêtement modulaire φ .
- Ensuite, dans notre cas, on peut déterminer théoriquement tous les points critiques de φ . Comme ce sont des points de Heegner et des pointes, on peut en déduire précisément les corps de nombres dans lesquels les points de ramification associés sont définis.
- Enfin, quatre de ces points sont des pointes, et il faut donc faire attention à cette éventualité dans l'utilisation de la méthode numérique que nous avons décrite plus haut.

Dans les calculs que nous avons effectués, plusieurs exemples peuvent se traiter de façon plus ou moins analogue. En tout cas, cela permet d'expliquer dans beaucoup de cas pourquoi certains points critiques sont des points quadratiques.

Cependant, dans le cas de la courbe E d'équation :

$$E : y^2 + xy = x^3 + x^2 - 11x ,$$

de conducteur $N = 33$, les points critiques de φ semblent être les points de Heegner suivants :

$$\begin{aligned} c_1 &= \frac{36 + \sqrt{-24}}{2 \times 33} & c_2 &= -\overline{c_1} , \\ c_3 &= \frac{36 + \sqrt{-24}}{4 \times 33} & c_4 &= -\overline{c_3} . \end{aligned}$$

Pourtant, $\deg(\varphi) = 3$ et aucune factorisation naturelle n'est possible.

La table III.1, donne la liste des courbes involutives non triviales (i.e. E non isomorphes à $X_0(N)$) de conducteur $N \leq 100$. La colonne $(U_j)_j$ fournit la liste (dans l'ordre) des opérateurs qui donnent une factorisation complète de φ .

Revenons brièvement sur l'étude des groupes $E(\mathbb{Q})^{\text{crit}}$ et $E(\mathbb{Q})^{\text{fond}}$. Dans le cas des courbes de rang nul, ces deux groupes sont, bien sûr, des groupes de torsion. Nous avons calculé (numériquement) les points critiques associés aux deux premières courbes de rang 2 ($N = 389$ et $N = 433$). Il semble que $E(\mathbb{Q})^{\text{fond}}$ soit aussi un groupe de torsion pour ces deux courbes. La situation est plus intéressante pour les courbes de rang 1. Dans ce

N	$[a_1, a_2, a_3, a_4, a_6]$	$(U_j)_j$	N	$[a_1, a_2, a_3, a_4, a_6]$	$(U_j)_j$
26	$[1, 0, 1, -5, -8]$	W_2	58	$[1, -1, 0, -1, 1]$	W_2, W_{29}
26	$[1, -1, 1, -3, 3]$	W_{13}	61	$[1, 0, 0, -2, 1]$	$W_6 1$
30	$[1, 0, 1, 1, 2]$	W_5	62	$[1, -1, 1, -1, 1]$	W_{31}
34	$[1, 0, 0, -3, 1]$	W_{17}	64	$[0, 0, 0, -4, 0]$	$(W_2 S_2)^2$
35	$[0, 1, 1, 9, 1]$	W_5	65	$[1, 0, 0, -1, 0]$	W_{65}
37	$[0, 0, 1, -1, 0]$	W_{37}	66	$[1, 0, 1, -6, 4]$	W_2, W_{11}
38	$[1, 1, 1, 0, 1]$	W_{19}	66	$[1, 1, 1, -2, -1]$	W_3, W_{11}
39	$[1, 1, 0, -4, -5]$	W_3	69	$[1, 0, 1, -1, -1]$	W_{23}
40	$[0, 0, 0, -7, -6]$	$(W_2 S_2)^2$	70	$[1, -1, 1, 2, -3]$	W_5, W_{14}
42	$[1, 1, 1, -4, 5]$	W_7	72	$[0, 0, 0, 6, -7]$	$W_2, (W_2 S_2)^2$
43	$[0, 1, 1, 0, 0]$	W_{43}	77	$[0, 0, 1, 2, 0]$	W_7, W_{11}
44	$[0, 1, 0, 3, -1]$	W_{11}	79	$[1, 1, 1, -2, 0]$	W_{79}
45	$[1, -1, 0, 0, -5]$	W_5	80	$[0, 0, 0, -7, 6]$	$W_2, (W_2 S_2)^2 W_2$
48	$[0, 1, 0, -4, -4]$	$(W_2 S_2)^2$	80	$[0, -1, 0, 4, -4]$	$(S_2 W_2)^2, (S_2 W_2)$
50	$[1, 0, 1, -1, -2]$	W_2	82	$[1, 0, 1, -2, 0]$	W_2, W_{41}
50	$[1, 1, 1, -3, 1]$	W_5	83	$[1, 1, 1, 1, 0]$	W_{83}
51	$[0, 1, 1, 1, -1]$	W_{17}	88	$[0, 0, 0, -4, 4]$	$W_2, W_{11}, (W_2 S_2)^2$
53	$[1, -1, 1, 0, 0]$	W_{53}	89	$[1, 1, 1, -1, 0]$	W_{89}
54	$[1, -1, 1, 1, -1]$	W_3	91	$[0, 0, 1, 1, 0]$	W_7, W_{13}
55	$[1, -1, 0, -4, 3]$	W_{11}	92	$[0, 1, 0, 2, 1]$	W_{23}
56	$[0, 0, 0, 1, 2]$	W_7	94	$[1, -1, 1, 0, -1]$	W_{47}
56	$[0, -1, 0, 0, -4]$	$S_2 W_7, (S_2 W_2)^2$	96	$[0, 1, 0, -2, 0]$	$W_2, (S_2 W_2)^2$
57	$[0, -1, 1, -2, 2]$	W_3, W_{19}	99	$[1, -1, 1, -2, 0]$	W_3, W_{11}

TAB. III.1 – Courbes involutives de conducteur $N \leq 100$, et $\deg(\varphi) \neq 1$

cas, le point i/\sqrt{N} est un point critique fondamental naturel. Pour les premières courbes, les groupes $E(\mathbb{Q})^{\text{crit}}$ et $E(\mathbb{Q})^{\text{fond}}$ sont souvent des sous-groupes d'indices finis dans $E(\mathbb{Q})$, mais pas toujours. Le premier exemple où $E(\mathbb{Q})^{\text{fond}}$ est un groupe de torsion est donné par la courbe de conducteur $N = 91 = 7 \times 13$ d'équation $y^2 + y = x^3 + x^2 - 7x + 5$. Ici, on a $a_7 = a_{13} = 1$ et la condition 2 sur les discriminants n'est pas satisfaite (cf. chapitre I). Le point $i/\sqrt{91}$ donne donc un point de torsion sur $E(\mathbb{Q})$. Par contre, pour cette courbe, $E(\mathbb{Q})^{\text{crit}}$ est un groupe d'indice fini dans $E(\mathbb{Q})$. Il est à noter que les 4 points elliptiques d'ordre 3 de $X_0(91)$ s'envoient, par φ , sur des points rationnels d'ordre infini. La première courbe de rang 1 pour laquelle on a $E(\mathbb{Q})^{\text{crit}} \subseteq E(\mathbb{Q})_{\text{tors}}$ est celle d'équation $y^2 = x^3 - x + 1$ de conducteur $N = 92$.

III.1.4 Cas d'une courbe de rang 2

Dans cette section, nous commentons les résultats que nous avons obtenus concernant la première courbe elliptique (au sens du conducteur) de rang 2. Il s'agit de la courbe d'équation :

$$E : y^2 + y = x^3 + x^2 - 2x ,$$

de conducteur $N = 389$. Le groupe de Mordeil-Weil $E(\mathbb{Q})$ est sans torsion et engendré par :

$$G_1 = [0, 0] \quad \text{et} \quad G_2 = [1, 0] .$$

Le genre de $X_0(389)$ vaut $g = 32$ et il n'y a ni point elliptique d'ordre 2 ni d'ordre 3. Enfin, on a $\deg(\varphi) = 40$. Nous avons pu déterminer, par la méthode décrite précédemment, les 62 points critiques du revêtement modulaire (les résultats complets figurent dans l'annexe B). Nous avons constaté quelques phénomènes intéressants :

- Conformément au théorème VI, on trouve deux points critiques fondamentaux :

$$\begin{aligned} c_3 &\approx 0.0169298394643814501869216816 \times i \\ c_4 &\approx 0.1518439730519631382000247052 \times i . \end{aligned}$$

- Plus étonnant, les calculs semblent indiquer que les deux points de Heegner :

$$\begin{aligned} c_1 &= \frac{337 + \sqrt{-19}}{2 \times 389} \\ c_2 &= \frac{-337 + \sqrt{-19}}{2 \times 389} , \end{aligned}$$

sont des points critiques ! Nous ne savons ni démontrer ce résultat, ni expliquer la particularité du discriminant -19 par rapport à la courbe.

- Enfin, deux des points critiques possède une partie réelle égale à $1/2$:

$$\begin{aligned} c_5 &\approx \frac{1}{2} + 0.008015879627931564443796916 \times i \\ c_6 &\approx \frac{1}{2} + 0.080175046492899577113086416 \times i . \end{aligned}$$

Cette situation apparaît aussi pour les courbes de rang 2. La droite $\Re(s) = 1/2$ possède des propriétés similaires à celles de la droite $\Re(s) = 0$.

Le dernier point peut s'expliquer en étudiant la fonction $f(\tau + \frac{1}{2})$ et sa "série L" : $L_2(f, s) = -\sum_n (-1)^n a(n) n^{-s}$ où on a posé $L(f, s) = \sum_n a(n) n^{-s}$. Le fait est qu'ici, on a $L_2(f, s) = (1 - \frac{a(2)}{2^{s-1}} + \frac{1}{2^{2s-2}}) L(f, s)$.

Soit $P \in E(\mathbb{C})$. En utilisant les points de ramification de φ , on peut donner une méthode générale qui calcule tous les antécédents de P par rapport au revêtement modulaire.

Si $G \in E(\mathbb{Q})$ et si x_1, x_2, \dots, x_{40} sont les 40 points au-dessus de G alors $j(x_k) \in \overline{\mathbb{Q}}$. De plus, si la précision est suffisamment grande, on peut calculer et reconnaître le polynôme :

$$P_G(X) = \prod_{j=1}^{40} (X - j(x_k)) \in \mathbb{Q}[X] .$$

Nous avons déterminé numériquement P_{G_1} , P_{G_2} , $P_{G_1+G_2}$, $P_{G_1-G_2}$, P_{2G_1} , P_{2G_2} . Tous ces polynômes sont irréductibles de degré 40 et à coefficients entiers. Notons que deux des antécédents du point $2G_1$ ont une partie réelle égale à $1/2$.

III.2 Développement de Fourier aux pointes

III.2.1 Motivations et notations

Comme nous l'avons déjà vu dans la partie précédente, il peut arriver qu'une pointe $P \in X_0(N)$ soit aussi un point critique du revêtement modulaire. Cela signifie que l'ordre d'annulation de f en P est ≥ 2 , et nous voulons le lire sur le développement de Fourier de f en la pointe. On explique ici comment l'on peut, dans certains cas, obtenir de tels développements. Les techniques utilisées étant assez générales, nous allons considérer le cadre plus large des formes modulaires de poids k sur $\Gamma_0(N)$ et caractère ε . Cependant, la définition du développement de Fourier en une pointe P est un peu plus délicate lorsque k est impair. C'est pour cette raison, et pour ne pas alourdir davantage nos propos, que nous allons nous restreindre aux poids pairs. On suppose donc dans toute la suite que k est pair.

On note $S_k(N, \varepsilon)$ l'espace vectoriel des formes modulaires paraboliques de poids k sur $\Gamma_0(N)$ et de caractère ε ; si $f \in S_k(N, \varepsilon)$:

$$f|_M = \varepsilon(d)f \quad \text{pour tout } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) .$$

On trouvera, par exemple dans [Li 1], [Atkin-Li] les résultats et outils que nous utiliserons sur ces formes. En particulier, il existe aussi une notion de newforms (cf. [Li 1]) et des opérateurs W_Q d'Atkin-Lehner ou plutôt d'Atkin-Li (cf. [Atkin-Li]). Pour ces opérateurs, une restriction supplémentaire sur les coefficients est demandée. Si on écrit $N = QM$ avec $\text{pgcd}(Q, M) = 1$ alors on décompose le caractère $\varepsilon \pmod{N}$ en $\varepsilon = \varepsilon_Q \varepsilon_M$, où ε_Q (resp. ε_M) est un caractère sur $(\mathbb{Z}/Q\mathbb{Z})^*$ (resp. sur $(\mathbb{Z}/M\mathbb{Z})^*$). L'opérateur W_Q est défini par :

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} , \quad \det(W_Q) = Q ,$$

où $y \equiv 1 \pmod{Q}$ et $x \equiv 1 \pmod{N/Q}$. De façon générale, si :

$$W'_Q = \begin{pmatrix} Qx' & y' \\ Nz' & Qw' \end{pmatrix} , \quad \det(W'_Q) = Q ,$$

est un opérateur sans ces conditions sur les coefficients et si $f \in S_k(N, \varepsilon)$ alors

$$f|_{W_Q} = \overline{\varepsilon_Q}(y') \overline{\varepsilon_M}(x') f|_{W_Q} .$$

On note $\mathcal{N}_k(N, \varepsilon)$ l'ensemble des newforms normalisées de $S_k(N, \varepsilon)$. Si $f \in \mathcal{N}_k(N, \varepsilon)$ alors $f|_{W_Q} = \lambda_Q(f)h$, où $h \in \mathcal{N}_k(N, \overline{\varepsilon_Q}\varepsilon_M)$ et $\lambda_Q(f)$ est une *pseudo-valeur propre* de W_Q . Le développement de Fourier de h à l'infini s'exprime facilement à l'aide de celui de f (cf. [Atkin-Li]). En effet, si $f(\tau) = \sum_{n \geq 1} a(n)q^n$ alors $h(\tau) = \sum_{n \geq 1} b(n)q^n$ où, pour tout p premier :

$$b(p) = \begin{cases} \overline{\varepsilon_Q}(p)a(p) & \text{si } p \nmid Q \\ \varepsilon_M(p)\overline{a(p)} & \text{sinon} \end{cases} . \quad (\text{III.10})$$

On obtient les autres coefficients de h à l'aide des propriétés de multiplicativité des $b(n)$. La pseudo-valeur propre $\lambda_Q(f)$ est, en fait, un nombre algébrique de norme absolue 1 ([Atkin-Li]).

Soit P une pointe de $X_0(N)$, et $M \in SL_2(\mathbb{Z})$ telle que $M\infty = P$, alors $f|_M$ est périodique de période ℓ (la largeur de la pointe P). Ainsi, on peut écrire :

$$f|_M = \sum_{n \geq 1} c(n)q^{n/\ell} ,$$

qui est le développement de Fourier de f en P . Soit $M' \in SL_2(\mathbb{Z})$ telle que $M'\infty = P$ et $\sum_n c'(n)q^{n/\ell}$ le développement de Fourier associé. Alors, il existe ζ une racine ℓ -ième de l'unité telle que $c'(n) = \zeta^n c(n)$ pour tout $n \geq 1$. Les coefficients du développement de Fourier de f ne dépendent donc pas de la matrice M choisie (à une racine ℓ -ième de l'unité près). En particulier, l'ordre d'annulation de f en P (i.e. le plus petit $n > 0$ tel $c(n) \neq 0$) est bien défini. Il est noté $\nu(f, P)$.

Remarques : 1) Le développement de Fourier de f en P commence en $n \geq 1$ car f est une forme modulaire *parabolique* (les formes paraboliques s'annulent aux pointes).
2) On peut aussi choisir des matrices $M \in SL_2(\mathbb{R})$ telles que $M\infty = P$. Dans ce cas, bien que la largeur de la pointe (i.e. le nombre ℓ) puisse être modifiée, l'ordre d'annulation de f en P , lui, reste inchangé.
3) Lorsque f est une forme modulaire associée à une courbe elliptique définie sur \mathbb{Q} , alors P est un point critique du revêtement modulaire si et seulement si $\nu(f, P) \geq 2$.

Soit χ un caractère modulo M . La tordue de f par χ est donnée par :

$$f_\chi = \sum_{n \geq 1} a(n)\chi(n)q^n ,$$

où $f(\tau) = \sum_n a(n)q^n$. On pose $S_M = \begin{pmatrix} 1 & 1/M \\ 0 & 1 \end{pmatrix}$ et on désigne par $R_\chi(M)$ l'opérateur :

$$f|_{R_\chi(M)} = \sum_{u \bmod M} \overline{\chi}(u) f|_{S_M^u} ,$$

et $R_\chi = R_\chi(\text{cond}(\chi))$ où $\text{cond}(\chi)$ est le conducteur de χ . On a $g(\overline{\chi})f_\chi = f|_{R_\chi}$ (ici $g(\overline{\chi})$ désigne la somme de Gauss de $\overline{\chi}$). Voici quelques propriétés simples de $R_\chi(M)$ (cf. [Li 2], par exemple). La lettre p désigne ici un nombre premier.

- Soit χ un caractère non trivial de conducteur $p^a > 1$ alors pour $b \geq a$ on a :

$$f|_{R_\chi(p^b)} = p^{b-a} g(\overline{\chi})(f|_{U_{p^{b-a}}})_\chi|_{B_{p^{b-a}}} \quad . \quad (\text{III.11})$$

- Soit χ_0 le caractère trivial alors :

$$f|_{R_{\chi_0}(p^b)} = p^b f|_{U_{p^b}}|_{B_{p^b}} - p^{b-1} f|_{U_{p^{b-1}}}|_{B_{p^{b-1}}} \quad . \quad (\text{III.12})$$

- Si ϕ désigne la fonction d'Euler alors pour $\text{pgcd}(a, M) = 1$:

$$\phi(M)f|_{S_M^a} = \sum_{\text{cond}(\chi)|M} \chi(a)f|_{R_\chi(M)} \quad . \quad (\text{III.13})$$

Dans ces formules, les opérateurs U_r et B_r pour $r \in \mathbb{N}$ sont définis par :

$$f|_{U_r}(\tau) = \sum_n a(nr)q^n \quad \text{et} \quad f|_{B_r} = \sum_n a(n)q^{nr} \quad .$$

Supposons que le conducteur $M = \text{cond}(\chi)$ soit premier avec N , et soit $f \in \mathcal{N}_k(N, \varepsilon)$, alors $f_\chi \in \mathcal{N}_k(NM^2, \varepsilon\chi^2)$, le diagramme suivant résume le résultat de l'action de l'opérateur W_Q sur l'action de “tordre” et réciproquement.

$$\begin{array}{ccc} f \in \mathcal{N}_k(N, \varepsilon) & \xrightarrow{\chi} & f_\chi \in \mathcal{N}_k(NM^2, \varepsilon\chi^2) \\ \downarrow w_Q & & \downarrow w_Q \\ h \in \mathcal{N}_k(N, \overline{\varepsilon_Q}\varepsilon_{N/Q}) & \xrightarrow{\chi} & h_\chi \in \mathcal{N}_k(NM^2, \overline{\varepsilon_Q}\varepsilon_{N/Q}\chi^2) \\ \lambda_Q(f) & & \lambda_Q(f_\chi) = \overline{\chi}(Q)\lambda_Q(f) \end{array} \quad (\text{III.14})$$

III.2.2 Pointes unitaires

Soit $f \in \mathcal{N}_k(N, \varepsilon)$ une forme dont on cherche le développement en une pointe $P = a/b$ unitaire i.e. $N = bQ$ avec $\text{pgcd}(b, Q) = 1$, la largeur de la pointe P est alors égale à $\ell = Q$. On prend $h \in \mathcal{N}_k(N, \overline{\varepsilon_Q}\varepsilon_M)$ la newform vérifiant :

$$f|_{W_Q} = \lambda_Q(f)h \quad .$$

Les coefficients $h(\tau) = \sum_n b(n)q^n$ sont explicites en fonction de ceux de f . De plus, $h|_{W_Q} = \lambda_Q(h)f$ où :

$$\lambda_Q(h) = \varepsilon_Q(-1)\overline{\varepsilon_b}(Q)\lambda_Q(f) \quad . \quad (\text{III.15})$$

On désigne par $c(n)$ les coefficients de Fourier de f en la pointe P . Ces nombres sont bien définis à une racine ℓ -ième de l'unité près.

Théorème VII On a :

$$\sum_{n \geq 1} c(n) q^{n/\ell} = \frac{\overline{\varepsilon}_b(-a) \varepsilon_Q(b) \lambda_Q(f)}{\ell^{k/2}} \sum_{n \geq 1} b(n) \zeta^n q^{n/\ell} , \quad (\text{III.16})$$

où ζ est une racine ℓ -ième de l'unité.

Preuve : On choisit un opérateur :

$$W'_Q = \begin{pmatrix} Qx & y \\ Nb & Qw \end{pmatrix} ,$$

avec $w = 1 - ab$ et $Qxw - yb^2 = 1$ (la deuxième condition est une relation de Bezout entre b^2 et Qw et ils sont premiers entre eux). On a :

$$\det(W'_Q) = Q^2 xw - b^2 Qy = Q .$$

De plus,

$$y \equiv -b^{-2} \pmod{Q} \quad \text{et} \quad x \equiv Q^{-1} \pmod{b} .$$

On fixe :

$$P = \begin{pmatrix} X & Y \\ N & -a' \end{pmatrix} \in \Gamma_0(N) \quad \text{où} \quad a' = aQx + by .$$

Enfin, on pose $W''_Q = PW'_Q$; on a $W''_Q \frac{a}{b} = \infty$. Soit :

$$M = \begin{pmatrix} a & u \\ b & v \end{pmatrix} \in SL_2(\mathbb{Z}) ,$$

alors, d'une part :

$$\begin{aligned} h|_{W''_Q M} &= h|_P|_{W'_Q}|_M = \varepsilon_b(-aQx) \overline{\varepsilon}_Q(-by) h|_{W'_Q}|_M \\ &= \varepsilon_b(-a) \varepsilon_Q(b) h|_{W'_Q}|_M \\ &= \varepsilon_b(-a) \varepsilon_Q(b) \overline{\varepsilon}_Q(-b^2) \varepsilon_b(-Q) \lambda_Q(h) f|_M \\ &= \varepsilon_b(-aQ) \overline{\varepsilon}_Q(b) \lambda_Q(h) \sum_{n \geq 1} c(n) q^{n/\ell} , \end{aligned}$$

et d'autre part :

$$\begin{aligned} h|_{W''_Q M} &= h|_N \quad \text{avec} \quad N = \begin{pmatrix} 1 & t \\ 0 & \ell \end{pmatrix} \quad \text{et} \quad t \in \mathbb{Z} \\ &= \ell^{k/2} \ell^{-k} h \left(\frac{\tau + t}{\ell} \right) \\ &= \frac{1}{\ell^{k/2}} \sum_{n \geq 1} b(n) \zeta^n q^{n/\ell} , \quad \zeta = e^{2i\pi t/\ell} . \end{aligned}$$

On conclut en utilisant la formule (III.15). □

Corollaire III.2.1 Soit $f = \sum_n a(n)q^n \in \mathcal{N}_2(N)$. Le développement de f en une pointe unitaire $P = a/b \in X_0(N)$ est donné par :

$$\sum_{n \geq 1} c(n)q^{n/\ell} = \frac{\pm 1}{\ell} \sum_{n \geq 1} a(n)\zeta^n q^{n/\ell} ,$$

où ζ est une racine ℓ -ième de l'unité.

Dans ce corollaire, le signe ± 1 est donné par la valeur propre de W_Q en f ($f|_{W_Q} = \pm f$).

Corollaire III.2.2 Soit E une courbe elliptique définie sur \mathbb{Q} de conducteur N et φ le revêtement modulaire associé. Les pointes unitaires de $X_0(N)$ ne sont pas des points critiques de φ . En particulier si N est sans facteur carré, aucune pointe n'est un point critique.

Soit χ un caractère de conducteur M premier avec N , alors $f_\chi \in \mathcal{N}_k(NM^2, \varepsilon\chi^2)$ et $P_M = a/bM^2$ est une pointe unitaire de $X_0(NM^2)$ de largeur $\ell = Q = N/b = NM^2/bM^2$. Si $\sum_n c(n)q^{n/\ell}$ désigne le développement de f en P alors :

Théorème VIII Le développement de Fourier de f_χ en la pointe P_M est de la forme :

$$\varepsilon_Q(M^2)\bar{\chi}(a^2Q) \sum_{n \geq 1} c(n)\chi(n)q^{n/\ell} .$$

Preuve : On part de l'égalité matricielle suivante :

$$\underbrace{S_M^u T \begin{pmatrix} a & X \\ bM^2 & Y \end{pmatrix}}_{A_1} \underbrace{\begin{pmatrix} Q & 0 \\ 0 & 1 \end{pmatrix}}_{A_3} = V \underbrace{\begin{pmatrix} a & r \\ b & s \end{pmatrix}}_{A_2} \begin{pmatrix} Q & 0 \\ 0 & 1 \end{pmatrix} S_M^v .$$

avec :

$$\begin{aligned} T &= \begin{pmatrix} * & * \\ * & 1 + avNM \end{pmatrix} \in \Gamma_0(NM^2) , \\ V &= \begin{pmatrix} as - xb & * \\ b(M^2s - y) & -bM^2r + ya \end{pmatrix} , \\ v &\equiv uy(Qa)^{-1} \pmod{M} , \end{aligned}$$

et où on a choisi X, Y, r, s convenablement pour que $V \in \Gamma_0(N)$ et $\det(A_1) = \det(A_2) = 1$. Ainsi, $as - xb \equiv M^{-2} \pmod{Q}$. On a alors :

$$\begin{aligned} \sum_{u \bmod M} \bar{\chi}(u) f|_{S_M^u}|_T|_{A_1}|_{A_3} &= g(\bar{\chi}) f|_{\chi}|_T|_{A_1}|_{A_3} \\ &= g(\bar{\chi}) \sum_{n \geq 1} d(n)q^n , \end{aligned}$$

où $\sum_n d(n)q^{n/\ell}$ est le développement de Fourier de f_χ en a/bM^2 . En utilisant l'égalité matricielle, on obtient :

$$\begin{aligned}
\sum_{u \bmod M} \bar{\chi}(u) f|_{S_M^u}|_T|_{A_1}|_{A_3} &= \sum_{u \bmod M} \bar{\chi}(u) f|_V|_{A_2}|_{A_3}|_{S_M^v} \\
&= \overline{\varepsilon_Q}(as - Xb) \sum_{u \bmod M} \bar{\chi}(u) f|_{A_2}|_{A_3}|_{S_M^v} \\
&= \varepsilon_Q(M^2) \sum_{v \bmod M} \bar{\chi}(v) \bar{\chi}(a^2 Q) f|_{A_2}|_{A_3}|_{S_M^v} \\
&= \varepsilon_Q(M^2) \bar{\chi}(a^2 Q) \sum_{v \bmod M} \bar{\chi}(v) \left(\sum_{n \geq 1} c(n) q^n \right) |_{S_M^v} \\
&= \varepsilon_Q(M^2) \bar{\chi}(a^2 Q) g(\bar{\chi}) \sum_{n \geq 1} c(n) \chi(n) q^n .
\end{aligned}$$

Et le théorème est montré. \square

Remarques : 1) L'utilisation du théorème VII et des relations (III.14) auraient aussi permis de démontrer le théorème VIII.

2) On voit ainsi que “tordre” en la pointe à l'infini est essentiellement équivalent à “tordre” en une pointe unitaire.

III.2.3 Pointes non unitaires

Soit $P = a/b \in X_0(N)$ une pointe non unitaire en laquelle nous voulons obtenir le développement de Fourier de $f \in \mathcal{N}_k(N, \varepsilon)$. Tout d'abord, nous pouvons toujours nous ramener à $b^2 \mid N$. En effet, décomposons b en produit de facteurs premiers et écrivons :

$$b = \prod_{j \in J} p_j^{\alpha_j} \quad \text{et} \quad I = \{j \in J \mid p_j^{2\alpha_j} \nmid N\} .$$

Posons $N = N' \prod_{j \in J} p_j^{\beta_j}$ avec $\text{pgcd}(N', b) = 1$ et $Q = \prod_{j \in J} p_j^{\beta_j}$. En choisissant convenablement les coefficients x, y, z , et w , on peut fixer un opérateur W_Q :

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} , \quad \det(W_Q) = Q$$

tel que $W_Q a/b = a'/b'$ avec :

$$b' = \prod_{j \in I} p_j^{\beta_j - \alpha_j} \prod_{j \notin I} p_j^{\alpha_j} .$$

On a ainsi $b'^2 \mid N$. Soit $h \in \mathcal{N}_k(N, \overline{\varepsilon_Q} \varepsilon_{N/Q})$ telle que $f|_{W_Q} = \lambda_Q(f)h$ et soit $M' \in SL_2(\mathbb{Z})$ telle que $M' \infty = a'/b'$. Le développement de Fourier de f en a/b se déduit de celui de h

en a'/b' :

$$\begin{aligned} f|_{W_Q}|_{M'} &= \varepsilon_Q y \overline{\varepsilon_{N/Q}}(x) \lambda_Q(f) h|_{M'} \\ &= \varepsilon_Q y \overline{\varepsilon_{N/Q}}(x) \underbrace{\sum_{n \geq 1} c(n) q^{n/\ell}}_{\text{dev. de } h \text{ en } a'/b'} . \end{aligned}$$

Et :

$$f|_{W_Q}|_{M'} = f|_M = \underbrace{\sum_{n \geq 1} d(n) q^{n/\ell}}_{\text{dev. de } f \text{ en } a/b} .$$

Notons qu'ici M n'appartient pas à $SL_2(\mathbb{Z})$ mais au sous-groupe G de $SL_2(\mathbb{R})$ engendré par $SL_2(\mathbb{Z})$ et $Q^{-1/2}W_Q$. Le nombre ℓ est la largeur de la pointe a/b , non pas par rapport à $SL_2(\mathbb{Z})$, mais par rapport à G . Cependant, l'ordre d'annulation de f en a/b reste inchangé et correspond donc au plus petit entier $n \geq 1$ tel que $c(n) \neq 1$.

On écrit $f(\tau) = \sum_{n \geq 1} a(n) q^n$ le développement de f en l'infini.

Soit donc $P = a/b$ une pointe unitaire avec $b^2 | N$; on a alors $\ell = N/b^2$. Soit $\sum_n c(n) q^{n/\ell}$ le développement de f en a/b . Avant d'énoncer la prochaine proposition, remarquons que comme $b^2 | N$, on a :

$$S_b^a W_N \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} (S_b^a W_N)^{-1} = \begin{pmatrix} 1 - \frac{aN}{b} & \frac{N}{b^2} a^2 \\ -N & 1 + \frac{aN}{b} \end{pmatrix} \in \Gamma_0(N) .$$

On en déduit que la fonction $f|_{S_b^a}|_{W_N}$ est périodique de période 1, elle admet donc un développement de la forme : $f|_{S_b^a}|_{W_N} = \sum_n a'(n) q^n$.

Proposition III.2.3 *On a :*

$$\sum_{n \geq 1} c(n) q^{n/\ell} = \frac{1}{\ell^{k/2}} \sum_{n \geq 1} a'(n) \zeta^n q^{n/\ell} ,$$

où $\zeta^N = 1$ et $\sum_n a'(n) q^n = f|_{S_b^a}|_{W_N}$.

Preuve : On pose :

$$M = \begin{pmatrix} a & x \\ b & y \end{pmatrix} \in SL_2(\mathbb{Z}) .$$

D'une part, on a :

$$f|_{S_b^a}|_{W_N}|_{W_N}|_{S_b^{-a}}|_M = (-1)^k f|_M = \sum_{n \geq 1} c(n) q^{n/\ell} .$$

Et d'autre part :

$$f|_{S_b^a}|_{W_N}|_{W_N}|_{S_b^{-a}}|_M = f|_{S_b^a}|_{W_N}|_{M'} ,$$

avec :

$$M' = \frac{1}{b} W_N S_b^{-a} M = \begin{pmatrix} 1 & y/b \\ 0 & N/b^2 \end{pmatrix} .$$

□

On est amené à trouver les coefficients $a'(n)$. L'idée est d'écrire (formule (III.13)) :

$$\phi(b)f|_{S_b^a} = \sum_{\text{cond}(\chi)|b} \chi(a)f|_{R_\chi(b)} ,$$

puis d'étudier l'action de W_N sur les $f|_{R_\chi(b)}$. Dans certaines situations, $f|_{R_\chi(b)}$ apparaît simplement comme la tordue de f par le caractère χ . On peut alors espérer que f_χ soit une newform, et ainsi pouvoir obtenir des informations sur les coefficients de $f_\chi|_{W_N}$.

Définition III.2.4 Soit χ un caractère modulo $b = \prod_{j \in J} p_j^{\alpha_j}$. On pose alors $r = |J|$. On décompose le caractère en ses composantes primaires :

$$\chi = \chi_1 \chi_2 \cdots \chi_r ,$$

où χ_j est un caractère modulo $p_j^{\alpha_j}$. On définit $\text{cond}'(\chi)$ par multiplicativité, en posant :

$$\text{cond}'(\chi_j) = \begin{cases} \text{cond}(\chi_j) & \text{si } \chi \text{ n'est pas le caractère trivial modulo } p_j^{\alpha_j} \\ p_j & \text{sinon.} \end{cases}$$

Enfin, si $I = \{j \in J \mid \chi_j \text{ est le caractère trivial modulo } p_j^{\alpha_j}\}$, on pose $tr = \prod_{j \in I} p_j^{\alpha_j}$, $nt = \prod_{j \in J \setminus I} p_j^{\alpha_j}$, $\chi_{tr} = \prod_{j \in I} \chi_j$ et $\chi_{nt} = \prod_{j \in J \setminus I} \chi_j$. On définit :

$$g'(\chi) = (-1)^{|I|} \chi_{nt}(tr) g(\chi_{nt}) ,$$

où $g(\chi_{nt})$ est la somme de Gauss de χ_{nt} .

Nous allons utiliser le lemme suivant qui permet de décomposer l'action de $R_\chi(b)$ en plusieurs composantes.

Lemme III.2.5 Soient n et m deux nombres premiers entre eux, et $\chi = \chi_n \chi_m$, un caractère modulo nm . On a :

$$f|_{R_\chi(nm)} = \overline{\chi_m}(n) \overline{\chi_n}(m) f|_{R_{\chi_n}(n)}|_{R_{\chi_m}(m)} . \quad (\text{III.17})$$

Preuve : On écrit :

$$\begin{aligned} f|_{R_{\chi_n}(n)}|_{R_{\chi_m}(m)} &= \sum_{a \bmod m} \overline{\chi_m}(a) \left(\sum_{b \bmod n} \overline{\chi_n}(b) f|_{S_b^n} \right) |_{S_m^a} \\ &= \sum_{a \bmod m} \sum_{b \bmod n} \overline{\chi_m}(a) \overline{\chi_n}(b) f|_{S_{mn}^{bm+an}} \\ &= \chi_m(n) \chi_n(m) \sum_{a \bmod m} \sum_{b \bmod n} \overline{\chi}(an + bm) f|_{S_{mn}^{bm+an}} \\ &= \chi_m(n) \chi_n(m) \sum_{v \bmod mn} \overline{\chi}(v) f|_{S_{mn}^v} = f|_{R_\chi(mn)} . \end{aligned}$$

□

Proposition III.2.6 *Si $a(p) = 0$ pour tout $p \mid b$, on a :*

$$\phi(b)f|_{S_b^a} = \sum_{\text{cond}'(\chi)=b} \chi(a)g'(\overline{\chi})f_{\chi_{nt}} . \quad (\text{III.18})$$

Preuve : En faisant une récurrence à partir de la formule (III.17), on montre que l'on a :

$$f|_{R_\chi(p_1^{\alpha_1} \dots p_r^{\alpha_r})} = \overline{\chi_1} \left(\frac{b}{p_1^{\alpha_1}} \right) \cdots \overline{\chi_r} \left(\frac{b}{p_r^{\alpha_r}} \right) f|_{R_{\chi_1}(p_1^{\alpha_1}) | \dots | R_{\chi_r}(p_r^{\alpha_r})} . \quad (\text{III.19})$$

D'après les formules (III.11) et (III.12), on obtient :

$$f|_{R_{\chi_j}(p_j^{\alpha_j})} = \begin{cases} 0 & \text{si } 1 < \text{cond}(\chi_j) < p_j^{\alpha_j} \quad \text{ou si } \text{cond } \chi_j = 1 \text{ et } \alpha_j \neq 1 \\ -f & \text{si } \text{cond}(\chi_j) = 1 \quad \text{et } \alpha_j = 1 \\ g(\overline{\chi_j})f|_{\chi_j} & \text{si } \text{cond}(\chi_j) = p_j^{\alpha_j} \end{cases} .$$

On voit donc, grâce à la formule (III.19) que $f|_{R_\chi(b)} = 0$ dès que $\text{cond}'(\chi) \neq b$. Sinon, on a :

$$\begin{aligned} f|_{R_\chi(p_1^{\alpha_1} \dots p_r^{\alpha_r})} &= f|_{R_{\chi_{tr}\chi_{nt}}(tr \, nt)} \\ &= \overline{\chi_{tr}}(nt) \overline{\chi_{nt}}(tr) f|_{R_{\chi_{tr}}(tr) | R_{\chi_{nt}}(nt)} \\ &= (-1)^{|I|} \chi_{nt}(tr) g(\overline{\chi_{nt}}) f_{\chi_{nt}} . \end{aligned}$$

□

Remarque : Comme $b^2 \mid N$, la condition $a(p) = 0$ pour tout $p \mid b$ est vérifiée dès que ε est un caractère modulo N/p ([Li 1]). C'est en particulier le cas si ε est le caractère trivial.

Corollaire III.2.7 *On suppose que la forme f est p -primitive et que $a(p) = 0$ pour tout $p \mid b$. Alors $f|_{\chi_{nt}} \in \mathcal{N}_k(N, \varepsilon_{\chi_{nt}}^2)$ et :*

$$\sum_n a'(n)q^n = \frac{1}{\phi(b)} \sum_{n \geq 1} \overline{a(n)} \left(\sum_{\text{cond}'(\chi)=b} \chi(a)g'(\overline{\chi})\lambda_N(f_{\chi_{nt}})\overline{\chi_{nt}}(n) \right) q^n .$$

Preuve : Pour $p \mid N$, notons ε_p la p -partie du caractère ε . Les hypothèses du corollaire entraînent que $\text{cond}(\varepsilon_p)^2 \mid N$ dès que $p \mid b$ ([Atkin-Li]). Ainsi, on a $f_{\chi_{nt}} \in S_k(N, \varepsilon_{\chi_{nt}}^2)$ ([Atkin-Li]). De plus, f étant p -primitive pour tout $p \mid b$, la forme $f_{\chi_{nt}}$ est une newform et son niveau est au moins N ([Atkin-Li]). En utilisant alors la formule (III.10), on en déduit le corollaire. □

Corollaire III.2.8 *Si $b = p^\alpha$ (i.e. $r=1$) et si $a(p) = 0$ alors :*

$$\phi(b)f|_{S_b^a} = \sum_{\text{cond } \chi=b} \chi(a)g(\overline{\chi})f_\chi - \begin{cases} f & \text{si } \alpha = 1 \\ 0 & \text{sinon} \end{cases} .$$

Exemple : Prenons $p = 2$ et supposons que $a(2) = 0$.

- Si $b = 2$ (et $4 \mid N$), il n'y a pas de caractère modulo 2 : $f|_{S_2} = -f$ et le développement de Fourier en $1/2$ est donc :

$$\frac{\pm 1}{\ell^{k/2}} \sum_{n \geq 1} \overline{a(n)} \zeta^n q^{n/\ell} .$$

Le signe ± 1 provient de l'action de W_N sur f .

- Si $b = 4$, il y a un caractère de conducteur 4 : $\xi(n) = (-1)^{(n-1)/2}$ pour n impair et on a :

$$2f|_{S_4^a} = \xi(a)g(\bar{\xi})f_{\xi} \quad \text{i.e.} \quad f|_{S_4^a} = i\xi(a)f_{\xi} .$$

- Si $b = 8$, il y a deux caractères de conducteur 8 : $\psi(n) = (-1)^{(n^2-1)/8}$ pour n impair et le caractère $\psi\xi$. Il vient :

$$f|_{S_8^a} = \frac{1}{\sqrt{2}} (\psi(a)f_{\psi} + \psi(a)\xi(a)f_{\psi\xi}) .$$

En reprenant notre étude sur les points critiques, on en déduit :

Proposition III.2.9 *Soient E une courbe elliptique de conducteur N pair, f la forme modulaire associée à E et φ le revêtement modulaire. Les pointes de la forme $a/2$ et $a/(N/2)$ ne sont jamais des points critiques pour φ . Si $2^4 \mid N$ et si f est 2-primitive (i.e. la valuation 2-adique de N est impaire ([Atkin-Li])) alors les pointes de la forme $a/4$ et $a/(N/4)$ ne sont pas des points critiques.*

Lorsque la forme f n'est pas p -primitive les actions de W_N sur les différentes tordues de f peuvent être plus délicates à traiter. Dans certains cas, on peut tout de même obtenir quelques résultats. Supposons pour cela que $f \in \mathcal{N}_k(N)$, avec $N = p^2M$, ne soit pas p -primitive avec p premier et $\text{pgcd}(p, M) = 1$. Soit χ un caractère de conducteur p . On décompose l'opérateur W_N en sa p -composante $W_p = W_{p^2}$ et en sa M composante W_M . L'action de W_M sur f_{χ} ne pose aucun problème ; en effet, comme M est premier avec p , on a :

$$f_{\chi}|_{W_M} = \overline{\chi}(M)(f|_{W_M})_{\chi} .$$

Nous nous intéressons donc seulement à l'action de W_{p^2} sur f_{χ} . Comme la forme f n'est pas p -primitive, il existe un caractère χ_0 de conducteur p et une forme $h \in \mathcal{N}(N', \overline{\chi_0}^2)$ telle que $h_{\chi_0} = f$. De plus, on a $N' = pM$ ou $N' = M$.

Proposition III.2.10 *Avec les notations ci-dessus, si $\chi \neq \chi_0$ et $\chi \neq \overline{\chi_0}$ on a :*

$$g(\overline{\chi_0}\chi)f_{\chi}|_{W_{p^2}} = \chi_0(-1)\chi(-1)g(\overline{\chi_0}\chi)f_{\overline{\chi}} .$$

Preuve : Supposons tout d'abord que χ_0^2 n'est pas le caractère trivial modulo p . Alors $N' = pM$ et $h \in \mathcal{N}(pM, \overline{\chi_0}^2)$. On a $\text{cond}(\overline{\chi_0}^2) = p$. On pose $\chi' = \overline{\chi_0}\chi$, $\text{cond}(\chi') = p$. D'après le corollaire 4.2. de [Atkin-Li], on déduit que :

$$\begin{aligned} g(\overline{\chi_0}\chi)h_{\chi_0\chi}|_{W_{p^2}} &= \chi_0(-1)\chi(-1)g(\overline{\chi_0}\chi)h_{\chi_0\overline{\chi}} \\ \text{i.e.} \quad g(\overline{\chi_0}\chi)f_{\chi}|_{W_{p^2}} &= \chi_0(-1)\chi(-1)g(\overline{\chi_0}\chi)f_{\overline{\chi}} . \end{aligned}$$

Si $\chi_0 = \overline{\chi_0}$ alors $h \in \mathcal{N}(N')$. Comme $\text{cond}(\chi_0\chi) = p$, le théorème 4.1. de [Atkin-Li] affirme que :

$$\lambda_p(h_{\chi_0\chi}) = \chi_0(-1)\chi(-1)g(\chi_0\chi)/g(\chi_0\overline{\chi}) .$$

Et on obtient alors, $g(\chi_0\overline{\chi})f_\chi|_{W_{p^2}} = \chi_0(-1)\chi(-1)g(\chi_0\chi)f'$ avec $f' \in \mathcal{N}(N, \overline{\chi}^2)$. On observe que $f' = f_{\overline{\chi}}$. \square

Traitons maintenant le cas où $\chi = \chi_0$:

Proposition III.2.11 *Toujours avec les notations ci-dessus, si $\chi_0 \neq \overline{\chi_0}$, on a :*

$$g(\overline{\chi_0}^2)f_{\chi_0}|_{W_{p^2}} = p h|_{U_p}|_{B_p} - h .$$

Preuve : On utilise toujours le corollaire 4.2. de [Atkin-Li]. On pose $\chi' = \chi_{tr}$ et $\chi = \chi_0^2$. On obtient :

$$g(\overline{\chi})h_\chi|_{W_p^2} = p\chi_0^2(-1) h|_{U_p}|_{B_p} - h .$$

Et la proposition s'ensuit. \square

Lorsque $\chi = \overline{\chi_0}$, alors on a $f_\chi = h - h|_{U_p}|_{B_p}$. Si le niveau exact de h est Mp , l'action de W_{p^2} sur f_χ est donnée par les deux égalités suivantes :

$$\begin{aligned} h|_{W_{p^2}}(\tau) &= p^{k/2}h|_{W_p}(p\tau) , \\ h|_{U_p}|_{B_p}|_{W_{p^2}} &= a(p)p^{k/2}h|_{W_p} . \end{aligned}$$

Ici, W_p est l'opérateur correspondant à l'espace $X_0(pM)$.

Nous terminerons ce chapitre par des exemples provenant de certains revêtements modulaires. Notons que les formes modulaires associées aux courbes elliptiques qui suivent ne sont pas 2-primitives.

Soit E la courbe elliptique de conducteur $N = 48$ et d'équation :

$$y^2 = x^3 + x^2 - 4x - 4 .$$

Soit $f = \sum_n a(n)q^n$ la forme modulaire associée à E . On a :

$$f|_{S_4^a} = i \xi(a)f_\xi .$$

Or, $f_\xi = h \in S_2(24)$ (ici h est la forme modulaire associée à la courbe elliptique de conducteur 24). On a alors :

$$h|_{W_{48}}(\tau) = -2h(2\tau) ,$$

et ainsi :

$$f|_{S_4^a}|_{W_{48}} = -2i \sum_{n \geq 1} a(n)(-1)^{(n-1)/2} q^{2n} .$$

De la proposition III.2.3, on déduit que les pointes $\pm 1/4$ et $\pm 1/12$ sont des points critiques de φ . Le genre de $X_0(48)$ étant égal à 3, ce sont les seuls points critiques du revêtement modulaire.

On considère la courbe E de conducteur $N = 64$ et d'équation :

$$y^2 = x^3 - 4x \quad .$$

On a :

$$f|_{S_8^a} = \frac{1}{\sqrt{2}} (\psi(a)f_\psi + \psi(a)\xi(a)f_{\psi\xi}) \quad .$$

Or $f_\psi = f_{\psi\xi} = h \in S_2(32)$ et $h|_{W_{64}}(\tau) = 2h(2\tau)$. On en déduit que les développements de Fourier de f aux pointes $1/8, 3/8, 5/8$ et $7/8$ sont donnés par :

$$\pm\sqrt{2}(1 \pm i) \sum_{n \geq 1} a(n)\psi(n)\zeta^n q^{2n/\ell} \quad ,$$

et que les pointes de la forme $a/8$ sont les quatre points critiques du revêtement modulaire.

Soit E la courbe d'équation :

$$y^2 = x^3 - 7x + 6 \quad ,$$

de conducteur $N = 80$. Comme dans le premier exemple, on a $f|_{S_4^a} = i\xi(a)f_\xi$, où ici $f_\xi = h \in S_2(40)$ et $h|_{W_{80}}(\tau) = -2h(2\tau)$. On en déduit que les pointes $\pm 1/4$ et $\pm 1/20$ sont 4 points critiques de φ . Les 8 autres points critiques sont des points de Heegner (c'est en fait l'exemple traité en détail dans la section III.1.3).

Enfin, soit E d'équation :

$$y^2 = x^3 - x^2 + 4x - 4 \quad ,$$

de conducteur $N = 80$. On a toujours $f|_{S_4^a} = i\xi(a)f_\xi$ mais cette fois-ci $f_\xi = h \in S_2(20)$ et $h|_{W_{80}}(\tau) = -4h(4\tau)$. On voit alors que les pointes $\pm 1/4$ et $\pm 1/20$ sont des points critiques d'ordre 3 de φ et sont donc les seuls points critiques.

Les 4 exemples que nous venons de donner sont les seuls exemples de courbes elliptiques de conducteur $N \leq 100$ pour lesquels des pointes de $X_0(N)$ sont aussi des points critiques du revêtement modulaire.

Chapitre IV

Heuristiques sur les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q}

Dans leur article [Cohen-Lenstra], Cohen et Lenstra donnent des conjectures sur les groupes de classes des corps de nombres. Dans ce chapitre, nous faisons un travail similaire au leur, pour les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q} . Pour cela, nous devons prendre en compte que ces groupes possèdent une structure particulière puisque, d'après un théorème de Cassels, ils sont munis (s'ils sont finis) d'une forme bilinéaire alternée non dégénérée. Après avoir établi quelques propriétés de ces groupes, nous donnons des heuristiques similaires à celles de Cohen et Lenstra adaptées à notre situation. Ce chapitre s'inspire largement de [Delaunay].

IV.1 Motivations et notations

Nous voulons faire une étude sur les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q} similaire à celle faite dans [Cohen-Lenstra] sur les groupes de classes d'un corps de nombres. On s'inspire pour cela de l'analogie certaine qui existe entre les corps de nombres d'une part, et les courbes elliptiques d'autre part. On peut la voir grâce aux correspondances suivantes :

Courbes elliptiques E/\mathbb{Q}		Corps de nombres K	
$E(\mathbb{Q})_{\text{tors}}$	\rightleftharpoons	$U(K)_{\text{tors}}$	racines de l'unité de K
$E(\mathbb{Q})$	\rightleftharpoons	$U(K)$	groupe des unités de K
$\text{III}(E)$	\rightleftharpoons	$Cl(K)$	groupe des classes de K
$R(E)$	\rightleftharpoons	$R(K)$	régulateur de K

Les parties de torsion des groupes $E(\mathbb{Q})$ et $U(K)$ sont toutes les deux faciles à déterminer

et jouent le même rôle. Pour un corps de nombres K , on connaît rapidement le rang du groupe des unités puisqu'il est égal à $r_1 + r_2 - 1$ où r_1 (resp. r_2) est le nombre de places réelles (resp. complexes) de K . Cependant, les unités ne sont pas toujours faciles à trouver. Pour le groupe de Mordell-Weil d'une courbe elliptique E , le rang est prédit par la conjecture de Birch et Swinnerton-Dyer, et calculer les points rationnels de $E(\mathbb{Q})$ peut aussi poser des difficultés si les générateurs ont de grands dénominateurs. Le groupe des classes d'un corps de nombres mesure, en quelque sorte, l'obstruction aux idéaux d'être principaux. Lorsque ce groupe n'est pas trivial, l'arithmétique dans K est plus compliquée à faire. De même, le groupe de Tate-Shafarevitch III d'une courbe elliptique mesure l'obstruction au principe "local-global". Lorsque III n'est pas trivial, l'étude de la courbe est rendue plus délicate. De plus, tout comme les points de Heegner pour les courbes elliptiques, il existe un procédé analytique pour obtenir certaines unités d'un corps de nombres.

Enfin, pour un corps de nombres K , on a la suite exacte suivante :

$$1 \rightarrow U(K)/U(K)^p \rightarrow S_p(K) \rightarrow Cl(K)[p] \rightarrow 1$$

où $S_p(K) = \{\alpha \in K^* | \alpha \mathbb{Z}_K = \mathfrak{q}^p\} / K^{*p}$ est le p -groupe de Selmer de K (cf. [Cohen 2] pour cette terminologie). Si $L(K, s)$ désigne la série L de K (i.e. la fonction zêta de Dedekind), on a :

$$L(K, s) \sim_{s=0} -s^r \frac{R(K) |Cl(K)|}{|U(K)_{\text{tors}}|} ,$$

où $r = r_1 + r_2 - 1$ est le rang du groupe des unités de K .

Pour une courbe elliptique E :

$$1 \rightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \rightarrow S_p(E) \rightarrow \text{III}(E)[p] \rightarrow 1 ,$$

où $S_p(E)$ est p -groupe de Selmer de E . Si $L(E, s)$ est la série L de E , la conjecture de Birch et Swinnerton-Dyer affirme que :

$$L(E, s) \sim_{s=1} (s-1)^r \frac{R(E) |\text{III}(E)|}{(|E(\mathbb{Q})_{\text{tors}}|)^2} c \Omega . \quad (\text{IV.1})$$

Ce sont clairement des expressions du même type. Cependant, pour la formule (IV.1), les termes principaux de droites sont des carrés :

- $R(E)$ est le déterminant d'une matrice de Gram (moralement c'est un carré).
- L'ordre du groupe $\text{III}(E)$ est un carré (s'il est fini).
- Au dénominateur se trouve le carré de l'ordre du groupe de torsion de $E(\mathbb{Q})$.

Nous admettons dans toute cette partie, la conjecture selon laquelle le groupe de Tate-Shafarevitch III d'une courbe elliptique est fini. Dans ces conditions, le groupe III est muni d'une forme β bilinéaire alternée non dégénérée à valeur dans \mathbb{Q}/\mathbb{Z} (cf. [Cassels]).

Nous dirons qu'un couple (G, β) est un groupe de type S si G est un groupe abélien fini et :

$$\beta : G \times G \longrightarrow \mathbb{Q}/\mathbb{Z} ,$$

tel que :

- β est bilinéaire.
- $\beta(x, x) = 0 \in \mathbb{Q}/\mathbb{Z}$ pour tout $x \in G$. Ceci entraîne que f est antisymétrique (i.e. $f(x, y) = -f(y, x)$). Il est à noter que la réciproque n'est vraie que dans le cas où l'espace d'arrivée vérifie $2a = 0 \Rightarrow a = 0$.
- Si $\beta(x, y) = 0$ pour tout $y \in G$ alors $x = 0$.

Nous sommes ainsi amenés à étudier de tels groupes. Deux groupes (G_1, β_1) et (G_2, β_2) de types S sont dit isomorphes s'il existe un isomorphisme de groupes $\sigma : G_1 \rightarrow G_2$ tel que :

$$\beta_2(\sigma(x), \sigma(y)) = \beta_1(x, y) \quad \text{pour tout } x, y \in G_1 .$$

Dans [Cohen-Lenstra], les groupes étudiés sont simplement les groupes abéliens finis et l'idée principale est, en quelque sorte, de pondérer chaque groupe G par un poids proportionnel à $1/|\text{Aut}(G)|$. Ici, nous devons remplacer $\text{Aut}(G)$ par son analogue $\text{Aut}^s(G)$ le groupe des automorphismes de (G, β) qui respectent la forme β .

On note \mathbb{P} l'ensemble des nombres premiers, dans la suite, la lettre p désignera toujours un élément de \mathbb{P} . De plus, on note $(q)_a$ le nombre :

$$\prod_{1 \leq i \leq a} (1 - q^i) , \quad \text{pour } a \in \mathbb{N} \text{ et } q \in \mathbb{R} .$$

Si G est un groupe abélien, on désigne par $r_p(G)$ le p -rang de G .

Dans [Cohen-Lenstra] on écrit $\sum_{G(n)}$ pour signifier que la somme porte sur tous les groupes

d'ordres n à isomorphisme près. De la même manière, on écrit : $\sum_{G^s(n)}$ pour une somme

qui porte sur tous les groupes de type S d'ordres n à isomorphisme près. Enfin, on définit pour (G, β) un groupe de type S :

$$\begin{aligned} w^s(G) &= \frac{1}{|\text{Aut}^s(G)|} \\ w^s(n) &= \sum_{G^s(n)} w^s(G) \\ w_a^s(G) &= \frac{1}{|\text{Aut}^s(G)|} \prod_{p|G} \frac{(1/p^2)_a}{(1/p^2)_{a-r_p(G)/2}} \\ w_a^s(n) &= \sum_{G^s(n)} w_a^s(G) \end{aligned}$$

qui jouent, comme nous le montrerons, des rôles analogues à (cf. [Cohen-Lenstra]) :

$$\begin{aligned}
 w(G) &= \frac{1}{|\mathrm{Aut}(G)|} \\
 w(n) &= \sum_{G(n)} w(G) \\
 w_a(G) &= \frac{|\{f : \mathbb{Z}^a \mapsto G \mid f \text{ homo. surjectif de groupe}\}|}{|G|^a |\mathrm{Aut}(G)|} \\
 &\stackrel{\text{th. [Cohen-Lenstra]}}{=} \frac{1}{|\mathrm{Aut}(G)|} \prod_{p \mid |G|} \frac{(1/p)_a}{(1/p)_{a-r_p(G)}} \\
 w_a(n) &= \sum_{G(n)} w_a(G)
 \end{aligned}$$

Nous ne savons pas donner pour $w_a^s(G)$ une définition similaire à $w_a(G)$ (i.e. en terme d'homomorphismes surjectifs ou du même style), c'est pour cela que l'on donne directement une formule qui paraît arbitraire, mais nous verrons dans la suite que c'est la formule qui convient.

IV.2 Groupes de type S

Commençons cette section en donnant un exemple fondamental de groupe de type S. On prend pour le groupe G :

$$G = (\mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p^{a_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{a_2}\mathbb{Z} \oplus \mathbb{Z}/p^{a_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{a_j}\mathbb{Z} \oplus \mathbb{Z}/p^{a_j}\mathbb{Z})$$

avec $a_1 \leq a_2 \leq \cdots \leq a_j$.

On note e_1, e_2, \dots, e_{2j} une “base canonique” (par exemple on prend pour e_i l'élément de G dont la i -ème composante est inversible modulo p , les autres étant nulles). On définit une forme bilinéaire alternée β en prenant :

$$\begin{aligned}
 f(e_{2i-1}, e_{2i}) &= -f(e_{2i}, e_{2i-1}) = 1/p^{a_i} \in \mathbb{Q}/\mathbb{Z} \\
 f(e_i, e_j) &= 0 \quad \text{sinon.}
 \end{aligned}$$

Il est facile de voir que (G, β) est un groupe de type S. Ainsi, si un groupe abélien fini G est de la forme $G = H \times H$, on peut le munir, par cette construction, d'une forme bilinéaire alternée non dégénérée (les p -composantes étant deux à deux orthogonales). Nous allons maintenant établir la réciproque.

Lemme IV.2.1 *Soit (G, β) un groupe de type S avec G un p -groupe. Soit $x \in G$ un élément d'ordre maximal, disons p^k . Alors :*

- *Il existe $y \in G$ d'ordre p^k avec $\beta(x, y) = 1/p^k \in \mathbb{Q}/\mathbb{Z}$.*
- *Il existe un sous groupe H de G tel que $(H, \beta|_{H \times H})$ soit un groupe de type S, et avec $G = (\langle x \rangle \oplus \langle y \rangle) \stackrel{\perp}{\oplus} H$.*

Preuve : Il existe dans G un élément y tel que $\beta(x, y) = a/p^k \in \mathbb{Q}/\mathbb{Z}$ avec $(a, p) = 1$. En effet : sinon $p^{k-1}x$ est dans le noyau de β donc est nul (β est non dégénérée) ce qui contredit le fait que x est d'ordre p^k .

Quitte à remplacer x par bx où b est l'inverse de a modulo p^k , on peut supposer que l'on a $\beta(x, y) = 1/p^k$. Il est alors clair que l'ordre de y est p^k (par maximalité de l'ordre). On a $\langle x, y \rangle = \langle x \rangle \oplus \langle y \rangle$ car si $\lambda x = \nu y$ alors $\beta(x, \nu y) = 0$ ainsi $p^k | \nu$ et $\nu y = \lambda x = 0$.

On pose alors $H = \{z \in G | \beta(x, z) = \beta(y, z) = 0\}$ et on constate que :

- H est un sous groupe de G .
- $H \cap \langle x, y \rangle = \{0\}$ car si $\lambda x + \nu y \in H$ on a $\beta(x, \lambda x + \nu y) = 0 = \nu/p^k$ donc $\nu y = 0$ de même $\lambda x = 0$.
- $G = \langle x, y \rangle \oplus H$ car tout élément $w \in G$ s'écrit sous la forme : $w = -p^k \beta(y, w)x + p^k \beta(x, w)y + (w + p^k \beta(y, w)x - p^k \beta(x, w)y)$.
- Et enfin $\beta|_{H \times H}$ est non dégénérée. □

Remarque : Dans la preuve du lemme, on a : $\langle x, y \rangle \simeq \mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^k\mathbb{Z}$.

On déduit du lemme le résultat suivant :

Proposition IV.2.2 *Soit (G, β) un p -groupe de type S , alors (G, β) est isomorphe au groupe de type S de l'exemple fondamental (avec des a_i convenables). En particulier $G \simeq H \times H$ et la structure de $\text{Aut}^s(G)$ est indépendante de β .*

Preuve : On démontre cette proposition par récurrence sur l'ordre du groupe en utilisant le lemme précédent.

Corollaire IV.2.3 *Si (G, β) est un groupe de type S , alors l'ordre de G est un carré parfait.*

On en déduit que $w_a^s(n) = w^s(n) = 0$ si n n'est pas un carré parfait.

Nous allons maintenant étudier le groupe $\text{Aut}^s(G)$ d'un groupe (G, β) de type S . Tout d'abord rappelons que les groupes abéliens d'ordre p^n sont en bijection avec les partitions de n .

Soit (ν) une partition de n , on note λ_i le nombre de i apparaissant dans cette partition si bien que l'on a $n = \lambda_1 + 2\lambda_2 + \dots + j\lambda_j$.

De plus, on note $\mu_1, \mu_2, \dots, \mu_j$ les parts de la partition associée à (ν) avec $\mu_k = \lambda_k + \lambda_{k+1} + \dots + \lambda_j$; on a bien $n = \mu_1 + \mu_2 + \dots + \mu_j$. On peut alors énoncer :

Théorème IX *Soit (G, β) un p -groupe de type S d'ordre p^{2n} avec $G \simeq H \times H$ et*

$$H \simeq (\mathbb{Z}/p\mathbb{Z})^{\lambda_1} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{\lambda_2} \oplus \dots \oplus (\mathbb{Z}/p^j\mathbb{Z})^{\lambda_j} .$$

Alors, en gardant les notations précédentes on a :

$$|\text{Aut}^s(G)| = p^{2(\mu_1^2 + \dots + \mu_j^2) + n} \prod_{1 \leq i \leq j} \left(\frac{1}{p^2} \right)_{\lambda_i} .$$

Le reste de la section est consacrée à la démonstration de ce théorème.

Définition IV.2.4 Soit a, b deux entiers positifs. Un vecteur de $(\mathbb{Z}/p^a\mathbb{Z})^b$ est dit d'ordre p^a si au moins une de ses composantes est d'ordre p^a . On pose :

$$S_a^b = |\{x \in (\mathbb{Z}/p^a\mathbb{Z})^b \mid \text{l'ordre de } x \text{ est } p^a\}|.$$

On a alors :

Proposition IV.2.5

$$S_a^b = p^{ba} \left(1 - \frac{1}{p^b}\right).$$

Preuve : Par récurrence sur b . Pour S_a^{b+1} , on compte le nombre de vecteurs dont toutes les composantes sont multiples de p . Pour la première, il y en a p^{a-1} , et pour les autres $p^{ba} - S_a^b = p^{b(a-1)}$ d'après l'hypothèse de récurrence. En tout, cela fait $p^{(b+1)(a-1)}$ vecteurs et la proposition est alors immédiate. \square

Preuve du théorème IX : Par récurrence sur n . On écrit :

$$G = \left(\underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}}_{2\lambda_1 \text{ fois}} \right) \oplus \left(\underbrace{\mathbb{Z}/p^2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^2\mathbb{Z}}_{2\lambda_2 \text{ fois}} \right) \oplus \cdots \oplus \left(\underbrace{\mathbb{Z}/p^j\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^j\mathbb{Z}}_{2\lambda_j \text{ fois}} \right)$$

On choisit la forme β de l'exemple fondamental.

Un automorphisme σ est donné par l'image d'une base de G . On prend la "base canonique" e_1, e_2, \dots , avec disons e_1 et e_2 les éléments de G ayant respectivement un "1" sur la dernière et l'avant dernière composante (et des zéros partout ailleurs); e_1 et e_2 sont d'ordre p^j .

Pour que σ respecte la forme β il faut et il suffit que $\beta(\sigma(e_i), \sigma(e_l)) = \beta(e_i, e_l)$.

Pour l'image de e_1 , on choisit un vecteur x d'ordre p^j (ordre maximal); il y en a :

$$\underbrace{p^{2j\lambda_j} \left(1 - \frac{1}{p^{2\lambda_j}}\right)}_{\substack{\text{nombre d'éléments} \\ \text{d'ordre } p^j \text{ dans } (\mathbb{Z}/p^j\mathbb{Z})^{2\lambda_j}}} \times \underbrace{p^{2n-2j\lambda_j}}_{\substack{\text{nombre de possibilités} \\ \text{pour remplir les autres} \\ \text{composantes}}} = p^{2n} \left(1 - \frac{1}{p^{2\lambda_j}}\right)$$

Ensuite, on choisit un élément $y' \in G$ comme dans le lemme IV.2.1. On a :

- $\beta(x, y') = 1/p^j$;
- $G = (\langle x \rangle \oplus \langle y' \rangle) \oplus^\perp H$

Pour l'image de e_2 , on choisit un vecteur y tel que $\beta(x, y) = \beta(e_1, e_2) = 1/p^j$. Il est facile de voir grâce à la dernière décomposition de G que l'on en a :

$$|\{y \in G | f(x, y) = 1/p^j\}| = p^{2n-j} .$$

On a donc fixé l'image de e_1 et de e_2 .

Pour e_3, e_4, \dots , on remarque qu'ils forment une base d'un groupe de type S isomorphe à H , et que leurs images doivent appartenir à H . Il y a donc $|\text{Aut}^s(H)|$ possibilités. On peut ainsi utiliser l'hypothèse de récurrence et un petit calcul donne le résultat voulu. \square

Remarque : En adaptant les calculs, on peut démontrer exactement de la même façon que l'ordre du groupe symplectique $S_p(2n, q)$ est :

$$|S_p(2n, q)| = q^{n^2} \prod_{1 \leq i \leq n} (q^{2i} - 1) .$$

Si $q = p$ est un nombre premier, on retrouve aussi ce résultat en appliquant le théorème avec $\lambda_1 = n$.

IV.3 Séries de Dirichlet et moyennes

IV.3.1 Deux séries de Dirichlet

Nous allons étudier ici $w^s(n^2)$ et $w_a^s(n^2)$. Rappelons tout d'abord un résultat de Hall (cf.[Hall]) :

Théorème X (Hall) *On a l'identité formelle : (en gardant les notations précédentes)*

$$\frac{x^n}{(x)_n} = \sum_{(\nu)=n} \frac{x^{\mu_1^2 + \mu_2^2 + \dots + \mu_j^2}}{(x)_{\lambda_1} (x)_{\lambda_2} \dots (x)_{\lambda_j}} ,$$

où la somme porte sur toutes les partitions (ν) de n .

De ce théorème, on déduit :

$$\frac{(1/p^2)^n}{(1/p^2)_n} = \sum_{(\nu)=n} \frac{(1/p)^{2(\mu_1^2 + \dots + \mu_j^2)}}{(1/p^2)_{\lambda_1} (1/p^2)_{\lambda_2} \dots (1/p^2)_{\lambda_j}} \text{ en prenant } x = 1/p^2 ,$$

donc :

$$\frac{(1/p)^{3n}}{(1/p^2)_n} = \sum_{(\nu)=n} \frac{(1/p)^{2(\mu_1^2 + \dots + \mu_j^2) + n}}{(1/p^2)_{\lambda_1} (1/p^2)_{\lambda_2} \dots (1/p^2)_{\lambda_j}} \text{ en multipliant par } (1/p)^n .$$

Le terme dans la somme est exactement $1/|\text{Aut}^s(G)|$ pour le groupe G correspondant à la partition ν d'où :

Proposition IV.3.1 On a :

$$\sum_{G^s(p^{2n})} \frac{1}{|\text{Aut}^s(G)|} = \frac{1}{p^{3n} (1/p^2)_n} .$$

On en déduit le corollaire suivant :

Corollaire IV.3.2

$$\sum_{G^s(n^2)} \frac{1}{|\text{Aut}^s(G)|} = \frac{1}{n^3} \prod_{p^\alpha \parallel n} \frac{1}{(1/p^2)_\alpha} .$$

Dans [Cohen-Lenstra], on généralise en quelque sorte la formule de Hall pour la famille de poids $w_k(G)$. En particulier, on trouve le théorème suivant :

Théorème XI (Cohen-Lenstra)

$$\sum_{G(n)} w_a(G) = \frac{1}{n} \prod_{p^\alpha \parallel n} \frac{(1/p)_{\alpha+a-1}}{(1/p)_{a-1} (1/p)_\alpha} .$$

Comme tout est multiplicatif, on peut regarder ce qui se passe pour les p -groupes, on obtient :

$$\sum_{G(p^n)} w_a(G) = \frac{1}{p^n} \frac{(1/p)_{n+a-1}}{(1/p)_{a-1} (1/p)_n} . \quad (\text{IV.2})$$

On sait que pour un p -groupe G correspondant à la partition (ν) de n on a (cf. [Hall] par exemple) :

$$|\text{Aut}(G)| = p^{\mu_1^2 + \dots + \mu_j^2} \prod_{1 \leq i \leq j} \left(\frac{1}{p} \right)_{\lambda_i} .$$

On déduit de cette formule et de la formule (IV.2) que :

$$\sum_{(\nu)=n} \frac{(1/p)_n}{(1/p)_{a-r(\nu)}} \frac{(1/p)^{\mu_1^2 + \dots + \mu_j^2}}{(1/p)_{\lambda_1} \dots (1/p)_{\lambda_j}} = \frac{1}{p^n} \frac{(1/p)_{n+a-1}}{(1/p)_{a-1} (1/p)_n} .$$

où la somme porte sur toutes les partitions de n et $r(\nu)$ désigne le nombre de parts de (ν) .

La formule précédente étant vraie pour tout p , c'est une égalité de fractions rationnelles. On peut donc substituer p^2 à p , puis multiplier le tout par $1/p^n$ et on obtient :

$$\sum_{(\nu)=n} \frac{(1/p^2)_n}{(1/p^2)_{a-r(\nu)}} \frac{(1/p)^{2(\mu_1^2 + \dots + \mu_j^2) + n}}{(1/p^2)_{\lambda_1} \dots (1/p^2)_{\lambda_j}} = \frac{1}{p^{3n}} \frac{(1/p^2)_{n+a-1}}{(1/p^2)_{a-1} (1/p^2)_n} .$$

Or le terme dans la somme est exactement $w_a^s(G)$ pour le groupe G de type S correspondant à (ν) ($r(\nu) = r_p(G)/2$) ; on vient donc d'établir :

Proposition IV.3.3

$$\sum_{G^s(p^{2n})} w_a^s(G) = \frac{1}{p^{3n}} \frac{(1/p^2)_{n+a-1}}{(1/p^2)_{a-1}(1/p^2)_n} .$$

Il s'ensuit :

Corollaire IV.3.4

$$\sum_{G^s(n^2)} w_a^s(G) = \frac{1}{n^3} \prod_{p^\alpha \parallel n} \frac{(1/p^2)_{\alpha+a-1}}{(1/p^2)_{a-1}(1/p^2)_\alpha} .$$

Les deux dernières formules généralisent celles obtenues avec $w^s(G)$ puisqu'on les retrouve en faisant $a \rightarrow +\infty$.

On définit maintenant deux séries de Dirichlet par :

$$\begin{aligned} \zeta^s(z) &= \sum_{n=1}^{\infty} \frac{w^s(n)}{n^z} , \\ \zeta_a^s(z) &= \sum_{n=1}^{\infty} \frac{w_a^s(n)}{n^z} . \end{aligned}$$

On aura besoin de la formule suivante :

Proposition IV.3.5 *Soit a un entier positif ou nul, on a l'égalité formelle :*

$$\sum_{\beta=0}^{\infty} X^\beta \frac{(X)_{\beta+a}}{(X)_\beta (X)_a} Y^\beta = \prod_{j=1}^{a+1} \frac{1}{1 - X^j Y} .$$

Preuve : Par récurrence sur a . □

En faisant $a \rightarrow +\infty$, on retrouve une identité due à Euler :

$$\sum_{\beta=0}^{\infty} \frac{X^\beta}{(X)_\beta} Y^\beta = \prod_{j=1}^{\infty} \frac{1}{1 - X^j Y} .$$

On peut alors démontrer le théorème suivant :

Théorème XII *On a :*

$$\begin{aligned} \zeta_a^s(z) &= \sum_{n=1}^{\infty} \frac{w_a^s(n)}{n^z} = \prod_{j=1}^a \zeta(2z + 2j + 1) , \\ \zeta^s(z) &= \sum_{n=1}^{\infty} \frac{w^s(n)}{n^z} = \prod_{j=1}^{\infty} \zeta(2z + 2j + 1) , \end{aligned}$$

où ζ désigne la fonction zêta de Riemann.

Preuve : On démontre la première formule, la deuxième s'obtient exactement de la même manière (ou en faisant $a = +\infty$).

$$\begin{aligned}
\zeta_a^s(z) &= \sum_{n=1}^{\infty} \frac{w_a^s(n)}{n^z} \\
&= \prod_p \left(\sum_{\nu=0}^{\infty} \frac{1}{p^{\nu z}} w_a^s(p^{\nu}) \right) \quad (\text{la fonction } w_a^s \text{ est multiplicative}) \\
&= \prod_p \left(\sum_{\nu=0}^{\infty} \frac{1}{p^{2\nu z}} w_a^s(p^{2\nu}) \right) \\
&= \prod_p \left(\sum_{\nu=0}^{\infty} \frac{1}{p^{2\nu z}} \frac{1}{p^{3\nu}} \frac{(1/p^2)_{\nu+a-1}}{(1/p^2)_{a-1} (1/p^2)_{\nu}} \right) \\
&= \prod_p \left(\sum_{\nu=0}^{\infty} \frac{1}{p^{2\nu}} \frac{(1/p^2)_{\nu+a-1}}{(1/p^2)_{a-1} (1/p^2)_{\nu}} \frac{1}{p^{\nu(2z+1)}} \right) \\
&= \prod_p \left(\prod_{j=1}^a \frac{1}{1 - (1/p)^{2z+2j+1}} \right) \quad \text{par la proposition IV.3.5}
\end{aligned}$$

Ce qui termine la preuve du théorème. □

Remarque : Ces résultats sont à comparer avec ceux obtenus dans [Cohen-Lenstra] où il est démontré :

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{w_a(n)}{n^z} &= \prod_{j=1}^a \zeta(z + k) \quad , \\
\sum_{n=1}^{\infty} \frac{w(n)}{n^z} &= \prod_{j=1}^{\infty} \zeta(z + k) \quad .
\end{aligned}$$

C'est dans ce sens que w_a^s correspond avec w_a .

IV.3.2 Moyennes

Comme dans [Cohen-Lenstra], nous allons définir la moyenne d'une fonction f définie sur les classes d'isomorphisme des groupes de type S.

Définition IV.3.6 On pose :

$$\begin{aligned} w^s(f, n^2) &= \sum_{G^s(n^2)} w^s(G) f(G) , \\ \zeta^s(f, z) &= \sum_n \frac{w^s(f, n)}{n^z} , \\ w_a^s(f, n^2) &= \sum_{G^s(n^2)} w_a^s(G) f(G) , \\ \zeta_a^s(f, z) &= \sum_n \frac{w_a^s(f, n)}{n^z} . \end{aligned}$$

Définition IV.3.7 Soit $u \geq 0$, on définit les nombres $c_{a,u}(f, n)$ par :

$$\sum_{n=1}^{\infty} \frac{c_{a,u}(f, n)}{n^z} = \frac{\zeta_a^s(f, z+u) \zeta_a^s(z)}{\zeta_a^s(z+u)} .$$

La (a, u) -moyenne de f est alors donnée par :

$$M_{a,u}^s(f) = \lim_{x \rightarrow +\infty} \frac{\sum_{n \leq x} n c_{a,u}(f, n)}{\sum_{n \leq x} n w_a^s(n)} .$$

Si $a = +\infty$, on parle de u -moyenne de f et on écrit $M_u^s(f)$ au lieu de $M_{+\infty,u}^s(f)$.

Remarque : Cette définition est l'analogue de la définition de (a, u) -moyenne dans [Cohen-Lenstra]. En particulier, la (a, u) -moyenne de f si elle existe est bien une moyenne (i.e. la (a, u) -moyenne d'une fonction constante est égale à cette constante).

Si f est la fonction caractéristique d'une propriété P , on parle de (a, u) -probabilité de P ou simplement de u -probabilité de P .

On a inclus le facteur n dans la définition afin que le terme du dénominateur diverge quand $x \rightarrow \infty$. De plus, on peut montrer que, pour une classe de fonctions raisonnables, la moyenne de f reste inchangée si on remplace n par n^l ($l \geq 1$). Ceci est *faux* si on remplace n par n^l avec $l < 1$, et en particulier si on remplace n par 1.

Nous allons utiliser le théorème Taubérien suivant ([Tenenbaum]) :

Proposition IV.3.8 Soit $(c(n))_n$ une suite de nombres positifs ou nuls. Si la série de Dirichlet $D(z) = \sum_n c(n)/n^z$ converge pour $\Re(z) > 0$ et si $D(z) - C/z$ se prolonge analytiquement à $\Re(z) \geq 0$ alors :

$$\sum_{n \leq x} c(n) \sim C \log(x) .$$

En appliquant cette proposition à $\zeta_a^s(z-1)$ (i.e. $c(n) = nw_a^s(n)$), on obtient :

$$\sum_{n \leq x} nw_a^s(n) \sim \frac{\prod_{2 \leq k \leq a} \zeta(2k-1)}{2} \log(x) .$$

En particulier, en faisant $a \rightarrow \infty$, il vient :

$$\sum_{n \leq x} \sum_{G^s(n)} \frac{|G|}{|\text{Aut}^s(G)|} \sim \frac{\zeta(3)\zeta(5)\zeta(7)\cdots}{2} \log(x) .$$

De plus, le théorème Taubérien permet d'obtenir directement la proposition suivante :

Proposition IV.3.9 *Soit f une fonction positive définie sur les classes d'isomorphisme des groupes de type S . Si $\zeta_a^s(f, z-1)$ converge pour $\Re(z) > 0$ et si $\zeta_a^s(f, z-1) - C/z$ se prolonge analytiquement à $\Re(z) \geq 0$ alors :*

1 Pour $u = 0$:

$$M_{a,0}^s(f) = \frac{2C}{\prod_{2 \leq k \leq a} \zeta(2k-1)} = \lim_{z \rightarrow 0} \frac{\zeta_a^s(f, z-1)}{\zeta_a^s(z-1)} .$$

2 Pour $u \neq 0$:

$$M_{a,u}^s(f) = \frac{\zeta_a^s(f, u-1)}{\zeta_a^s(u-1)} .$$

Pour nos applications, nous devons nous restreindre à des \mathcal{P} -parties de groupes de type S , où $\mathcal{P} \subset \mathbb{P}$ est un ensemble de nombres premiers. Ainsi, on note $f \circ \mathcal{P}$ la fonction $G \mapsto f(G_{\mathcal{P}})$ avec $G_{\mathcal{P}}$ désignant la \mathcal{P} -partie de G et $\mathbb{N}_{\mathcal{P}}$ l'ensemble défini par :

$$\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N}, p|n \Rightarrow p \in \mathcal{P}\}.$$

On a :

Proposition IV.3.10 *Soit $\mathcal{P} \subset \mathbb{P}$ un ensemble de nombres premiers, on a :*

$$w_a^s(f \circ \mathcal{P}, n) = w_a^s(f, n_1)w_a^s(n_2) ,$$

où $n = n_1 n_2$ et n_1 est la \mathcal{P} -partie de n .

En particulier, il vient :

$$\zeta_a^s(f \circ \mathcal{P}, z) = \left(\sum_{n \in \mathbb{N}_{\mathcal{P}}} \frac{w_a^s(f, n)}{n^z} \right) \prod_{p \notin \mathcal{P}} \prod_{k=1}^a \frac{1}{1 - \left(\frac{1}{p}\right)^{2z+2k+1}} .$$

Nous donnons maintenant des exemples de moyennes. Pour des raisons de simplicité, nous prenons $a = \infty$.

Exemple 1. Soit $\alpha \in \mathbb{R}$ et $u > \alpha$. La u -moyenne de $|G|^\alpha$ est :

$$\frac{\zeta(2u - 2\alpha + 1)\zeta(2u - 2\alpha + 3) \cdots}{\zeta(2u + 1)\zeta(2u + 3) \cdots}.$$

En particulier, si $u \geq 2$, la u -moyenne de $|G|$ est : $\zeta(2u - 1)$.

Exemple 2. Soit L un \mathcal{P} -groupe de type S avec $|L| = \ell$. La u -probabilité pour que la \mathcal{P} -partie d'un groupe de type S soit isomorphe à L est :

$$\frac{\ell^{1-u}}{|\text{Aut}^s(L)|} \prod_{p \in \mathcal{P}} \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2u+2k-1}}\right).$$

Exemple 3. Supposons que l'on ait $p|n \Rightarrow p \in \mathcal{P}$. La u -probabilité pour que la \mathcal{P} -partie d'un groupe de type S soit de cardinal n est :

$$n^{1-u} w^s(n) \prod_{p \in \mathcal{P}} \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2u+2k-1}}\right).$$

Exemple 4. La u -probabilité pour que $G_p \neq \{0\}$ est :

$$1 - \prod_{k=1}^{\infty} \left(1 - (1/p)^{2u+2k-1}\right).$$

Exemple 5.

La u -probabilité pour que la \mathcal{P} -partie d'un groupe de type S soit isomorphe au carré d'un groupe cyclique est :

$$\prod_{p \in \mathcal{P}} \frac{1 - 1/p^2 + 1/p^{2u+3}}{(1 - 1/p^2)} \prod_{k=2}^{\infty} \left(1 - (1/p)^{2u+2k-1}\right).$$

En particulier si $\mathcal{P} = \mathbb{P}$ la probabilité est :

$$\prod_{p \in \mathbb{P}} (1 - 1/p^2 + 1/p^{2u+3}) \frac{\zeta(2)}{\zeta(2u+3)\zeta(2u+5)\zeta(2u+7) \cdots}.$$

Tous ces exemples proviennent directement des propositions IV.3.9 et IV.3.10, le dernier nécessitant un petit calcul.

On pose $f(G) = 1$ si, G est de la forme $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, et $f(G) = 0$ sinon. On a par la proposition IV.3.10 :

$$\zeta^s(f \circ \mathcal{P}, z) = \left(\sum_{n \in \mathbb{N}_{\mathcal{P}}} \frac{w^s(f, n)}{n^z} \right) \prod_{p \notin \mathcal{P}} \prod_{k=1}^{\infty} \frac{1}{1 - (1/p)^{2z+2k+1}}.$$

Le terme entre parenthèses donne :

$$\begin{aligned}
 \sum \frac{1}{n^{2z}} \sum_{G^s(n^2)} f(G) w^s(G) &= \sum \frac{1}{n^{2z}} \frac{1}{n^3} \prod_{p|n} (1 - 1/p^2) \\
 &\stackrel{(1)}{=} \prod_{p \in \mathcal{P}} \left(1 + \sum_{\nu=1}^{\infty} \frac{1}{p^{2\nu z} p^{3\nu} (1 - 1/p^2)} \right) \\
 &= \prod_{p \in \mathcal{P}} \left(1 + \frac{1}{1 - 1/p^2} \frac{1}{p^{2z+3}} \frac{1}{1 - (1/p)^{2z+3}} \right) \\
 &= \prod_{p \in \mathcal{P}} \frac{1 - 1/p^2 + 1/p^{2z+5}}{(1 - 1/p^2)(1 - 1/p^{2z+3})} .
 \end{aligned}$$

L'égalité (1) s'obtient par multiplicativité de la fonction. Pour conclure, on utilise la proposition IV.3.9 en faisant $z = u - 1$ (ou $z \rightarrow -1$).

IV.3.3 Moyennes sur les p -rangs

Nous obtenons ici des renseignements sur le p -rang des groupes de type S. Pour simplifier les calculs nous avons toujours pris $a = +\infty$ mais des résultats analogues peuvent être obtenus avec a fini. La première proposition est la suivante :

Proposition IV.3.11 *Soit α et r deux entiers positifs avec $r \leq \alpha$. On a :*

$$\sum_{G^s(p^{2\alpha}), r_p(G)=2r} w^s(G) = w^s(p^{2\alpha}) \frac{(1/p^2)_{\alpha-1} (1/p^2)_{\alpha}}{(1/p^2)_{r-1} (1/p^2)_r (1/p^2)_{\alpha-r}} p^{-2r^2+2r} .$$

Preuve : On utilise exactement la même idée que pour la proposition IV.3.3, avec la formule suivante, démontrée dans [Cohen-Lenstra] :

$$\sum_{G(p^{\alpha}), r_p(G)=r} w(G) = w(p^{\alpha}) \frac{(1/p)_{\alpha-1} (1/p)_{\alpha}}{(1/p)_{r-1} (1/p)_r (1/p)_{\alpha-r}} p^{-r^2+r} .$$

□

Corollaire IV.3.12 *Soit $n \in \mathbb{Z}$ avec $p^{\alpha} \parallel n$ alors :*

$$\sum_{G^s(n^2), r_p(G)=2r} w^s(G) = w^s(n^2) \frac{(1/p^2)_{\alpha-1} (1/p^2)_{\alpha}}{(1/p^2)_{r-1} (1/p^2)_r (1/p^2)_{\alpha-r}} p^{-2r^2+2r} .$$

Preuve : On écrit $n = p^{\alpha} n_2$ et on a :

$$\begin{aligned}
 \sum_{G^s(n^2), r_p(G)=2r} w^s(G) &= \sum_{H^s(n_2^2)} w^s(H) \sum_{G^s(p^{2\alpha}), r_p(G)=2r} w^s(G) \\
 &= w^s(n_2^2) \sum_{G^s(p^{2\alpha}), r_p(G)=2r} w^s(G)
 \end{aligned}$$

Puis on utilise la proposition IV.3.11. □

Finalement, nous pouvons montrer :

Proposition IV.3.13 *Soit r un entier positif, on a :*

$$\sum_{G^s(p, 2r)} \frac{w^s(G)}{|G|^z} = \frac{p^{-r(2r+2z+1)}}{(1/p^2)_r} \prod_{j=1}^r \frac{1}{1 - 1/p^{2z+2j+1}} ,$$

où la somme porte sur tous les p -groupes (G, β) de type S avec $r_p(G) = 2r$.

Preuve : On écrit :

$$\begin{aligned} \sum_{G^s(p, 2r)} \frac{w^s(G)}{|G|^z} &= \sum_{\alpha=0}^{\infty} \frac{1}{p^{2\alpha z}} \sum_{G(p^{2\alpha}), r_p(G)=2r} w^s(G) \\ &= \sum_{\alpha=r}^{\infty} \frac{1}{p^{2\alpha z}} w^s(p^{2\alpha}) p^{-2r^2+2r} \frac{(1/p^2)_{\alpha-1} (1/p^2)_{\alpha}}{(1/p^2)_{r-1} (1/p^2)_r (1/p^2)_{\alpha-r}} \\ &\stackrel{(1)}{=} \frac{p^{-2r^2}}{(1/p^2)_r} \sum_{\alpha=r}^{\infty} \frac{1}{p^{2\alpha z - 2r + 3\alpha}} \frac{(1/p^2)_{\alpha-1} (1/p^2)_{\alpha}}{(1/p^2)_{\alpha} (1/p^2)_{r-1} (1/p^2)_{\alpha-r}} \\ &= \frac{p^{-2r^2}}{(1/p^2)_r} \sum_{\beta=0}^{\infty} \frac{1}{p^{\beta(2z+3)+r(2z+1)}} \frac{(1/p^2)_{\beta+r-1}}{(1/p^2)_{\beta} (1/p^2)_{r-1}} \\ &= \frac{p^{-r(2r+2z+1)}}{(1/p^2)_r} \sum_{\beta=0}^{\infty} \frac{1}{p^{2\beta(z+3/2)}} \frac{(1/p^2)_{\beta+r-1}}{(1/p^2)_{\beta} (1/p^2)_{r-1}} \end{aligned}$$

L'égalité (1) provient de la proposition IV.3.1. Pour conclure, on utilise la proposition IV.3.3 avec $a = r - 1$. □

Nous obtenons alors facilement :

Exemple 6. La u -probabilité pour que le p -rang d'un groupe de type S soit $2r$ est :

$$\frac{p^{-r(2u+2r-1)}}{(1/p^2)_r} \prod_{k=r+1}^{\infty} (1 - 1/p^{2u+2k-1}) .$$

C'est immédiat avec la proposition précédente et les résultats sur la moyenne de la section précédente.

Enfin, nous avons le résultat suivant qui s'obtient avec les mêmes techniques que la proposition IV.3.11 avec la formule 6.4 de [Cohen-Lenstra] :

Proposition IV.3.14 Soit $\alpha \leq \beta$ deux entiers naturels, on a :

$$\sum_{G^s(p^{2\beta})} w^s(G) \prod_{0 \leq i < \alpha} (p^{r_p(G)} - p^{2i}) = \frac{w^s(p^{2\beta-2\alpha})}{p^\alpha} .$$

On déduit de cette proposition le corollaire suivant :

Corollaire IV.3.15 Soit n un entier positif avec $p^\alpha | n$, on a :

$$\sum_{G^s(n^2)} w^s(G) \prod_{0 \leq i < \alpha} (p^{r_p(G)} - p^{2i}) = \frac{w^s(n^2/p^{2\alpha})}{p^\alpha} .$$

Ce corollaire permet d'obtenir :

Exemple 7. La 0-moyenne de la fonction $p^{r_p(G)}$ est $1 + p$.

IV.4 L'assertion fondamentale

En utilisant l'analogie entre les unités des corps de nombres et les points rationnels des courbes elliptiques, on peut maintenant donner une heuristique à la "Cohen-Lenstra" sur les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q} , et déduire de cette heuristique et des résultats sur les groupes de type S, quelques conjectures sur les fréquences d'apparitions de certains groupes de Tate-Shafarevitch. Soit donc \mathcal{E}_u l'ensemble des classes d'isomorphismes des courbes elliptiques E de rang u définies sur \mathbb{Q} , que l'on suppose ordonné par le conducteur $N(E)$. Si f est une fonction définie sur les classes d'isomorphisme des groupes de type S, on pose :

$$\omega_u(f, x) = \sum_{E \in \mathcal{E}_u, N(E) \leq x} f(\text{III}(E)) , \quad \omega_u(x) = \sum_{E \in \mathcal{E}_u, N(E) \leq x} 1 .$$

On définit une moyenne sur f en posant :

$$M_u(f) = \lim_{x \rightarrow +\infty} \frac{\omega_u(f, x)}{\omega_u(x)} .$$

L'assertion heuristique fondamentale est la suivante :

$$M_u(f) = M_{u/2}^s(f) .$$

Remarque : Dans le cas du groupe des classes d'un corps de nombres, la 2-partie joue un rôle particulier. C'est pour cela que dans les conjectures originales de Cohen-Lenstra, il est nécessaire d'enlever cette 2-partie. Dans notre situation, il semble que nous n'ayons pas à appliquer de tels procédés.

Donnons quelques conséquences de cette assertion.

IV.4.1 Cas du rang 0

La probabilité pour que III soit isomorphe au carré d'un groupe cyclique est :

$$\prod_{p \in \mathbb{P}} (1 - 1/p^2 + 1/p^3) \frac{\zeta(2)}{\zeta(3)\zeta(5)\zeta(7)\dots} \sim 0.977076 .$$

La probabilité pour que $p \in \mathbb{P}$ divise $|\text{III}|$ est :

$$f_0(p) = 1 - \prod_{k=1}^{\infty} (1 - (1/p)^{2k-1}) .$$

En particulier :

$$\begin{aligned} f_0(2) &\simeq 0.580577 , \\ f_0(3) &\simeq 0.360995 , \\ f_0(5) &\simeq 0.206660 , \\ f_0(7) &\simeq 0.145408 . \end{aligned}$$

Le tableau suivant donne la probabilité pour que la p -partie de III soit isomorphe à un groupe G :

$p \backslash G$	$(\mathbb{Z}/p\mathbb{Z})^2$	$(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})^2$	$(\mathbb{Z}/p^2\mathbb{Z})^2$
2	0.387	0.0129	0.1935
3	0.1354	0.00056	0.045

La probabilité pour que $r_p(\text{III}) = 2r$ est :

$$\frac{p^{-r(2r-1)}}{(1/p^2)_r} \prod_{k=r+1}^{\infty} (1 - 1/p^{2k-1}) .$$

IV.4.2 Cas du rang 1

La probabilité pour que III soit le carré d'un groupe cyclique est :

$$\prod_{p \in \mathbb{P}} (1 - 1/p^2 + 1/p^4) \frac{\zeta(2)}{\zeta(4)\zeta(6)\zeta(8)\dots} \sim 0.99437; .$$

La probabilité pour que p divise $|\text{III}|$ est :

$$f_1(p) = 1 - \prod_{k=1}^{\infty} (1 - (1/p)^{2k}) .$$

En particulier :

$$\begin{aligned} f_1(2) &\simeq 0.311462 , \\ f_1(3) &\simeq 0.123439 , \\ f_1(5) &\simeq 0.041599 , \\ f_1(7) &\simeq 0.020824 . \end{aligned}$$

Soit L un groupe de type S, la probabilité pour que III soit isomorphe à L est :

$$\frac{\sqrt{|L|}}{|\text{Aut}^s(L)|} \frac{1}{\zeta(2)\zeta(4)\zeta(6)\cdots} .$$

En particulier $|\text{III}| = 1$ avec une probabilité d'environ 0.54914.

Une preuve de cette assertion heuristique ou de ses conséquences est bien sûr hors de portée. De plus, il est difficile de vérifier numériquement les valeurs prédites ici, car les groupes de Tate-Shafarevitch non-triviaux apparaissent plutôt pour des conducteurs élevés. Cependant, nous pouvons faire quelques remarques allant dans le sens de nos prédictions.

Tout d'abord, les résultats que nous donnons sont de natures différentes selon la parité du rang (dans le sens où ils impliquent des valeurs de la fonction zêta de Riemann aux entiers impairs ou pairs). Ceci semble naturel car les courbes elliptiques, elles aussi, sont classées en deux catégories selon le signe de l'équation fonctionnelle et donc selon la parité de leur rang, si l'on croit aux conjectures de Birch et Swinnerton-Dyer. Une conséquence de notre assertion est que le p -rang d'un groupe de Tate-Shafarevitch non trivial est souvent 2. Tous les groupes de Tate-Shafarevitch non triviaux des courbes elliptiques des tables de Cremona ont un p -rang égal à 2 ([Cremona-Mazur]).

On ne peut pas envisager de vérifier notre assertion en étudiant seulement des familles de courbes elliptiques car le comportement d'une famille spécifique peut être totalement différent du comportement global. Il peut néanmoins subsister des traces de quelques phénomènes. En particulier, notre assertion implique que pour un groupe de type S donné, la fréquence d'apparition des groupes de Tate-Shafarevitch isomorphes à ce groupe est nulle dans le cas des courbes de rang 0 et est strictement positive pour les courbes de rang ≥ 1 .

En étudiant la famille de courbes elliptiques $x^3 + y^3 = m$ dans le cas du rang 0, Zagier et Kramarz (cf. [Zagier-Kramarz]) suggèrent que la fréquence d'apparitions des groupes de Tate-Shafarevitch isomorphes à un groupe fixé pourrait être nulle.

Dans le cas du rang 1, on calcule dans [Delaunay-Duquesne] l'ordre "analytique" des groupes de Tate-Shafarevitch d'un nombre important de courbes elliptiques associées aux "simplest cubic fields". Pour les premiers carrés n^2 ($n = 1, 2, 3, 5$), il semble y avoir une densité positive des groupes de Tate-Shafarevich d'ordres n^2 . Cette densité ne correspond

pas aux valeurs prédites ici, mais encore une fois, il ne s'agit là que d'une famille de courbes elliptiques.

Chapitre V

Vérification numérique des conjectures de Deligne

Lorsque nous avons calculé le degré modulaire d’une courbe elliptique E , nous avons utilisé, dans la partie II.3, le carré symétrique de la série L de la forme modulaire associée à E . Ceci s’inscrit, en fait, dans un cadre plus général, où l’on définit des puissances symétriques de tout ordre d’une série L provenant d’une forme modulaire. On conjecture que ces nouvelles séries L se prolongent à tout le plan complexe en des fonctions entières et qu’elles vérifient des équations fonctionnelles classiques. Une conjecture, principalement due à Deligne, affirme que les valeurs de ces puissances symétriques aux “points critiques” ne dépendent, à un nombre rationnel près, que de deux nombres, c_+ et c_- , naturellement attachés à la forme f initialement considérée. Dans ce chapitre, on se propose de vérifier numériquement ces conjectures sur un certain nombre d’exemples.

V.1 Séries L et puissances symétriques

V.1.1 Définition et propriétés

Bien que l’on puisse définir la notion de puissances symétriques dans le vaste contexte des représentations cuspidales de dimension 2, nous ne considérerons ici que le cadre provenant des formes modulaires classiques. Soit f une newform normalisée de poids k sur $\Gamma_0(N)$ et de caractère trivial. On remarque que k est pair. On écrit le développement de Fourier de f à l’infini :

$$f(\tau) = \sum_{n \geq 1} a(n)q^n .$$

Nous supposons en outre que $a(n) \in \mathbb{Z}$ pour tout n . La série L de f est donnée par :

$$L(f, s) = \sum_{n \geq 1} \frac{a(n)}{n^s} \quad \Re(s) > \frac{k+1}{2} ,$$

et se décompose en un produit de facteurs Eulériens :

$$\begin{aligned}
 L(f, s) &= \prod_p L_p(f, p^{-s})^{-1} \\
 &= \prod_{p \nmid N} (1 - a(p)p^{-s} + p^{k-1}p^{-2s})^{-1} \prod_{p \mid N} (1 - a(p)p^{-s})^{-1} \\
 &= \prod_p (1 - \alpha(p)p^{-s})^{-1} (1 - \beta(p)p^{-s})^{-1} ,
 \end{aligned}$$

où :

$$\begin{cases} \alpha(p) + \beta(p) &= a(p) \\ |\alpha(p)| &= p^{(k-1)/2} & \text{si } p \nmid N \\ \beta(p) &= 0 & \text{si } p \mid N \end{cases} .$$

On peut alors définir la puissance symétrique m -ième de $L(f, s)$ en posant :

$$L(\text{Sym}^m(f), s) = \prod_p L_p(\text{Sym}^m(f), p^{-s})^{-1} , \quad (\text{V.1})$$

où pour tout p premier ne divisant pas N on a :

$$L_p(\text{Sym}^m(f), X) = \prod_{i=0}^m (1 - \alpha(p)^i \beta(p)^{m-i} X) . \quad (\text{V.2})$$

Les bornes $|\alpha(p)| = p^{(k-1)/2}$ entraînent que la série de Dirichlet (V.1) converge pour $\Re(s) > 1 + m \frac{k-1}{2}$. En particulier, pour tout s appartenant à ce demi-plan de convergence, on a :

$$L(\text{Sym}^m(f), s) \neq 0 .$$

Ces fonctions L jouent un rôle important en théorie des nombres et proviennent en fait d'objets arithmétiques naturels ([Deligne], [Shahidi 1]). On s'attend à ce qu'elles satisfassent certaines propriétés, notamment on espère pouvoir les prolonger et qu'elles vérifient une équation fonctionnelle. On peut même donner la forme de l'équation fonctionnelle (cf. [Serre 2]). Pour cela, posons :

$$\begin{aligned}
 \widetilde{\gamma}_m(s) &= (2\pi)^{-rs} \prod_{j=0}^{r-1} \Gamma(s - j(k-1)) & \text{si } m = 2r - 1 . \\
 \widetilde{\gamma}_m(s) &= (2\pi)^{-rs} \pi^{-s/2} \prod_{j=0}^{r-1} \Gamma(s - j(k-1)) \Gamma\left(\frac{s}{2} - \left\lfloor \frac{r(k-1)}{2} \right\rfloor\right) & \text{si } m = 2r .
 \end{aligned}$$

On fait la conjecture suivante :

Conjecture V.1.1 *Il existe un entier $B \in \mathbb{N}$ et pour tout $p|N$, il existe un facteur local $L_p(\text{Sym}^m(f), X)$ tels que la série $L(\text{Sym}^m(f), s)$ se prolonge méromorphiquement à tout le plan complexe et vérifie l'équation fonctionnelle :*

$$\Lambda(\text{Sym}^m(f), s) = \pm \Lambda(\text{Sym}^m(f), (k-1)m+1-s) ,$$

où

$$\Lambda(\text{Sym}^m(f), s) = B^{\frac{sm}{2}} \widetilde{\gamma}_m(s) L(\text{Sym}^m(f), s) .$$

Dans la suite, nous noterons $\gamma_m(s)$ la fonction $B^{sm/2} \widetilde{\gamma}_m(s)$. Le développement en produit de facteurs Eulériens de $L(\text{Sym}^m(f), s)$ permet d'obtenir les coefficients de cette série de Dirichlet, on écrit :

$$L(\text{Sym}^m(f), s) = \sum_{n \geq 1} \frac{b(n)}{n^s} .$$

Remarques : 1) Comme nous l'avons mentionné plus haut, on peut définir des puissances symétriques de séries L dans un contexte beaucoup plus général. On peut trouver dans la littérature de nombreuses conjectures reliées à ces fonctions incluant celle que nous venons de donner ([Shahidi 1], [Shahidi 2]).

3) Pour $m = 1$, on a simplement $L(\text{Sym}^1(f), s) = L(f, s)$ et $B = N$. L'équation fonctionnelle est alors un fait classique sur ces séries de Dirichlet.

4) Pour $m = 2$, il s'agit du carré symétrique et la conjecture V.1.1 a été établie dans un cadre très général ([Ogg], [Shahidi 2]). Dans la partie II.3, nous avons utilisé les propriétés de ce carré symétrique dans le cas des formes de poids 2.

5) D'autres résultats importants sont connus pour les premières puissances symétriques d'ordres supérieures (cf. [Shahidi 2]).

Afin de pouvoir évaluer la fonction $L(\text{Sym}^m(f), s)$, nous allons utiliser cette équation fonctionnelle. Nous admettons donc dans toute la suite, la validité de la conjecture V.1.1, sans chercher à différencier les résultats établis de ceux qui ne le sont pas encore.

V.1.2 Conjectures de Deligne

Soit $L(s) = \sum_n c(n)n^{-s}$ une série L motivique (i.e. provenant d'un objet mathématique "naturel" comme un corps de nombres, une forme modulaire, etc...) et satisfaisant une équation fonctionnelle de type classique :

$$\gamma(s) L(s) = \gamma(K-s) L(K-s) ,$$

où la fonction $\gamma(s)$ est un produit de facteurs gammas. Deligne ([Deligne]) définit un point critique pour $L(s)$ comme étant un entier $q \in \mathbb{Z}$ tel que ni la fonction $\gamma(s)$ ni la fonction $\gamma(K-s)$ n'ont de pôle en $s = q$.

Exemple : Prenons pour $L(s)$ la série $L(f, s)$ de la forme modulaire de poids k que nous avons fixée dans la partie précédente. Les points critiques de $L(f, s)$ sont les entiers :

$$q = 1, 2, \dots, k-1 .$$

Les points critiques de $L(\text{Sym}^2(f), s)$ sont les entiers :

$$\begin{aligned} q &= 1, 3, \dots, k-1 \\ \text{et} \quad q &= k, k+2, \dots, 2(k-1) . \end{aligned}$$

Plus généralement, grâce à la conjecture V.1.1, on peut voir que les points critiques de $L(\text{Sym}^m(f), s)$ sont les entiers q tels que :

– Si $m = 2r - 1$ est impair :

$$(r-1)(k-1) + 1 \leq q \leq r(k-1) .$$

– Si $m = 2r$ est pair :

$$\begin{cases} r(k-1) + 1 \leq q \leq (r+1)(k-1) & \text{et } q \text{ est pair} \\ (r-1)(k-1) + 1 \leq q \leq r(k-1) & \text{et } q \text{ est impair} . \end{cases}$$

La philosophie générale de Deligne dans [Deligne] prédit alors que la valeur de la fonction $L(s)$ en un point critique q est de la forme $a c(q)$ où a est un nombre algébrique et $c(q)$ une “période” (la valeur d’une certaine intégrale). C’est exactement ce qui se produit, par exemple, pour la fonction ζ de Riemann ; les points critiques sont les entiers pairs positifs et les entiers impairs négatifs. Il est bien connu que $\zeta(q)$ est rationnel pour $q \leq 0$ impair et que $\zeta(q)$ est un multiple rationnel de π^q pour $q > 0$ pair. Dans le cadre qui nous intéresse, la théorie de Deligne permet de définir deux nombres c_+ et c_- attachés à la forme modulaire f (en fait, ces deux nombres sont seulement définis à un rationnel près) et de conjecturer que la valeur de $L(\text{Sym}^m(f), s)$ en un point critique s’exprime à l’aide d’un nombre rationnel et de puissances convenables de c_+ , c_- et π . Dans la suite, on écrira $= (*)$ pour signifier “égal à un rationnel près”. La conjecture précise de Deligne ([Deligne]) est :

Conjecture V.1.2 *Si q est un point critique de $L(\text{Sym}^m(f), s)$ alors :*

– Si $m = 2r - 1$ est impair :

$$L(\text{Sym}^m(f), q) = (*) \begin{cases} (2\pi)^{rq - \frac{r(r-1)}{2}(k-1)} c_+^{\frac{r(r+1)}{2}} c_-^{\frac{r(r-1)}{2}} & \text{si } q \text{ est pair} \\ (2\pi)^{rq - \frac{r(r-1)}{2}(k-1)} c_+^{\frac{r(r-1)}{2}} c_-^{\frac{r(r+1)}{2}} & \text{si } q \text{ est impair} . \end{cases}$$

– Si $m = 2r$ est pair :

$$L(\text{Sym}^m(f), q) = (*) \begin{cases} (2\pi)^{(r+1)q - \frac{r(r+1)}{2}(k-1)} (c_+ c_-)^{\frac{r(r+1)}{2}} & \text{si } q \text{ est pair} \\ (2\pi)^{rq - \frac{r(r-1)}{2}(k-1)} (c_+ c_-)^{\frac{r(r+1)}{2}} & \text{si } q \text{ est impair} . \end{cases}$$

Pour $m = 1$, la conjecture de Deligne est un résultat connu que l'on obtient en étudiant les périodes de f i.e. les intégrales d'Eichler :

$$r_l(f) = i^l \int_0^{i\infty} f(\tau) \tau^l d\tau \quad \text{pour } l = 0, 1, \dots, k-2 .$$

Il n'est pas difficile d'écrire $r_l(f)$ en fonction de $L(f, l+1)$. Les travaux d'Eichler de Shimura et de Manin montrent alors que l'on peut trouver deux nombres c_+ et c_- tels que :

$$\begin{aligned} L(f, q) &= (*) (2\pi)^q c_+ & \text{si } q \text{ est pair} , \\ L(f, q) &= (*) (2\pi)^q c_- & \text{si } q \text{ est impair} . \end{aligned}$$

De plus, le produit $c_+ c_-$ est, à un rationnel près, le carré de la norme de f au sens de Petersson.

Pour $m = 2$, la méthode de Rankin permet d'obtenir :

$$\|f\|^2 = \frac{N}{2^{2k-1} \pi^{k+1}} \Gamma(k) L(\text{Sym}^2(f), k) ,$$

si N est sans facteur carré (sinon l'égalité précédente a lieu à un rationnel près, ce qui ne modifie en rien le raisonnement puisque tout se passe "à un rationnel près"). Comme $c_+ c_- = (*) \|f\|^2$, on obtient :

$$L(\text{Sym}^2(f), k) = (*) (2\pi)^{k+1} c_+ c_- .$$

Ce qui est exactement l'expression de la conjecture V.1.2 pour $m = 2$ et $q = k$. Cela montre que $L(\text{Sym}^2(f), k) \neq 0$. C'est un cas particulier d'une conjecture générale qui prédit que $L(\text{Sym}^m(f), s) \neq 0$ sur la droite $\Re(s) = 1 + m \frac{k-1}{2}$.

V.2 Vérification Numérique des conjectures de Deligne

V.2.1 Détermination de la série L

Pour vérifier les conjectures de Deligne, nous devons évaluer la fonction $\Lambda(\text{Sym}^m(f), s)$ aux points critiques. Comme cette fonction vérifie une équation fonctionnelle classique, nous pouvons appliquer, comme dans la partie II.3, la méthode décrite dans [Cohen 2]. En suivant ce procédé, on a :

$$\Lambda(\text{Sym}^m(f), s) = \sum_{n \geq 1} \frac{b(n)}{n^s} F(s, nt_0) + w \sum_{n \geq 1} \frac{b(n)}{n^{K-s}} F(K-s, \frac{n}{t_0}) , \quad (\text{V.3})$$

où :

- t_0 est un nombre réel strictement positif (la meilleure valeur de t_0 pour les calculs est donnée par $t_0 = 1$).
- $w = \pm 1$ est le signe de l'équation fonctionnelle.
- $K = (k-1)m + 1$ est le point de symétrie de l'équation fonctionnelle.
- $F(s, x)$ est définie par :

$$F(s, x) = \gamma_m(s) - \int_0^x \frac{1}{2i\pi} \int_{\Re(z)=\delta} t^{-z} \gamma_m(z) dz t^{s-1} dt .$$

La formule (V.3) est une série rapidement convergente, pratique pour évaluer la fonction $\Lambda(\text{Sym}^m(f), s)$ en $s \in \mathbb{C}$. Pour calculer $F(s, x)$, on déplace, dans l'intégrale :

$$W(t) = \frac{1}{2i\pi} \int_{\Re(z)=\delta} t^{-z} \gamma_m(z) dz ,$$

la droite d'intégration vers la gauche pour faire apparaître les contributions des résidus de la fonctions $t^{-z} \gamma_m(z)$. En effet, on peut voir que :

$$W(t) = \sum_a \text{res}_{z=a}(t^{-z} \gamma_m(z)) .$$

Posons $m = 2r - 1 + \varepsilon$ ($\varepsilon = 0$ ou 1 suivant que l'on prend une puissance impaire ou paire). Pour obtenir les résidus de la fonction $t^{-z} \gamma_m(z)$, on écrit :

$$\prod_{j=0}^{r-1} \Gamma(z - j(k-1)) = \Gamma(z)^r \prod_{i=1}^{(r-1)(k-1)} \frac{1}{(z-i)^{\lceil \frac{i}{k-1} \rceil}} ,$$

$$\Gamma\left(\frac{z}{2} - \ell\right) = 2^\ell \Gamma\left(\frac{z}{2}\right) \prod_{i=1}^{\ell} \frac{1}{z-2i} ,$$

dans l'expression définissant $\widetilde{\gamma}_m(z)$. Puis, on utilise l'égalité :

$$\log(\Gamma(1+X)) = \sum_{n \geq 1} \frac{(-1)^n}{n} \zeta(n) X^n \quad (\text{où par convention, } \zeta(1) = \gamma = 0.5772 \dots) ,$$

pour déterminer le développement en série de Laurent de la fonction $\Gamma(z)^r \Gamma(z/2)^\varepsilon$. On obtient alors le développement de la fonction $\gamma_m(z)$ puis les résidus de $t^{-z} \gamma_m(z)$. On en déduit enfin une valeur numérique pour $F(s, x)$ par la formule :

$$F(s, x) = \gamma_m(s) - \sum_a \int_0^x \text{res}_{z=a}(t^{-z} \gamma_m(z)) t^{s-1} dt .$$

Cette méthode est rapide pour calculer $F(s, x)$; cependant il faut se méfier des problèmes numériques qui peuvent se produire lorsque x devient grand.

Pour calculer $\Lambda(\text{Sym}^m(f), s)$, il nous faut au préalable trouver les bons facteurs locaux, $L_p(\text{Sym}^m(f), X)$ pour $p \mid N$, le nombre B de la conjecture V.1.1 et le signe de w l'équation fonctionnelle. Un moyen systématique pour faire ceci, pourrait être de considérer :

- Tous les facteurs Eulériens $L_p(\text{Sym}^m(f), X)$ pour $p \mid N$ possibles (ils doivent être des polynômes de degrés $\leq m + 1$ à coefficients entiers).
- Tous les diviseurs B de N .
- Tous les w possibles pour le signe de l'équation fonctionnelle (i.e. $w = 1$ ou $w = -1$).

On se fixe alors un choix de $L(\text{Sym}^m(f), s)$, de B et de w . Ensuite, on évalue, en utilisant la série (V.3), la fonction $\Lambda(\text{Sym}^m(f), s)$ en un point du plan complexe et en prenant deux valeurs distinctes pour t_0 . Si les calculs obtenus pour $\Lambda(\text{Sym}^m(f), s)$ sont différents (à la précision des calculs) alors le choix que nous avons fait est sûrement mauvais. On recommence le procédé en faisant un autre choix (d'après [Serre] il n'y a qu'un nombre fini de facteurs Eulériens possibles). On voit ainsi comment l'on peut obtenir toutes les constantes de l'équation fonctionnelle. Bien sûr, toutes ces valeurs ainsi obtenues sont conjecturales, mais de toute façon le prolongement et l'équation fonctionnelle de $L(\text{Sym}^m(f), s)$ le sont déjà...

En principe, le cas de N sans facteur carré devrait être plus simple à traiter. Par exemple, pour le carré symétrique et N sans facteur carré, on peut montrer ([Ogg]) que tous les facteurs Eulériens sont donnés par la formule (V.2) (même les facteurs locaux aux nombres premiers divisant N), que $B = N$, et que le signe de l'équation fonctionnelle est toujours positif.

C'est essentiellement pour cette raison que nous n'avons considéré dans nos exemples que des conducteurs sans facteurs carrés. Les calculs que nous avons faits nous conduisent à constater, dans ce cas, que les faits suivants semblent se produire de façon systématique (du moins pour les premières puissances que nous avons traitées) :

- Le nombre B intervenant dans l'équation fonctionnelle de la conjecture V.1.1 est égal à N .
- Pour tout p premier, le facteur local $L_p(\text{Sym}^m(f), X)$ est donné par la formule V.2.
- Le signe w de l'équation fonctionnelle ne dépend que de m et du signe de l'équation fonctionnelle de $L(f, s)$. En particulier, $w = 1$ lorsque m est pair.

Nous ne chercherons pas à montrer ces faits. Nous vérifions simplement qu'ils sont bien conformes aux résultats numériques obtenus. Une vérification supplémentaire est faite en constatant que l'on obtient bien un nombre qui semble être rationnel dans les conjectures de Deligne.

V.2.2 Normalisation de c_+ et c_-

Pour vérifier les conjectures de Deligne, il faut définir les périodes c_+ et c_- . Comme tout se passe “à un rationnel près”, le choix que nous allons faire sera de toute façon plus ou moins arbitraire. Cependant, un “mauvais” choix risque de rendre les calculs encore plus compliqués. Il nous faut trouver une normalisation qui permette de vérifier la conjecture V.1.2 le plus facilement possible.

Prenons l'exemple de la forme modulaire de poids 4 sur $\Gamma_0(5)$ ayant des coefficients $a(n)$

entiers :

$$f(\tau) = q - 4q^2 + 2q^3 + 8q^4 - 5q^5 + \dots$$

Si on prend $c_+ = L(f, 2)/(2\pi)^2$ et $c_- = L(f, 3)/(2\pi)^3$, alors certes,

$$\begin{aligned} \frac{L(\text{Sym}^2(f), 4)}{(2\pi)^5(c_+c_-)} &\approx 4.333333333333333333 \approx \frac{13}{3}, \\ \frac{L(\text{Sym}^2(f), 6)}{(2\pi)^9(c_+c_-)} &\approx 0.0026666666666666666 \approx \frac{1}{375}, \end{aligned}$$

sont faciles à reconnaître en tant que nombres rationnels, mais il est plus difficile d'en faire autant pour :

$$\begin{aligned} \frac{L(\text{Sym}^6(f), 10)}{(2\pi)^{22}(c_+c_-)^6} &\approx 4842888904.56594160297864 \approx \frac{24713262080000}{5103}, \\ \frac{L(\text{Sym}^6(f), 12)}{(2\pi)^{30}(c_+c_-)^6} &\approx 2663.91594974897882834390 \approx \frac{5451745614848}{2046515625}. \end{aligned}$$

Il faut donc faire attention aux choix des périodes c_+ et c_- mais aussi à la normalisation de la série $L(\text{Sym}^m(f), s)$. En effet, on remarque qu'en utilisant directement les valeurs de $L(\text{Sym}^m(f), q)$ pour vérifier la conjecture V.1.2, il apparaît de gros dénominateurs qui proviennent des facteurs gammas lorsqu'on a divisé $\Lambda(\text{Sym}^m(f), q)$ par $\gamma_m(q)$. On préfère donc travailler sur la fonction complétée elle-même et reformuler pour cela la conjecture de Deligne. On pose $r = \lceil m/2 \rceil$. Si q est un point critique pour $L(\text{Sym}^m(f), s)$, la conjecture V.1.2 est équivalente à :

$$\Lambda(\text{Sym}^m(f), q) = (*) \left(\frac{c_+c_-}{\pi^{k-1}} \right)^{\frac{r(r-1)}{2}} B^{\frac{mq}{2}} \begin{cases} c_{\pm}^r & \text{pour } m \text{ impair et } (-1)^q = \pm 1. \\ (c_+c_-)^r (\sqrt{\pi})^{-q} & \text{pour } m \text{ pair et } (-1)^q = 1. \\ \left(\frac{c_+c_-}{\pi^{k-1}} \right)^r (2\sqrt{\pi})^q & \text{pour } m \text{ pair et } (-1)^q = -1. \end{cases} \quad (\text{V.4})$$

C'est cette formule que nous vérifions en divisant la valeur de $\Lambda(\text{Sym}^m(f), q)$ par le membre de droite de la formule (V.4) et en constatant que le nombre ainsi obtenu et noté $\sigma(f, m, q)$ semble être un rationnel convenable.

On normalisera toujours le choix de c_+ et c_- afin d'avoir :

$$c_+c_- = \frac{\Lambda(\text{Sym}^2(f), 2k-2)}{(2N)^{2k-2}}.$$

Et pour c_- , on prend :

$$c_- = \frac{\Lambda(f, k-1)}{N^{(k-1)/2}},$$

s'il est non nul. S'il est nul, alors $k = 2$ et f est associée à une courbe elliptique E définie sur \mathbb{Q} ; on prendra alors $c_- = \Omega/(2\pi)$, où Ω est la période réelle de E .

Notons de plus, que l'équation fonctionnelle nous permet de ne vérifier la formule (V.4) que pour la moitié des points critiques.

Lorsque $\sigma(f, m, q)$ possède un grand dénominateur et que la précision n'est pas assez élevée, il est difficile de déterminer le nombre rationnel caché derrière. Le dénominateur en question peut provenir du choix de notre normalisation pour c_+ et c_- . Dans ce cas, pour le simplifier, on divise $\sigma(f, m, q)$ par un des nombres $\sigma(f, 1, q')$ avec q' pair. En principe, on obtient un nombre plus simple à reconnaître.

V.2.3 Exemple

Prenons la forme modulaire f de poids 2 sur $\Gamma_0(11)$ associée à la courbe elliptique d'équation :

$$y^2 + y = x^3 - x^2 - 10x - 20 .$$

Les calculs donnent :

$$\begin{aligned} c_+ &\approx 0.052767699011444883083799947381425072667974 \\ c_- &\approx 0.040400186918863279214419198537327720301074 \end{aligned}$$

Les valeurs obtenues pour $\sigma(f, m, q)$ semblent toutes correspondre à des nombres rationnels donnés dans le tableau suivant :

Puissance 1 : • signe : 1 • $\sigma(f, 1, 1) = 1$	Puissance 2 : • signe : 1 • $\sigma(f, 2, 2) = 1$	Puissance 3 : • signe : 1 • $\sigma(f, 3, 2) = 2^4 \times 5^{-1} \times 11^2$
Puissance 4 : • signe : 1 Pas de valeur critique	Puissance 5 : • signe : -1 • $\sigma(f, 5, 3) = 0$	Puissance 6 : • signe : 1 • $\sigma(f, 6, 4) = 2^6 \times 3 \times 5^7$
Puissance 7 : • signe : -1 • $\sigma(f, 7, 4) = 0$	Puissance 8 : • signe : 1 Pas de valeur critique	Puissance 9 : (*) • signe : 1 • $\sigma(f, 9, 5) \stackrel{?}{=} 2^{18} \times 3^2 \times 5^{21}$

Insistons sur le fait que ces égalités sont seulement numériques et ne sont pas démontrées (malgré le symbole “=”). Nous avons fait les calculs en utilisant les 10^6 premiers coefficients de Fourier de f et les valeurs que nous obtenons sont suffisamment précises pour se convaincre des résultats (avec toute la réserve qu'il faut y donner). Cependant, pour $m = 9$, on trouve :

$$\sigma(f, 9, 5) = 1124.999999999991227663421435 \dots \times 10^{18} ,$$

et nous en avons déduit la valeur 1125×10^{18} du tableau. Ceci manque clairement de précision d'où le symbole $\stackrel{?}{=}$.

V.2.4 “Grandes” puissances symétriques

Pour vérifier numériquement la conjecture de Deligne pour les “grandes” puissances symétriques (disons $m \geq 5, 6$), il faut connaître beaucoup de termes dans le développement de Fourier de la forme modulaire f . Malheureusement, les calculs de ces coefficients prennent trop de temps. Lorsque f provient d’une courbe elliptique définie sur \mathbb{Q} , les algorithmes classiques pour déterminer le nombre de points sur $E(\mathbb{F}_p)$, pour p premier, sont rapides et nous permettent d’obtenir un nombre important de coefficients de f . C’est pour cela que nous avons pu aller assez loin dans l’exemple précédent.

Lorsque $k \geq 4$, il arrive, quelquefois, que la forme modulaire f s’exprime simplement à l’aide de la fonction η de Dedekind et de ses puissances :

$$\eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n) .$$

Les coefficients de η et η^3 sont faciles à obtenir grâce à l’identité triple de Jacobi. Nous avons :

Proposition V.2.1

$$\begin{aligned} \eta(\tau) &= q^{1/24} \left(1 + \sum_{n \geq 1} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2}) \right) , \\ \eta^3(\tau) &= q^{1/8} \sum_{n \geq 0} (-1)^n (2n+1) q^{n(n+1)/2} . \end{aligned}$$

1 Poids 4

Prenons $f = q - 4q^2 + 2q^3 + 8q^4 + \dots$ la forme modulaire de poids 4 sur $\Gamma_0(5)$ à coefficients entiers. On a :

$$f(\tau) = \eta(\tau)^4 \eta(5\tau)^4 ,$$

et les séries lacunaires de la proposition V.2.1 nous permettent de calculer un nombre important de coefficients pour f . On peut donc évaluer numériquement les fonctions $\Lambda(\text{Sym}^m(f), s)$ et donner les résultats obtenus (avec 3×10^5 coefficients).

Puissance : 1 • signe : +1 $\sigma(f, 1, 2) = 2^1 \cdot 5^2$ $\sigma(f, 1, 3) = 1$	Puissance : 2 • signe : +1 $\sigma(f, 2, 4) = 2^{-2} \cdot 5^2 \cdot 13^1$ $\sigma(f, 2, 6) = 1$	Puissance : 3 • signe : -1 $\sigma(f, 3, 5) = 0$ $\sigma(f, 3, 6) = 2^5 \cdot 5^7 \cdot 13^1$
Puissance : 4 • signe : +1 $\sigma(f, 4, 8) = 2^1 \cdot 5^5 \cdot 13^4$	Puissance : 5 • signe : -1 $\sigma(f, 5, 8) = 0$ $\sigma(f, 5, 9) = 2^5 \cdot 3^1 \cdot 5^9 \cdot 13^6$	Puissance : 6 • signe : +1 $\sigma(f, 6, 10) = 2^7 \cdot 3^1 \cdot 5^{18} \cdot 13^6$ $\sigma(f, 6, 12) = 2^{10} \cdot 3^2 \cdot 5^{10} \cdot 13^6 \cdot 1103^1$
Puissance : 7 • signe : +1 $\sigma(f, 7, 11) = 2^{13} \cdot 3^1 \cdot 5^{20} \cdot 7^1 \cdot 13^{10}$ $\sigma(f, 7, 12) = 2^{18} \cdot 3^1 \cdot 5^{27} \cdot 13^6 \cdot 15817^1$	Puissance : 8 • signe : +1 $\sigma(f, 8, 14) \stackrel{?}{=} 2^{13} \cdot 3^1 \cdot 5^{25} \cdot 13^{10} \cdot 313^1 \cdot 62039^1$	

Pour la puissance 8-ième, on obtient seulement

$$\sigma(f, 8, 14)/\sigma(f, 1, 2)^{10} \approx 200772354857377105724999.999340238 \dots ,$$

la valeur donnée dans le tableau est donc à prendre avec beaucoup de précautions!! Pour les “grandes” puissances, nous avons souvent utilisé ce procédé approximatif. A partir de maintenant, nous omettrons de le signaler et n’écrirons plus ce symbole \approx .

2 Poids 6

Prenons $f = q - 6q^2 + 9q^3 + \dots$ la forme modulaire de poids 6 sur $\Gamma_0(3)$ à coefficients entiers. Dans ce cas, on a :

$$f(\tau) = \eta(\tau)^6 \eta(3\tau)^6 .$$

Puissance : 1 • signe : +1 $\sigma(f, 1, 3) = 2^{-1} \cdot 3^{-1} \cdot 13^1$ $\sigma(f, 1, 4) = 3^5$ $\sigma(f, 1, 5) = 1$	Puissance : 2 • signe : +1 $\sigma(f, 2, 6) = 2^{-3} \cdot 3^5 \cdot 13^1$ $\sigma(f, 2, 8) = 2^{-5} \cdot 3^3 \cdot 13^1$ $\sigma(f, 2, 10) = 1$	Puissance : 3 • signe : +1 $\sigma(f, 3, 8) = 2^5 \cdot 3^{19} \cdot 13^1$ $\sigma(f, 3, 9) = 3^7 \cdot 13^3$ $\sigma(f, 3, 10) = 2^6 \cdot 3^{17} \cdot 13^1$
Puissance : 4 • signe : +1 $\sigma(f, 4, 12) = 3^{18} \cdot 13^3$ $\sigma(f, 4, 14) = 2^{-2} \cdot 3^{13} \cdot 7^1 \cdot 13^3 \cdot 23^1$	Puissance : 5 • signe : -1 $\sigma(f, 5, 13) = 0$ $\sigma(f, 5, 14) = 2^{13} \cdot 3^{41} \cdot 13^3$ $\sigma(f, 5, 15) = 2^4 \cdot 3^{21} \cdot 5^1 \cdot 13^6 \cdot 53^1$	Puissance : 6 • signe : +1 $\sigma(f, 6, 16) = 2^1 \cdot 3^{46} \cdot 7^2 \cdot 13^6$ $\sigma(f, 6, 18) = 2^2 \cdot 3^{38} \cdot 5^1 \cdot 13^7 \cdot 773^1$ $\sigma(f, 6, 20) = 2^3 \cdot 3^{33} \cdot 13^6 \cdot 947^1 \cdot 21863^1$
Puissance : 7 • signe : -1 $\sigma(f, 7, 18) = 0$ $\sigma(f, 7, 19) = 2^9 \cdot 3^{51} \cdot 5^1 \cdot 13^{10} \cdot 19^1 \cdot 23^1$ $\sigma(f, 7, 20) = 2^{20} \cdot 3^{69} \cdot 5^1 \cdot 13^6 \cdot 110069^1$	Puissance : 8 • signe : +1 $\sigma(f, 8, 22) = 2^8 \cdot 3^{77} \cdot 5^1 \cdot 13^{10} \cdot 604697^1$ $\sigma(f, 8, 24) = 2^7 \cdot 3^{64} \cdot 5^1 \cdot 7^1 \cdot 13^{10} \cdot 1216387^1 \cdot 2773721^1$	

(Résultats obtenus avec 3×10^5 coefficients de f).

3 Poids 8

Prenons $f = q - 8q^2 + 12q^3 + \dots$ la forme modulaire de poids 8 sur $\Gamma_0(2)$ à coefficients entiers. Dans ce cas, on a :

$$f(\tau) = \eta(\tau)^8 \eta(2\tau)^8 .$$

Puissance : 1 • signe : +1 $\sigma(f, 1, 4) = 2^{13} \cdot 3^{-2}$ $\sigma(f, 1, 5) = 3^{-1} \cdot 5^{-1} \cdot 17^1$ $\sigma(f, 1, 6) = 2^{14} \cdot 3^{-3}$ $\sigma(f, 1, 7) = 1$	Puissance : 2 • signe : +1 $\sigma(f, 2, 8) = 2^8 \cdot 3^{-2} \cdot 17^1$ $\sigma(f, 2, 10) = 2^6 \cdot 3^{-2} \cdot 5^{-1} \cdot 17^1$ $\sigma(f, 2, 12) = 2^4 \cdot 3^{-4} \cdot 17^1$ $\sigma(f, 2, 14) = 1$	Puissance : 3 • signe : -1 $\sigma(f, 3, 11) = 0$ $\sigma(f, 3, 12) = 2^{16} \cdot 3^2 \cdot 17^1$ $\sigma(f, 3, 13) = 2^{15} \cdot 3^{-2} \cdot 17^3$ $\sigma(f, 3, 14) = 2^{42} \cdot 3^{-3} \cdot 5^1 \cdot 17^1$
Puissance : 4 • signe : +1 $\sigma(f, 4, 16) = 2^{36} \cdot 3^{-3} \cdot 5^1 \cdot 17^3$ $\sigma(f, 4, 18) = 2^{32} \cdot 3^{-4} \cdot 5^1 \cdot 17^4$ $\sigma(f, 4, 20) = 2^{28} \cdot 3^{-4} \cdot 5^{-1} \cdot 17^3 \cdot 9781^1$	Puissance : 5 • signe : -1 $\sigma(f, 5, 18) = 0$ $\sigma(f, 5, 19) = 2^{53} \cdot 3^{-1} \cdot 17^6$ $\sigma(f, 5, 20) = 2^{91} \cdot 3^{-3} \cdot 5^2 \cdot 7^1 \cdot 17^3$ $\sigma(f, 5, 21) = 2^{46} \cdot 3^{-2} \cdot 5^1 \cdot 7^1 \cdot 17^6 \cdot 331^1$	Puissance : 6 • signe : +1 $\sigma(f, 6, 22) = 2^{87} \cdot 3^{-3} \cdot 5^2 \cdot 17^6 \cdot 23^1$ $\sigma(f, 6, 24) = 2^{81} \cdot 3^{-2} \cdot 5^1 \cdot 17^7 \cdot 379^1$ $\sigma(f, 6, 26) = 2^{73} \cdot 3^{-4} \cdot 5^2 \cdot 13^1 \cdot 17^6 \cdot 29^1 \cdot 130643^1$ $\sigma(f, 6, 28) = 2^{67} \cdot 3^{-3} \cdot 5^2 \cdot 17^6 \cdot 53948084623^1$
Puissance : 7 • signe : +1 $\sigma(f, 7, 25) = 2^{107} \cdot 3^{-1} \cdot 5^2 \cdot 7^1 \cdot 17^{10}$ $\sigma(f, 7, 26) = 2^{159} \cdot 3^{-4} \cdot 5^5 \cdot 17^7 \cdot 41^1$ $\sigma(f, 7, 27) = 2^{102} \cdot 3^{-3} \cdot 5^2 \cdot 7^1 \cdot 17^{10} \cdot 59^1 \cdot 73^1 \cdot 269^1$ $\sigma(f, 7, 28) = 2^{152} \cdot 3^{-4} \cdot 5^4 \cdot 7^1 \cdot 17^6 \cdot 157^1 \cdot 258119^1$	Puissance : 8 • signe : +1 $\sigma(f, 8, 30) = 2^{151} \cdot 3^{-1} \cdot 5^5 \cdot 17^{10} \cdot 43^1 \cdot 22861^1$ $\sigma(f, 8, 32) = 2^{139} \cdot 3^{-5} \cdot 5^3 \cdot 7^1 \cdot 17^{10} \cdot 144562028920291^1$ $\sigma(f, 8, 34) = 2^{132} \cdot 3^{-2} \cdot 5^4 \cdot 7^1 \cdot 17^{10} \cdot 884011^1 \cdot 99566748443^1$	

Annexe A

Calcul des séries L : méthode alternative

Comme nous l'avons vu dans cette thèse, il est utile de pouvoir évaluer des séries de Dirichlet provenant d'objets arithmétiques ou géométriques (cf. section II.3 et chapitre V). Ces séries satisfont souvent une équation fonctionnelle de type classique et la méthode que nous avons employée se ramenait à calculer des fonctions du type :

$$f(s, x) = \int_x^\infty \frac{1}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} t^{-z} \gamma(z) dz t^{s-1} dt ,$$

où $\gamma(z)$ est un produit de facteurs gammas. L'idée était alors de déplacer la droite d'intégration vers la gauche pour obtenir une somme de résidus et d'intervertir les symboles $\sum_{\text{résidus}}$ et \int_x^∞ . Ceci donne une méthode rapide et efficace mais, comme nous l'avons expliqué, des problèmes numériques importants peuvent survenir quand x devient grand (du même type que si on calcule e^{-x} pour x grand en utilisant la série $\sum (-1)^n x^n / n!$). Un des remèdes possibles peut être d'augmenter la précision avec laquelle nous faisons les calculs.

Dans cette annexe, nous proposons une méthode alternative pour calculer les fonctions $f(s, x)$ (du moins une partie) en évitant tous ces problèmes numériques. Cette méthode est certes rapide et stable mais elle repose simplement sur une observation numérique et elle n'est pas démontrée. On peut néanmoins trouver un procédé pour certifier au “coup par coup” les résultats obtenus. Afin de ne pas alourdir l'exposé, nous allons juste expliquer cette méthode dans le cas particulier où :

$$f(s, x) = \int_x^\infty \frac{1}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} t^{-z} \Gamma(z)^n dz t^{s-1} dt . \quad (\text{A.1})$$

La même méthode peut être obtenue dans un cadre plus beaucoup général.

A.1 Les fonctions K_j

Fixons les valeurs de s , de n et de $x > 0$ et posons :

$$K_0(t) = \frac{1}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} \Gamma(z)^n t^{-z} dz .$$

On définit les fonctions K_j par récurrence :

$$K_j(t) = tK'_{j-1}(t) \text{ pour } j \geq 1 .$$

Les fonctions K_j sont infiniment dérivables et sont à décroissance rapide. Afin d'éviter toute confusion, précisons que nos fonctions K_j ne sont pas les fonctions de Bessel et que nous n'utiliserons pas ces dernières ici.

Proposition A.1.1 *Pour tout $j \geq 0$:*

$$K_j(t) = \frac{(-1)^j}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} \Gamma(z)^n z^j t^{-z} dz . \quad (\text{A.2})$$

De plus on a :

$$(-1)^n K'_{n-1}(t) = K_0(t) . \quad (\text{A.3})$$

Preuve : La première égalité se démontre facilement par récurrence. Pour la seconde, on écrit :

$$K_{n-1}(t) = \frac{(-1)^{n-1}}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} \Gamma(z)^n z^{n-1} t^{-z} dz .$$

Et donc :

$$K'_{n-1}(t) = \frac{(-1)^n}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} \Gamma(z)^n z^n t^{-z-1} dz ,$$

on conclut en utilisant le fait que $z\Gamma(z) = \Gamma(z+1)$ et en faisant le changement de variables $z+1 \leftrightarrow z$. \square

Remarque : La méthode que nous proposons repose sur l'équation différentielle (A.3), satisfaite par K_0 . Dans un cadre plus général, l'équation différentielle est du même type mais un peu plus technique à écrire.

Dans notre contexte particulier, on peut donner quelques propriétés des fonctions K_j . On définit les nombres λ_k^j par récurrence :

$$\begin{aligned} \lambda_1^j &= 1 \text{ pour tout } j \geq 1 \\ \lambda_j^j &= 1 \text{ pour tout } j \geq 1 \\ \lambda_k^{j+1} &= k\lambda_k^j + \lambda_{k-1}^j \text{ pour } 2 \leq k \leq j . \end{aligned}$$

Les premières valeurs de λ_k^j sont données dans le tableau suivant :

	k					
j	1					
	1	1				
	1	3	1			
	1	7	6	1		
	1	15	25	10	1	
	1	31	90	65	15	1

Ces nombres nous permettent d'écrire K_j en fonction de K_0 . On montre en effet par récurrence :

Proposition A.1.2 *Pour tout $j \geq 1$ on a :*

$$K_l(t) = \sum_{k=1}^l \lambda_k^l t^k K_0^{(k)}(t) .$$

En utilisant l'équation (A.3), on obtient :

Corollaire A.1.3 *La fonction K_0 satisfait à l'équation différentielle :*

$$\sum_{k=1}^n \lambda_k^n t^{k-1} K_0^{(k)}(t) = (-1)^n K_0(t) .$$

Pour calculer $K_j(t)$, nous partons de :

$$K_l(x) = \frac{(-1)^l}{2i\pi} \int_{\delta-i\infty}^{\delta+i\infty} \Gamma(z)^n z^l t^{-z} dz .$$

En ramenant le contour d'intégration vers la gauche, on a :

$$K_l(t) = (-1)^l \sum_{a=0}^{\infty} \text{res}_{z=-a} (\Gamma(z)^n z^l t^{-z})$$

On écrit :

$$\Gamma(z)^n = \sum_{k=1}^n \frac{A_{a,k}}{(z+a)^k} + \text{holomorphe en } z = -a .$$

Alors, en posant :

$$u_{a,k} = \sum_{j=0}^{\min(l, n-k)} \binom{l}{k} A_{a,j+k} (-a)^{l-j} ,$$

on obtient :

$$K_l(t) = (-1)^i \sum_{a=0}^{\infty} t^a \sum_{j=0}^{n-1} \frac{(-1)^j}{j!} u_{a,j+1} (\ln t)^j \quad \text{pour } l \leq n-1 .$$

Cette formule permet de calculer les fonctions $K_j(t)$, lorsque t devient grand, nous obtenons les mêmes problèmes numériques qu'avec la fonction $f(s, x)$. On peut aussi utiliser l'équation différentielle satisfaite par $K_0(t)$.

En effet, supposons que nous avons calculé K_0, K_1, \dots, K_{n-1} on en déduit alors facilement $K_0, K'_0, \dots, K_0^{(n-1)}$ par la formule :

$$\begin{pmatrix} K_0(t) \\ K_1(t) \\ K_2(t) \\ \vdots \\ K_{n-1}(t) \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & t & 0 & \cdots & \cdots & 0 \\ 0 & t & t^2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & t & \lambda_2^{n-1}t^2 & \cdots & \lambda_{n-2}^{n-1}t^{n-2} & t^{n-1} \end{pmatrix} \begin{pmatrix} K_0(t) \\ K'_0(t) \\ K''_0(t) \\ \vdots \\ K_0^{(n-1)}(t) \end{pmatrix}$$

Connaissant $K_0, K'_0, \dots, K_0^{n-1}$ on calcule toutes les dérivées d'ordre supérieur de K_0 grâce à l'équation différentielle satisfaite par K_0 .

On obtient alors par la série de Taylor :

$$K_0(t') = \sum_{n=0}^{\infty} \frac{K_0^{(n)}(t)}{n!} h^n \text{ où } t' = t + h$$

ainsi que les dérivées :

$$K_0^{(j)}(t') = \sum_{n=0}^{\infty} \frac{K_0^{(j+n)}(t)}{n!} h^n \text{ où } t' = t + h$$

Enfin, en réitérant le procédé, on obtient les valeurs de $K_0^{(j)}(t + lh)$ où $l \in \mathbb{N}$.

On peut bien sûr appliquer cette méthode directement à la fonction $f(s, x)$. Mais ceci ne supprime pas les problèmes numériques. Néanmoins, remarquons que dans notre situation le calcul de $K_j(t)$ ne fait intervenir qu'une seule variable.

A.2 Relations linéaires

Revenons au calcul de $f(s, x)$ où les nombres s et x sont toujours fixés. On pose

$$f_j(a, b) = \int_0^{\infty} \frac{t^{a-1} K_j(x+t)}{(x+t)^b} dt.$$

Ces définitions ont un sens pour $a > 0$ et b quelconque.

On effectue un changement de variables :

$$f_0(a, b) = \int_x^{\infty} \frac{(t-x)^{a-1} K_0(t)}{t^b} dt$$

Donc $f_0(1, 1-s) = f(s, x)$.

Nous allons obtenir des relations entre les fonctions $f_j(a, b)$.

Proposition A.2.1 *Pour $a > 0$, on a :*

$$f_j(a, b) = f_j(a+1, b+1) + x f_j(a, b+1) \quad (\text{A.4})$$

$$f_j(a+1, b+1) = -a f_{j-1}(a, b) + b f_{j-1}(a+1, b+1) \quad \text{pour } j \geq 1 \quad (\text{A.5})$$

$$f_0(a+1, b+1) = (-1)^{n+1} a f_{n-1}(a, b+1) + (-1)^n (b+1) f_{n-1}(a+1, b+2) \quad (\text{A.6})$$

$$f_0(1, b) = \frac{(-1)^{n+1}}{x^b} K_{n-1}(x) + (-1)^n b f_n(1, b+1) \quad (\text{A.7})$$

Preuve : Pour l'équation (A.4), on écrit :

$$\begin{aligned} f_j(a, b) &= \int_0^\infty \frac{t^{a-1} K_j(x+t)}{(x+t)^b} dt = \int_0^\infty \frac{t^{a-2} K_j(x+t)(x+t-x)}{(x+t)^b} dt \\ &= f_j(a-1, b-1) - x f_j(a-1, b) \quad \text{pour } a > 1. \end{aligned}$$

Les trois autres s'obtiennent par une intégration par parties, en utilisant en plus l'égalité (A.3) pour la formule (A.6). \square

Les relations (A.4), (A.5) et (A.6) permettent d'écrire le système suivant :

$$\begin{pmatrix} a & 0 & \cdots & 0 & 0 & 0 \\ 0 & a & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \cdots & \ddots & a & 0 & 0 \\ 0 & \cdots & \cdots & \ddots & 1 & -x \\ 0 & \cdots & \cdots & \cdots & 0 & (-1)^{n+1} a \end{pmatrix} V_1 = \begin{pmatrix} b & -1 & 0 & \cdots & 0 \\ 0 & b & -1 & \cdots & 0 \\ \vdots & & & & \vdots \\ \vdots & \cdots & b & -1 & 0 \\ 0 & \cdots & \cdots & 1 & 0 \\ 1 & \cdots & \cdots & \cdots & (-1)^{n+1} (b+1) \end{pmatrix} V_2$$

où l'on a posé :

$$V_1 = \begin{pmatrix} f_0(a, b) \\ f_1(a, b) \\ \vdots \\ \vdots \\ f_{n-1}(a, b) \\ f_{n-1}(a, b+1) \end{pmatrix} \quad \text{et} \quad V_2 = \begin{pmatrix} f_0(a+1, b+1) \\ f_1(a+1, b+1) \\ \vdots \\ \vdots \\ f_{n-1}(a+1, b+1) \\ f_{n-1}(a+1, b+2) \end{pmatrix}.$$

En d'autres termes, on a :

$$\begin{pmatrix} f_0(a, b) \\ f_1(a, b) \\ \vdots \\ \vdots \\ f_{n-1}(a, b) \\ f_{n-1}(a, b+1) \end{pmatrix} = M_{a,b} \begin{pmatrix} f_0(a+1, b+1) \\ f_1(a+1, b+1) \\ \vdots \\ \vdots \\ f_{n-1}(a+1, b+1) \\ f_{n-1}(a+1, b+2) \end{pmatrix}, \quad (\text{A.8})$$

où la matrice $M_{a,b}$ est une matrice carrée d'ordre $n + 1$. Dans la relation (A.7), on pose $b = 1 - s$ et $a = 1$:

$$f(s, x) = f_0(1, b) = \frac{(-1)^{n+1} K_{n-1}(x)}{x^b (1 + (-1)^{n+1} b \alpha)} ,$$

où

$$\alpha = \frac{f_{n-1}(1, b+1)}{f_0(1, b)} .$$

Toujours avec $b = 1 - s$ et $a = 1$, on écrit :

$$V = \begin{pmatrix} f_0(a, b) \\ f_1(a, b) \\ \vdots \\ \vdots \\ f_{n-1}(a, b) \\ f_{n-1}(a, b+1) \end{pmatrix} \quad \text{et} \quad M_i = M_{i, b+i} .$$

Pour un vecteur W , désignons par sW le vecteur dont les composantes sont celles de W où l'on a remplacé a par $a + 1$ et b par $b + 1$.

La relation (A.8) nous donne :

$$V = M_1 sV = M_1 M_2 s^2 V = \cdots = M_1 M_2 \cdots M_N s^N V \quad \text{pour tout } N \geq 0 .$$

Ecrivons $A_N = \prod_{i=1}^N M_i$ et $A_N(i, j)$ l'élément de A_N situé sur la i -ème ligne et la j -ème colonne. Sur tous les exemples numériques que nous avons traités, il semble que la suite $\left(\frac{A_N(i, j)}{A_N(i', j)} \right)_N$ converge rapidement (et d'autant plus rapidement que x est grand) vers un nombre indépendant de j . Cela suggère que :

$$\lim_{N \rightarrow \infty} \frac{A_N(i, j)}{A_N(i', j)} = \frac{V(i)}{V(i')} ,$$

où $V(i)$ désigne la i -ème composante du vecteur V .

Toutes les expériences ont confirmé numériquement ce résultat. Supposons qu'il soit vrai. Alors, en prenant $i = n + 1$ et $i' = 1$ on peut facilement calculer

$$\alpha = \frac{f_{n-1}(1, b+1)}{f_0(1, b)} = \lim_{N \rightarrow \infty} \frac{A_N(n+1)}{A_N(1, 1)} .$$

Cette méthode de produit de matrices pour obtenir α est stable et ne pose pas de problèmes numériques.

Si les considérations de convergence décrites plus haut sont exactes, nous avons décomposé le calcul de la fonction $f(s, x)$ en deux parties :

- Le calcul de la fonction $K_{n-1}(x)$ qui est indépendant de s . Pour évaluer la série L initiale nous pouvons éventuellement stocker les valeurs de $K_{n-1}(x)$ dont nous avons besoin.
- Le calcul du nombre $\alpha = \alpha(s, x)$ que l'on obtient par :

$$\alpha = \lim_{N \rightarrow \infty} \frac{A_N(r_2 + 1)}{A_N(1, 1)}$$

la suite étant rapidement convergente.

Le procédé que nous venons de décrire peut être vu comme une sorte de généralisation de l'obtention de fractions continues comme celle que l'on obtient pour calculer la fonction gamma incomplète (i.e. $n = 1$).

Annexe B

Résultats numériques concernant la courbe elliptique de conducteur $N=389$

Soit E la courbe elliptique d'équation :

$$E : y^2 + y = x^3 + x^2 - 2x ,$$

de conducteur $N = 389$. Le groupe $E(\mathbb{Q})$ est de rang 2 engendré par :

$$G_1 = [0, 0] \quad \text{et} \quad G_2 = [1, 0] .$$

Soit φ le revêtement modulaire associé à E . Dans cette annexe, nous donnons les résultats numériques que nous avons commentés dans la section III.1.4. En particulier, on y trouve :

- La liste des points critiques c_1, c_2, \dots, c_{62} de φ .
- Le polynôme $P_1 \in \mathbb{Q}[X]$:

$$P_1(X) = \prod_{k=3}^{62} (X - x(\varphi(c_k))) \quad \text{où } x(P) \text{ est l'abscisse de } P \in E(\mathbb{C}) .$$

On commence le produit à $k = 3$ car $\varphi(c_1) = \varphi(c_2) = 0$.

- Les 40 antécédents du point $2G_1 = [3, 5]$.

B.1 Liste des points critiques

Les termes c_{2k} n'apparaissant pas dans cette liste sont donnés par $c_{2k} = -\overline{c_{2k-1}}$.

$$\begin{aligned}
 c_1 &= \frac{337 + \sqrt{-19}}{2 \times 389} & c_2 &= \frac{-337 + \sqrt{-19}}{2 \times 389} \\
 c_3 &= 0.0169298394643814501869216816 \times i \\
 c_4 &= 0.1518439730519631382000247052 \times i \\
 c_5 &= 0.5 + 0.008015879627931564443796916 \times i \\
 c_6 &= 0.5 + 0.080175046492899577113086416 \times i \\
 c_7 &= 0.02489642044037443954525903258 + 0.00564865990070200826361858946 \times i \\
 c_9 &= 0.09820046073461433181656257427 + 0.02228035175219491948160801927 \times i \\
 c_{11} &= 0.06061017101313141993674166117 + 0.00354050671735277814655230651 \times i \\
 c_{13} &= 0.04226934265352015675890371453 + 0.00246913825025260410189481694 \times i \\
 c_{15} &= 0.3902442956238162807139357767 + 0.002766585552744354841892506947 \times i \\
 c_{17} &= 0.06248646799039751593557104390 + 0.01398547324695967367418811615 \times i \\
 c_{19} &= 0.03917747151074379725440242644 + 0.00876854617196849709886860871 \times i \\
 c_{21} &= 0.1072102112558578489914990843 + 0.003075419394055893630033828109 \times i \\
 c_{23} &= 0.4494617329515394241059200688 + 0.003955565882962623894055876094 \times i \\
 c_{25} &= 0.1310574780941578098408512958 + 0.009647179140939464406216125381 \times i \\
 c_{27} &= 0.3731249289111188740319602957 + 0.002986250451962655866460874275 \times i \\
 c_{29} &= 0.1594541823540566414249637115 + 0.031175552580630690931852010200 \times i \\
 c_{31} &= 0.01552825557080691376902834316 + 0.00303599404472344618938174377 \times i \\
 c_{33} &= 0.2137775071733359561773558040 + 0.003585737259079438417302207985 \times i \\
 c_{35} &= 0.2152934316765863042634947839 + 0.003478547372159323507354332464 \times i \\
 c_{37} &= 0.2520459956517099527461510460 + 0.004094276700968517931622511770 \times i \\
 c_{39} &= 0.2656916163477357887787260636 + 0.031400760387431680563965445540 \times i \\
 c_{41} &= 0.2618474714688031315021995690 + 0.004506195763459539891506137214 \times i \\
 c_{43} &= 0.3050500744052461788878773820 + 0.014860597525484795148768724090 \times i \\
 c_{45} &= 0.3412474991645296669751522177 + 0.004158263143097656740792771359 \times i \\
 c_{47} &= 0.3137865818042318362931053269 + 0.008113029813547437164048036268 \times i \\
 c_{49} &= 0.3457986860680679812710046552 + 0.005173840687682593563086006370 \times i \\
 c_{51} &= 0.3252228061309324011397356272 + 0.002655200603430997372309123612 \times i \\
 c_{53} &= 0.3651417638963494533658217150 + 0.010413350688240294969764942280 \times i \\
 c_{55} &= 0.4160618872793281095962056769 + 0.012435419466218010031473993780 \times i \\
 c_{57} &= 0.4040026959791110241640876983 + 0.003098963567005679486007369526 \times i \\
 c_{59} &= 0.4656495916318387457888961271 + 0.002975791782683325886586763052 \times i \\
 c_{61} &= 0.1321583429394540711823667399 + 0.003437825764182021045848180770 \times i
 \end{aligned}$$

B.2 Le polynôme $P_1(X)$

$$\begin{aligned}
P_1(X) = & (2^{52} \times 7^6 \times 11^3 \times 19^5 \times 67^3 \times 389^7)^{-2} \times \\
& (\quad 707889861317778831208944651568865754551406509688881152 \, X^{30} \\
& + \quad 834557663050046985257231767182269324529342906797949714432 \, X^{29} \\
& - \quad 3630210902541588073207896151095674348223725236816682418176 \, X^{28} \\
& - \quad 231702969335247899465247744750855234889798654015444560642048 \, X^{27} \\
& - \quad 2562832168952967662524709734210291559562387478203656459780096 \, X^{26} \\
& - \quad 15539757045506884120685003997425258192139401519198659300818944 \, X^{25} \\
& - \quad 60438809023812596963992992251718248308133928044569784810995712 \, X^{24} \\
& - \quad 147826657724160190274344736760833306263665379508363886682177536 \, X^{23} \\
& - \quad 147674170608120424872899229735514055260897184355337662468456448 \, X^{22} \\
& + \quad 465556868451584729555860515820870799360477588728428049183408128 \, X^{21} \\
& + \quad 2619635756145254579217912566690963637925215438729770461950836736 \, X^{20} \\
& + \quad 6378387308737247627929297024700040581244674641289800555697192960 \, X^{19} \\
& + \quad 7732361158763272469864188395910725417770651257661257658967269376 \, X^{18} \\
& - \quad 3835335951909622226444482139140598014860472741243084996059805696 \, X^{17} \\
& - \quad 39281958148909912311420150500170560058297986353149550575900556800 \, X^{16} \\
& - \quad 85158058874220847674717178430084581331900714270826571756706789584 \, X^{15} \\
& - \quad 73419358179723071338966963818931251847022784221378897196195724384 \, X^{14} \\
& + \quad 86073016022338603184213207582385814244796939089128207814835775096 \, X^{13} \\
& + \quad 371701180032465398274114081329826396564273204825592723545895750269 \, X^{12} \\
& + \quad 430456544977714949946942505571878340174233616242960840631974205972 \, X^{11} \\
& - \quad 179002967834429776896792021802224291312333632355491785978373783856 \, X^{10} \\
& - \quad 1056567453685647422341332769701325300277823747476086616740680242356 \, X^9 \\
& - \quad 1231789599443621660934200800885614024590448731863802188501607950980 \, X^8 \\
& + \quad 1202240739072977863729357142278132161377123050517038004103607540544 \, X^7 \\
& + \quad 3755647019936208048924144581996301616966358066228396383311126013042 \, X^6 \\
& - \quad 2372833922700041274006124915896789197910139971625188407237191632868 \, X^5 \\
& - \quad 4341998501919292050426385161117862860545406865920554845141809050576 \, X^4 \\
& + \quad 3788952346466036554444656776318150062322166011037475306076616841412 \, X^3 \\
& + \quad 1504384053237343874945890756689028618601606192743636857169653962356 \, X^2 \\
& - \quad 2535336418085957202911384913038751322166191044322920183208833342952 \, X \\
& + \quad 763370576114992064188237143950491471375923741587724187809565278481)^2
\end{aligned}$$

B.3 Les antécédents du points $2G_1$

Les termes x_{2k} n'apparaissant pas dans cette liste sont donnés par $x_{2k} = -\overline{x_{2k-1}}$.

$$\begin{aligned}
x_1 &= 0.50000000000000000000000000000000 + 0.05350159387790578867619146 \times i \\
x_2 &= 0.50000000000000000000000000000000 + 0.12467049112580589496758601 \times i \\
x_3 &= 0.39540803714907501733509689 + 0.00303465155965499556342344 \times i \\
x_5 &= 0.08868044267107809258316586 + 0.00290371422872963715889882 \times i \\
x_7 &= 0.14679829229350011346405875 + 0.00457327347986726117197030 \times i \\
x_9 &= 0.06908457077368200142872350 + 0.00270004859251262162547975 \times i \\
x_{11} &= 0.19765010141051441026067503 + 0.01597944433249162301975551 \times i \\
x_{13} &= 0.45591592941378382702756273 + 0.00252236619274394083228565 \times i \\
x_{15} &= 0.36688367539356351877731785 + 0.00312551627242172175017597 \times i \\
x_{17} &= 0.23889946623123366752330257 + 0.00291006276041852848205223 \times i \\
x_{19} &= 0.01470846531431719353291839 + 0.00771346097986983504070560 \times i \\
x_{21} &= 0.22462102586730975753891037 + 0.00965422011192792731890770 \times i \\
x_{23} &= 0.49129921632975956564217307 + 0.00257513036872268439402058 \times i \\
x_{25} &= 0.10140713973360423182022244 + 0.00243008356623841645110313 \times i \\
x_{27} &= 0.43884922682347698119300056 + 0.00344444258875730195332726 \times i \\
x_{29} &= 0.16715898135877532725860155 + 0.00450026704068726424572735 \times i \\
x_{31} &= 0.07558310445584470383154802 + 0.00310383426714575065239980 \times i \\
x_{33} &= 0.40710870745656985161068531 + 0.00314572338408201578108965 \times i \\
x_{35} &= 0.24439542828401350136234511 + 0.00684316856591630116038598 \times i \\
x_{37} &= 0.34932337973365503833209553 + 0.01943816852295751128570264 \times i \\
x_{39} &= 0.47004200985759789804496554 + 0.00781056786834524999819313 \times i
\end{aligned}$$

Annexe C

Conjecture de Deligne : valeurs numériques

Dans cette annexe figurent les valeurs numériques obtenues concernant les vérifications des conjectures de Deligne (chapitre V). Nous considérons les newforms normalisées de poids 2, 4, 6, 8, et 10, à coefficients entiers et de petits niveaux.

Pour chaque poids, nous décrivons d’abord la liste des formes traitées. Puis, nous donnons, pour chacune des puissances symétriques, les résultats de nos calculs, c’est-à-dire :

- Le signe de l’équation fonctionnelle.
- Les nombres rationnels que nous avons reconnus pour les différentes valeurs de $\sigma(f, m, q)$.

Nous n’avons pris qu’un nombre limité de coefficients $a(n)$ dans les séries L définissant $L(f, s)$; les valeurs $\sigma(f, m, q)$ ne sont donc pas toujours très précises. Néanmoins, elles “ressemblent” fortement aux nombres rationnels donnés (mais nous n’avons pas utilisé le symbole $\stackrel{?}{=}$ comme dans le chapitre V). Ceci nous donne un argument numérique allant dans le sens des conjectures de Deligne.

C.1 Poids 2

On considère ici les formes modulaires de poids 2 associées aux courbes elliptiques définies sur \mathbb{Q} . On prend :

$$\begin{aligned} F_1 &\in S_2(11), & F_2 &\in S_2(14), & F_3 &\in S_2(15), \\ F_4 &\in S_2(17), & F_5 &\in S_2(19), & F_6 &\in S_2(21), \\ F_7, F_8 &\in S_2(26), & F_9 &\in S_2(30), & F_S &\in S_2(37) . \end{aligned}$$

La forme F_7 (resp. F_8) correspond à la courbe elliptique de coefficients $[1, 0, 1, -5, -8]$ (resp. $[1, -1, 1, -3, 3]$). Pour la forme F_S , on choisit la forme modulaire provenant de la courbe elliptique de rang 1 sur \mathbb{Q} . Les premières puissances symétriques pour F_1 sont traitées

dans le chapitre V. Nous avons utilisé, pour les calculs, les 100000 premiers coefficients de Fourier de ces formes modulaires (300000 pour F_S). Le tableau suivant donne les valeurs obtenues concernant les formes $F_2, F_3, F_4, F_5, F_6, F_7, F_8$ et F_9 .

$m \setminus F_k$	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
Puissance 1 • signe : $\sigma(f, 1, 1)$	+1 1	+1 1	+1 1	+1 1	+1 1	+1 1	+1 1	+1 1
Puissance 2 • signe : $\sigma(f, 1, 2)$	+1 1	+1 1	+1 1	+1 1	+1 1	+1 1	+1 1	+1 1
Puissance 3 • signe : $\sigma(f, 1, 2)$	+1 $2^5 \cdot 3^{-1} \cdot 7^2$	+1 $2^3 \cdot 3^2 \cdot 5^2$	+1 $2^4 \cdot 17^2$	+1 $2^4 \cdot 3^{-1} \cdot 19^2$	+1 $2^3 \cdot 3^2 \cdot 7^2$	+1 $2^4 \cdot 3^{-1} \cdot 13^2$	+1 $2^4 \cdot 7^{-1} \cdot 13^2$	+1 $2^3 \cdot 3^1 \cdot 5^2$
Puissance 4 • signe :	+1	+1	+1	+1	+1	+1	+1	+1
Puissance 5 • signe : $\sigma(f, 1, 3)$	-1 0	-1 0	-1 0	-1 0	-1 0	-1 0	-1 0	-1 0
Puissance 6 • signe : $\sigma(f, 1, 4)$	+1 $2^{11} \cdot 3^8$	+1 $2^{24} \cdot 3^1$	+1 $2^{26} \cdot 3^1$	+1 $2^6 \cdot 3^{10} \cdot 5^2$	+1 $2^{22} \cdot 3^2$	+1 $2^3 \cdot 3^8 \cdot 5^1 \cdot 23^1$	+1 $2^3 \cdot 3^2 \cdot 7^3 \cdot 23^1$	+1 $2^{11} \cdot 3^4 \cdot 7^1$
Puissance 7 • signe : $\sigma(f, 1, 4)$	-1 0	-1 0	-1 0	-1 0	-1 0	-1 0	-1 0	-1 0
Puissance 8 • signe :	+1	+1	+1	+1	+1	+1	+1	+1

Les résultats pour la forme F_S sont donnés dans le tableau suivant :

Puissance 1 : • signe : -1 • $\sigma(f, 1, 1) = 0$	Puissance 2 : • signe : +1 • $\sigma(f, 2, 2) = 1$	Puissance 3 : • signe : -1 • $\sigma(f, 3, 2) = 0$
Puissance 4 : • signe : +1 Pas de valeur critique	Puissance 5 : • signe : +1 • $\sigma(f, 5, 3) = 2^8 \cdot 5^1$	Puissance 6 : • signe : +1 • $\sigma(f, 6, 4) = 2^5 \cdot 3^5 \cdot 7^1$

C.2 Poids 4

On considère les formes modulaires de poids 4 sur $\Gamma_0(N)$ avec $N < 20$ sans facteur carré. Pour fixer les notations, on prend :

$$\begin{aligned} F_1 &\in S_4(5), & F_2 &\in S_4(6), & F_3 &\in S_4(7), \\ F_4 &\in S_4(10), & F_5 &\in S_4(13), & F_6, F_7 &\in S_4(14), \\ F_8, F_9 &\in S_4(15), & F_{10} &\in S_4(17), & F_{11} &\in S_4(19) . \end{aligned}$$

Afin d'éviter toute ambiguïté, précisons que le développement de Fourier des formes F_6 , F_7 , F_8 et F_9 commencent par :

$$\begin{aligned} F_6 &= q + 2q^2 + \cdots , \\ F_7 &= q - 2q^2 + \cdots , \\ F_8 &= q + q^2 + \cdots , \\ F_9 &= q + 3q^2 + \cdots . \end{aligned}$$

Le cas de la forme F_1 est traité dans le chapitre V.

Nous n'avons utilisé ici que les 50000 premiers coefficients de $L(f, s)$ (obtenus par le logiciel Magma ([Magma])).

$m \backslash F_k$	F_2	F_3	F_4	F_5
Puissance 1 • signe : $\sigma(f, 1, 2)$ $\sigma(f, 1, 3)$	+1 $2^3 \cdot 3^2$ 1	+1 $2^4 \cdot 7$ 1	+1 $2^2 \cdot 3^{-1} \cdot 5^3$ 1	-1 0 1
Puissance 2 • signe : $\sigma(f, 2, 4)$ $\sigma(f, 2, 6)$	+1 $2 \cdot 3^2 \cdot 5$ 1	+1 $2 \cdot 5 \cdot 7$ 1	+1 5^3 1	+1 $2 \cdot 7 \cdot 13^3 \cdot 173^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 3, 5)$ $\sigma(f, 3, 6)$	-1 0 $2^{12} \cdot 3^7 \cdot 5$	-1 0 $2^{10} \cdot 5 \cdot 7^4 \cdot 11$	-1 0 $2^8 \cdot 5^8$	+1 $2^2 \cdot 3 \cdot 7^3 \cdot 13^4 \cdot 173^{-1}$ $2^9 \cdot 3^2 \cdot 7 \cdot 13^8 \cdot 173^{-3}$
Puissance 4 • signe : $\sigma(f, 4, 8)$	+1 $2^9 \cdot 3^6 \cdot 5^4$	+1 $2^8 \cdot 3^2 \cdot 5^4 \cdot 7^3$	+1 $2^5 \cdot 3^2 \cdot 5^6 \cdot 43$	+1 $2^8 \cdot 3 \cdot 7^5 \cdot 11 \cdot 13^6 \cdot 173^{-3}$
Puissance 5 • signe : $\sigma(f, 5, 8)$ $\sigma(f, 5, 9)$	-1 0 $2^{16} \cdot 3^9 \cdot 5^6$	-1 0 $2^{12} \cdot 3^3 \cdot 5^6 \cdot 7^6$	-1 0 $2^{16} \cdot 3^5 \cdot 3^{10}$	+1 $2^{20} \cdot 3 \cdot 7^5 \cdot 13^{18} \cdot 173^{-6}$ $2^6 \cdot 3 \cdot 7^6 \cdot 13^6 \cdot 173^{-3} \cdot 48228629$
Puissance 6 • signe : $\sigma(f, 6, 10)$ $\sigma(f, 6, 12)$	+1 $2^{28} \cdot 3^{20} \cdot 5^8$ $2^{18} \cdot 3^{13} \cdot 5^9 \cdot 7 \cdot 109$	+1 $2^{17} \cdot 3^2 \cdot 5^6 \cdot 7^{13} \cdot 19$ $2^{15} \cdot 3^3 \cdot 5^7 \cdot 7^4 \cdot 13^2 \cdot 61949$	+1 $2^{22} \cdot 3^4 \cdot 5^{19}$ $2^9 \cdot 3^4 \cdot 5^{12} \cdot 59 \cdot 753229$	
Puissance 7 • signe : $\sigma(f, 7, 11)$ $\sigma(f, 7, 12)$	+1 $2^{34} \cdot 3^{23} \cdot 5^{12} \cdot 7$ $2^{46} \cdot 3^{31} \cdot 5^7 \cdot 13 \cdot 23$			

$m \setminus F_k$	F_6	F_7	F_8	F_9
Puissance 1 • signe : $\sigma(f, 1, 2)$ $\sigma(f, 1, 3)$	+1 $2^4 \cdot 3^{-1} \cdot 7^2$ 1	+1 $2^3 \cdot 7^3 \cdot 17^{-1}$ 1	+1 $2^2 \cdot 3^3 \cdot 5^3 \cdot 47^{-1}$ 1	+1 $2^3 \cdot 3^2 \cdot 5^3 \cdot 29^{-1}$ 1
Puissance 2 • signe : $\sigma(f, 2, 4)$ $\sigma(f, 2, 6)$	+1 $2 \cdot 7^2$ 1	+1 $2 \cdot 5^2 \cdot 7^2 \cdot 17^{-1}$ 1	+1 $2^2 \cdot 3^2 \cdot 5^3 \cdot 47^{-1}$ 1	+1 $2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 29^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 3, 5)$ $\sigma(f, 3, 6)$	-1 0 $2^{12} \cdot 3 \cdot 7^5$	-1 0 $2^{12} \cdot 5^3 \cdot 7^7 \cdot 17^{-3}$	-1 0 $2^{11} \cdot 3^9 \cdot 5^8 \cdot 47^{-3}$	-1 0 $2^8 \cdot 3^7 \cdot 5^7 \cdot 29^{-3} \cdot 71$
Puissance 4 • signe : $\sigma(f, 4, 8)$	+1 $2^7 \cdot 3^3 \cdot 7^4 \cdot 31$	+1 $2^8 \cdot 3 \cdot 5^5 \cdot 7^4 \cdot 17^{-3} \cdot 151$	+1 $2^{15} \cdot 3^5 \cdot 5^6 \cdot 47^{-3} \cdot 347$	+1 $2^{11} \cdot 3^6 \cdot 5^4 \cdot 7 \cdot 29^{-3} \cdot 673$
Puissance 5 • signe : $\sigma(f, 5, 8)$ $\sigma(f, 5, 9)$	-1 0 $2^{11} \cdot 3^6 \cdot 7^7 \cdot 67$	-1 0 $2^{13} \cdot 3 \cdot 5^8 \cdot 7^5 \cdot 13^{-3} \cdot 3307$	-1 0 $2^{26} \cdot 3^5 \cdot 5^{10} \cdot 47^{-3} \cdot 113$	-1 0 $2^{10} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 13^2 \cdot 29^{-3} \cdot 20029$

$m \setminus F_k$	F_{10}	F_{11}
Puissance 1 • signe : $\sigma(f, 1, 2)$ $\sigma(f, 1, 3)$	-1 0 1	-1 0 1
Puissance 2 • signe : $\sigma(f, 2, 4)$ $\sigma(f, 2, 6)$	+1 $2^{-1} \cdot 17^3 \cdot 19^{-1}$ 1	+1 $2 \cdot 3^{-1} \cdot 19^3 \cdot 47^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 3, 5)$ $\sigma(f, 3, 6)$	+1 $2^4 \cdot 3^3 \cdot 17^4 \cdot 19^{-1}$ $2^2 \cdot 3^{-1} \cdot 17^8 \cdot 19^{-3} \cdot 23$	+1 $2^2 \cdot 3^2 \cdot 7^2 \cdot 19^4 \cdot 47^{-1}$ $2^9 \cdot 3^{-4} \cdot 19^8 \cdot 47^{-3} \cdot 59$
Puissance 4 • signe : $\sigma(f, 4, 8)$	+1 $2^2 \cdot 3^3 \cdot 17^6 \cdot 19^{-1} \cdot 409$	+1 $2^9 \cdot 3^{-1} \cdot 19^6 \cdot 47^{-3} \cdot 2137$
Puissance 5 • signe : $\sigma(f, 5, 8)$ $\sigma(f, 5, 9)$	+1 $2^5 \cdot 7^2 \cdot 17^{18} \cdot 19^{-4}$ $2^6 \cdot 3^6 \cdot 5 \cdot 17^6 \cdot 19^{-3} \cdot 1061 \cdot 2767$	+1 $2^{26} \cdot 3^{-4} \cdot 5^2 \cdot 19^{18} \cdot 47^{-6}$???

C.3 Poids 6

On considère les formes modulaires de poids 6 sur $\Gamma_0(N)$ avec $N \leq 10$ sans facteur carré. Pour fixer les notations, on prend :

$$\begin{aligned} F_1 &\in S_6(3), & F_2 &\in S_6(5), & F_3 &\in S_6(6), \\ F_4 &\in S_6(7), & F_5, F_6, F_7 &\in S_6(10) \quad . \end{aligned}$$

Précisons que le développement de Fourier des formes F_5, F_6, F_7 commencent par :

$$\begin{aligned} F_5 &= q + 4q^2 + \cdots \\ F_6 &= q - 4q^2 + 24q^3 + \cdots \\ F_7 &= q - 4q^2 - 26q^3 + \cdots \end{aligned}$$

Le cas de la forme F_1 est traité dans le chapitre V.

Nous n'avons utilisé ici aussi que les 50000 premiers coefficients de $L(f, s)$ (obtenus par le logiciel Magma).

$m \setminus F_k$	F_2	F_3
Puissance 1 • signe : $\sigma(f, 1, 3)$ $\sigma(f, 1, 4)$ $\sigma(f, 1, 5)$	+1 $2^{-1}.5^{-1}.31$ $2^{-1}.3.5^5.11^{-1}$ 1	+1 $2^{-1}.7$ $2^8.3^5.131^{-1}$ 1
Puissance 2 • signe : $\sigma(f, 2, 6)$ $\sigma(f, 2, 8)$ $\sigma(f, 2, 10)$	+1 $2^{-4}.3.5^4.11^{-1}.31$ $2^{-6}.3^2.5^2.11^{-1}.31$ 1	+1 $2^4.3^6.7^1.131^{-1}$ $2^3.3^3.7^1.131^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 3, 8)$ $\sigma(f, 3, 9)$ $\sigma(f, 3, 10)$	+1 $2^1.3^3.5^{16}.11^{-3}.31^1$ $2^{-1}.3^2.5^3.11^{-1}.31^3$ $2^2.3^3.5^{13}.11^{-3}.31^1.41^1$	+1 $2^{26}.3^{20}.7^1.131^{-3}$ $2^7.3^8.7^3.131^{-1}$ $2^{25}.3^{17}.7^1.11^1.131^{-3}$
Puissance 4 • signe : $\sigma(f, 4, 12)$ $\sigma(f, 4, 14)$	+1 $2^{-4}.3^3.5^{11}.11^{-3}.29^1.31^4$ $2^{-6}.3^2.5^8.11^{-3}.31^3.143833^1$	+1 $2^{17}.3^{18}.7^4.19^1.131^{-3}$ $2^{13}.3^{12}.7^3.131^{-3}.313^1.709^1$
Puissance 5 • signe : $\sigma(f, 5, 13)$ $\sigma(f, 5, 14)$ $\sigma(f, 5, 15)$	-1 0 $2^4.3^7.5^{31}.11^{-6}.13^1.31^4$ $3^4.5^{10}.11^{-3}.17^1.31^6.14923^1$	-1 0 $2^{51}.3^{40}.7^4.89^1.131^{-6}$ $2^5.3^9.5^1.7^6.131^{-1}.150791^1$
Puissance 6 • signe : $\sigma(f, 6, 16,)$ $\sigma(f, 6, 18)$ $\sigma(f, 6, 20)$	+1 $2^{-8}.3^7.5^{31}.11^{-6}.13^1.23^1.31^6.353^1$ $2^{-7}.3^9.5^{23}.11^{-6}.31^7.48171881^1$ $2^{-6}.3^6.5^{18}.11^{-5}.31^6.43^1.109^1.55889^1.83903^1$	+1 $2^{44}.3^{46}.7^6.131^{-6}.571^1$ $2^{43}.3^{39}.5^2.7^7.29^1.131^{-6}.263^1$ $2^{34}.3^{32}.7^6.11^1.131^{-6}.494562355127^1$

$m \setminus F_k$	F_4	F_5
Puissance 1 • signe : $\sigma(f, 1, 3)$ $\sigma(f, 1, 4)$ $\sigma(f, 1, 5)$	-1 0 $2^2.3^1.7^4.277^{-1}$ 1	+1 $2.7.3^{-1}$ $2^9.3^{-1}.5^4.181^{-1}$ 1
Puissance 2 • signe : $\sigma(f, 2, 6)$ $\sigma(f, 2, 8)$ $\sigma(f, 2, 10)$	+1 $2^{-3}.3^1.7^5.43^1.277^{-1}$ $2^{-5}.3^2.7^1.43^2.277^{-1}$ 1	+1 $2^6.3^{-1}.5^4.7^1.181^{-1}$ $2^2.3^{-1}.5^1.7^1.43^1.181^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 3, 8)$ $\sigma(f, 3, 9)$ $\sigma(f, 3, 10)$	-1 0 $2^{-4}.3^2.7^5.43^3.277^{-1}$ $2^7.3^3.7^{11}.43^1.277^{-3}.2617^1$	+1 $2^{29}.3^{-2}.5^{14}.7^1.181^{-3}$ $2^7.5^3.7^3.53^1.181^{-1}$ $2^{26}.5^{10}.7^1.11^1.19^1.181^{-3}$
Puissance 4 • signe : $\sigma(f, 4, 12)$ $\sigma(f, 4, 14)$	+1 $2^{-5}.3^7.7^{13}.43^4.277^{-3}$ $2^{-5}.3^3.7^7.43^3.277^{-3}.52007113^1$	+1 $2^{19}.3^{-1}.5^9.7^4.181^{-3}.8681^1$ $2^{14}.3^{-1}.5^6.7^3.181^{-3}.30561577^1$
Puissance 5 • signe : $\sigma(f, 5, 13)$ $\sigma(f, 5, 14)$ $\sigma(f, 5, 15)$	+1 $2^{-8}.3^5.5^3.7^{19}.43^6.277^{-3}$ $2^7.3^7.7^{25}.43^4.277^{-6}.60716479^1$ $2^{-6}.3^6.5^1.7^{12}.13^1.29^1.43^6.277^{-3}.3259^1$	-1 0 $2^{54}.3^{-1}.5^{26}.7^4.13^1.181^{-6}.223^1$ $2^{27}.3^2.5^{10}.7^6.137^1.181^{-3}.2713^1$

$m \setminus F_k$	F_6	F_7
Puissance 1 • signe : $\sigma(f, 1, 3)$ $\sigma(f, 1, 4)$ $\sigma(f, 1, 5)$	+1 $5^2.2^{-1}.3^{-1}$ $2^8.3^{-1}.5^4.137^{-1}$ 1	-1 0 $2^9.5^4.2017^{-1}$ 1
Puissance 2 • signe : $\sigma(f, 2, 6)$ $\sigma(f, 2, 8)$ $\sigma(f, 2, 10)$	+1 $2^4.3^{-1}.5^5.7^1.137^{-1}$ $2^2.3^{-1}.5^2.7^2.137^{-1}$ 1	+1 $2^6.3^2.5^5.2017^{-1}$ $2^2.3^5.5^2.2017^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 3, 8)$ $\sigma(f, 3, 9)$ $\sigma(f, 3, 10)$	+1 $2^{28}.3^{-2}.5^{15}.137^{-3}$ $2^6.5^6.13^1.23^1.137^{-1}$ $2^{26}.5^{12}.17^1.137^{-3}$	-1 0 $2^7.3^7.5^6.2017^{-1}$ $2^{26}.3^3.5^{12}.7^1.163^1.2017^{-3}$
Puissance 4 • signe : $\sigma(f, 4, 12)$ $\sigma(f, 4, 14)$	+1 $2^{16}.3^{-1}.5^{14}.7^2.137^{-3}.397^1$ $2^{12}.3^{-1}.5^8.7^1.11^1.137^{-3}.9065449^1$	+1 $2^{19}.3^9.5^{13}.769^1.2017^{-3}$ $2^{14}.3^7.5^8.2017^{-3}.85486963^1$
Puissance 5 • signe : $\sigma(f, 5, 13)$ $\sigma(f, 5, 14)$ $\sigma(f, 5, 15)$	-1 0 $2^{54}.3^{-1}.5^{28}.11^2.137^{-6}.163^1$ $2^{18}.3^2.5^{15}.23^1.59^1.137^{-3}.397^1.7603^1$	+1 $2^{26}.3^{16}.5^{20}.2017^{-3}$ $2^{55}.3^{10}.5^{28}.7^1.2017^{-6}.47741^1$ $2^{23}.3^{15}.5^{15}.2017^{-3}.538357^1$

C.4 Poids 8

On considère les trois premières formes modulaires de poids 8 i.e.

$$F_1 \in S_8(2), \quad F_2 \in S_8(3), \quad F_3 \in S_8(5) \quad .$$

Le cas de la forme F_1 est traité dans le chapitre V.

Nous n'avons utilisé ici aussi que les 50000 premiers coefficients de $L(f, s)$ (obtenus par le logiciel Magma).

$m \setminus F_k$	F_2	F_3
Puissance 1 • signe : $\sigma(f, 1, 4)$ $\sigma(f, 1, 5)$ $\sigma(f, 1, 6)$ $\sigma(f, 1, 7)$	$+1$ $2^6.3^7.89^{-1}$ $2^{-1}.3^{-1}.5^{-1}.41^1$ $2^5.3^7.89^{-1}$ 1	-1 0 $2^{-1}.3^{-2}.13^1$ $2^4.3^{-1}.5^6.179^{-1}$ 1
Puissance 2 • signe : $\sigma(f, 1, 8)$ $\sigma(f, 1, 10)$ $\sigma(f, 1, 12)$ $\sigma(f, 1, 14)$	$+1$ $2^{-1}.3^7.41^1.89^{-1}$ $3^5.5^{-1}.41^1.89^{-1}$ $2^{-3}.3^1.19^1.41^1.89^{-1}$ 1	$+1$ $2^{-2}.3^{-2}.5^8.13^1.179^{-1}$ $3^{-2}.5^5.13^1.179^{-1}$ $2^{-4}.3^{-4}.5^2.13^1.29^1.83^1.179^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 1, 11)$ $\sigma(f, 1, 12)$ $\sigma(f, 1, 13)$ $\sigma(f, 1, 14)$	-1 0 $2^{15}.3^{24}.7^1.41^1.89^{-3}$ $2^3.3^7.41^3.89^{-1}$ $2^{16}.3^{25}.5^1.41^1.89^{-3}$	$+1$ $2^3.3^{-4}.5^{11}.13^3.179^{-1}$ $2^{11}.3^{-2}.5^{23}.13^1.179^{-3}$ $2^{12}.3^{-6}.5^8.13^3.179^{-1}$ $2^{12}.3^1.5^{21}.13^1.179^{-3}$
Puissance 4 • signe : $\sigma(f, 1, 16)$ $\sigma(f, 1, 18)$ $\sigma(f, 1, 20)$	$+1$ $2^5.3^{23}.5^1.41^4.89^{-3}$ $2^3.3^{19}.5^1.11^2.41^4.89^{-3}$ $2^5.3^{14}.5^{-1}.13^1.41^3.89^{-3}.191^1.4397^1$	$+1$ $2^1.3^{-7}.5^{23}.13^4.17^1.41^1.179^{-3}$ $2^{-1}.3^{-7}.5^{18}.7^2.13^3.173^1.179^{-3}.6961^1$ $2^1.3^{-6}.5^{11}.13^4.23^1.179^{-3}.7549^1.267419^1$
Puissance 5 • signe : $\sigma(f, 1, 18)$ $\sigma(f, 1, 19)$ $\sigma(f, 1, 20)$ $\sigma(f, 1, 21)$	-1 0 $2^9.3^{28}.7^1.41^6.89^{-3}.131^1$ $2^{30}.3^{49}.5^2.13^1.41^4.89^{-6}.269^1$ $2^{11}.3^{23}.5^1.7^1.37^1.41^6.89^{-3}.1117^1$	$+1$ $2^{20}.3^{-6}.5^{52}.13^3.179^{-6}$ $2^9.3^{-9}.5^{27}.13^6.179^{-3}.750929^1$ $2^{21}.3^{-7}.5^{48}.13^5.179^{-6}.1913^1$ $2^{12}.3^{-10}.5^{24}.7^1.13^6.19^1.83^1.137^1.179^{-3}.569^1$
Puissance 6 • signe : $\sigma(f, 1, 22)$ $\sigma(f, 1, 24)$ $\sigma(f, 1, 26)$ $\sigma(f, 1, 28)$	$+1$ $2^{14}.3^{57}.5^2.41^6.89^{-6}.7219^1$ $2^{12}.3^{49}.5^1.41^7.79^1.89^{-6}.1476359^1$ $2^{15}.3^{44}.5^2.17^1.23^1.41^6.89^{-6}.109^1.257^1.43597^1$ $2^{12}.3^{37}.5^2.41^6.89^{-6}.426556356498684053^1$	

C.5 Poids 10

On considère les deux premières formes modulaires de poids 10 : facteur carré. On prend :

$$F_1 \in S_{10}(2), \quad F_2 \in S_{10}(3) \quad ,$$

avec $F_2 = q + 18q^2 + \dots$. Nous n'avons utilisé ici aussi que les 50000 premiers coefficients de $L(f, s)$ (obtenus par le logiciel Magma).

$m \setminus F_k$	F_1	F_2
Puissance 1 • signe : $\sigma(f, 1, 5)$ $\sigma(f, 1, 6)$ $\sigma(f, 1, 7)$ $\sigma(f, 1, 8)$ $\sigma(f, 1, 9)$	+1 $2^{-1}.3^{-1}.5^{-1}.31^1$ $2^{17}.3^{-1}.5^{-1}.7^{-1}$ $2^{-1}.3^{-1}.7^{-1}.31^1$ $2^{17}.3^{-1}.5^{-1}.7^{-1}$ 1	+1 $2^{-1}.3^2.5^{-1}.7^{-1}.11^1$ $2^7.3^9.5^{-1}.337^{-1}$ $2^{-1}.7^{-1}.11^1$ $2^4.3^9.5^{-1}.7^1.337^{-1}$ 1
Puissance 2 • signe : $\sigma(f, 1, 10)$ $\sigma(f, 1, 12)$ $\sigma(f, 1, 14)$ $\sigma(f, 1, 16)$ $\sigma(f, 1, 18)$	+1 $2^{10}.3^{-1}.5^{-1}.7^{-1}.31^1$ $2^6.3^{-1}.5^{-1}.7^{-1}.31^1$ $2^8.3^{-2}.5^{-1}.7^{-2}.31^1$ $3^{-2}.5^{-2}.7^{-1}.31^1.73^1$ 1	+1 $2^{-2}.3^{11}.5^{-1}.11^1.337^{-1}$ $2^{-1}.3^7.5^{-1}.7^{-1}.11^1.17^1.337^{-1}$ $2^{-1}.3^5.5^{-1}.7^{-1}.11^1.31^1.337^{-1}$ $2^{-7}.3^3.5^{-2}.11^1.29^1.179^1.337^{-1}$ 1
Puissance 3 • signe : $\sigma(f, 1, 14)$ $\sigma(f, 1, 15)$ $\sigma(f, 1, 16)$ $\sigma(f, 1, 17)$ $\sigma(f, 1, 18)$	+1 $2^{55}.3^{-1}.5^{-2}.7^{-3}.31^1$ $2^{14}.5^{-1}.7^{-1}.31^3$ $2^{50}.3^{-1}.5^{-2}.7^{-3}.31^1.47^1$ $2^{14}.7^{-1}.31^3$ $2^{52}.5^{-1}.7^{-2}.31^1$	+1 $2^{16}.3^{36}.5^{-2}.7^{-1}.11^1.337^{-3}$ $2^5.3^{15}.5^{-1}.7^{-2}.11^3.337^{-1}$ $2^{16}.3^{31}.5^{-2}.11^1.107^1.337^{-3}$ $2^1.3^{14}.7^{-1}.11^4.337^{-1}$ $2^{17}.3^{27}.5^{-1}.7^1.11^1.337^{-3}.1367^1$
Puissance 4 • signe : $\sigma(f, 1, 20)$ $\sigma(f, 1, 22)$ $\sigma(f, 1, 24)$ $\sigma(f, 1, 26)$	+1 $2^{39}.3^{-1}.5^{-2}.7^{-2}.31^4$ $2^{34}.3^{-2}.7^{-2}.31^3.113^1$ $2^{31}.5^{-3}.7^{-3}.31^3.73^1.3607^1$ $2^{27}.3^{-1}.5^{-1}.7^{-3}.13^1.31^3.337^1.809^1$	+1 $2^4.3^{36}.5^{-2}.7^{-1}.11^4.23^1.337^{-3}$ $3^{28}.11^3.19^2.337^{-3}.443^1$ $3^{22}.5^{-3}.7^{-1}.11^3.83^1.337^{-3}.859^1.4395959^1$ $2^{-1}.3^{20}.5^{-1}.7^{-1}.11^4.127^1.337^{-3}.15359^1.74279^1$
Puissance 5 • signe : $\sigma(f, 1, 23)$ $\sigma(f, 1, 24)$ $\sigma(f, 1, 25)$ $\sigma(f, 1, 26)$ $\sigma(f, 1, 27)$	-1 0 $2^{107}.5^{-3}.7^{-4}.31^3.349^1$ $2^{49}.3^{-1}.5^{-1}.7^{-3}.31^6.114797^1$ $2^{103}.3^2.5^{-2}.7^{-5}.31^4.2273^1$ $2^{47}.7^{-2}.31^6.71^1.9293^1$	-1 0 $2^{30}.3^{70}.5^{-3}.11^3.337^{-6}.328061^1$ $2^{10}.3^{39}.5^{-1}.7^{-4}.11^6.19^1.127^1.337^{-3}.298031^1$ $2^{30}.3^{65}.5^{-2}.11^4.19^1.337^{-6}.5926567^1$ $2^8.3^{34}.7^{-3}.11^6.67^1.337^{-3}.112771^1.381077^1$
Puissance 6 • signe : $\sigma(f, 1, 28)$ $\sigma(f, 1, 30)$ $\sigma(f, 1, 32)$ $\sigma(f, 1, 34)$ $\sigma(f, 1, 36)$	+1 $2^{94}.3^2.5^{-2}.7^{-5}.31^6.26783^1$ $2^{84}.3^1.5^{-2}.7^{-5}.31^6.179^1.4431719^1$ $2^{76}.3^1.5^{-2}.7^{-5}.31^7.348439610993^1$ $2^{75}.3^1.5^{-2}.7^{-5}.31^6.3248070191048671^1$???	

Bibliographie

- [Atkin-Lehner] A. Atkin et J. Lehner, *Hecke operators on $\Gamma_0(N)$* , Math. Ann. **185** (1970), pp. 134-160.
- [Atkin-Li] A. Atkin et W. Li, *Twists of newforms and pseudo-eigenvalues of W -operators*, Invent. Math. **48** (1978), pp. 221-243.
- [Birch] B. J. Birch, *Heegner points of elliptic curves*, Symp. Math. Inst. Alta Math **15**, (1975), pp. 441-445.
- [Breuil etc.] C. Breuil, B. Conrad, F. Diamond et R. Taylor, *On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises*, J. Amer. Math. Soc **14** (2001) no. 4, pp. 843-939.
- [Bump-Friedberg-Hoffstein] D. Bump, S. Friedberg et J. Hoffstein, *Non vanishing theorems for L -functions of modular forms and their derivatives*, Invent. Math. **102** (1990), pp. 543-618.
- [Cassels] J. Cassels *Arithmetics on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine angew. Math. **211** (1962), pp. 95-112.
- [Coates-Schmidt] J. Coates et C. G. Schmidt, *Iwasawa theory for the symmetric square of an elliptic curve*, J. Reine angew. Math. **375** (1987), pp. 104-156.
- [Cohen 1] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math. **138**, Springer-Verlag, New-York, 4-th corrected printing (2000).
- [Cohen 2] H. Cohen, *Advanced topics in computational algebraic number theory*, Graduate Texts in Math. **193**, Springer-Verlag, New-York (2000).
- [Cohen-Lenstra] H. Cohen et H. W. Lenstra, *Heuristics on class groups of number fields*, dans Number theory (Noordwijkerhout, 1983), ed. H. Jager, Lecture Notes in Math. **1068**, Springer Verlag (1984), pp. 33-62.
- [Cremona 1] J. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, 1997.
- [Cremona 2] J. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, Math. Comp. **64** (1995), no. 211, pp. 1235-1250.
- [Cremona 3] J. Cremona, *Tables de courbes elliptiques*, disponible sur le site [http ://www.maths.nott.ac.uk/personal/~jec/ftp/data/INDEX.html](http://www.maths.nott.ac.uk/personal/~jec/ftp/data/INDEX.html)
- [Cremona-Mazur] J. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Exp. Math. **9** :1 (2000), pp. 13-28.

- [Delaunay] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over \mathbb{Q}* , Exp. Math. **10** :2 (2001), pp. 191-196.
- [Delaunay-Duquesne] C. Delaunay et S. Duquesne *Numerical investigations related to the derivatives of the L -series of certain elliptic curves*, preprint.
- [Deligne] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Proceedings of Symposia in Pure Mathematics **33** :2 (1979), pp. 313-346.
- [Elkies] N. Elkies, *Heegner point computations*, Algorithmic Number Theory, eds L. Adelman, M. Huang, ANTS-I, Lecture notes in computer science, **877** (1994), pp. 122-133.
- [Green] P. Green, *Routines pour le calcul des points de Heegner sous PARI* disponible sur le site <http://www.math.mcgill.ca/~darmon/heegner/heegner.html>
- [Goldfeld-Hoffstein-Lieman] D. Goldfeld, J. Hoffstein et D. Lieman, *An effective zero-free region*, Ann. of Math. (2) no. 1 **140** (1994), pp. 177-181.
- [Gross] B. H. Gross, *Heegner points on $X_0(N)$* , Modular Forms ed. R. A. Rankin, (1984), pp.87-105.
- [Gross-Kohnen-Zagier] B. H. Gross, W. Kohnen et D. Zagier, *Heegner points and derivative of L -series. II*, Math. Ann. **278** (1987), pp. 497-562.
- [Gross-Zagier] B. H. Gross et D. Zagier, *Heegner points and derivative of L -series*, Invent. Math. **84** (1986), pp. 225-320.
- [Hall] P. Hall, *A partition formula connected with Abelian groups*, Comment. Math. Helv. **11** (1938-39), 126-129.
- [Hayashi] Y. Hayashi, *The Rankin's L -function and Heegner points for general discriminants*, Proc. Japan. Acad. **71** serie A (1995), pp. 30-32.
- [Kolyvagin] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\text{III}(E/\mathbb{Q})$ for a subclass of Weil curves*, (Russian) Izv. Akad. Nauk. Ser. Mat **52**, (1988) no 6, pp. 1154-1180 ; translation in Math USSR Izv. **33** no. 3 (1989), pp. 473-499.
- [Kowalski] E. Kowalski, *The rank of the jacobian of modular curves : analytic methods*, PhD Thesis, Rutgers University (1998).
- [Murty-Murty] M. Murty et V. Murty, *Mean values of derivatives of modular L -series*, Ann. of Math. **133** (1991), pp. 447-475.
- [Li 1] W. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), pp. 285-315.
- [Li 2] W. Li, *L -series of Rankin type and their functional Equations*, Math. Ann. **244** (1979), pp. 135-166.
- [Magma] Magma, renseignements sur <http://magma.maths.usyd.edu.au/magma/>
- [Mazur-Swinnerton-Dyer] B. Mazur et P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), pp.1-61.
- [mwrnk] J. Cremona, *mwrnk*, disponible par ftp <http://euclid.ex.ac.uk/pub/cremona/progs/>
- [Ogg] A. Ogg, *On a convolution of L -series*, Invent. Math. **7** (1969), pp. 297-312.

- [Pari] C. Batut, K. Belabas, D. Bernardi, H. Cohen, et M. Olivier, PARI-GP, version 2.1.0, disponible par ftp ://megrez.math.u-bordeaux.fr/pub/pari
- [Satgé] P. Satgé, *Groupes de Selmer et corps cubiques*, Journal of Number Theory **23** (1986), pp. 294-317.
- [Serre] J. P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou (1969/70), exp. 19.
- [Serre 2] J. P. Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Séminaire Delange-Pisot-Poitou (1967/68), exp. 14.
- [Shahidi 1] F. Shahidi, *Third symmetric power L -function for $GL(2)$* , Comp. Math **70** (1989), pp. 245-273.
- [Shahidi 2] F. Shahidi, *Symmetric power L -functions for $GL(2)$* , Elliptic curves and related topics ed. H. Kisilevsky et M. Murty, CRM Proceedings and lecture notes **4** (1994), pp. 159-182
- [Shimura 1] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Math. Soc. of Japan **11**, Princeton University Press (1971).
- [Shimura 2] G. Shimura, *The special values of the zeta functions associated with cusp forms*, Com. Pure Appl. Math. **29** (1976), pp. 783-804.
- [Silverman] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math. **151**, Springer-Verlag, New-York (1994).
- [Skoruppa-Zagier] N. Skoruppa et D. Zagier, *Jacobi forms and a certain space of modular forms*, Invent. Math. **94** (1988), pp. 113-146.
- [Stephens] N. Stephens, *Computation of rational points on elliptic curves using Heegner points*, Number theory and applications ed. R. A. Mollin, (1989), pp. 205-214.
- [Stevens] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Inv. Math. **98** (1989), pp. 75-106.
- [Swinnerton-Dyer-Birch] H. Swinnerton-Dyer et B. Birch, *Elliptic curves and modular functions*, in Modular functions of one variable IV, Springer Lectures notes **476**, Berlin-Heidelberg-New-York (1975), pp. 2-32.
- [Szpiro] L. Szpiro, *Discriminant et conducteur de courbes elliptiques*, Séminaire sur les pinceaux de courbes elliptiques, Astérisque **183** ed. L. Szpiro (1990), pp. 7-18.
- [Taylor-Wiles] R. Taylor et A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995) no. 3, pp. 553-572
- [Tenenbaum] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Cours Spécialisés SMF **1**, Société Mathématique de France, 1995.
- [Tollis] E. Tollis, *Zeros of Dedekind zeta functions in the critical strip*, Math. Comp. **66** (1997), pp. 1295-1321.
- [Washington] L. Washington, *Number fields and elliptic curves*, Number theory and applications ed. R. A. Mollin, (1989), pp. 245-278.

- [Watkins] M. Watkins, *Computing the modular degree of an elliptic curve*, preprint.
- [Wiles] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995) no. 3, pp. 443-551.
- [Zagier] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (3) (1985), pp. 372-384.
- [Zagier-Kramarz] D. Zagier et G. Kramarz, *Numerical investigations related to the L -series of certain elliptic curves*, Journal of the Indian Math. Soc. **52** (1987), pp. 51-69.

Résumé : Cette thèse est constituée de plusieurs parties indépendantes qui s'intègrent toutes dans le cadre général de l'étude des courbes elliptiques et des formes modulaires. Nous nous intéressons tout d'abord au revêtement modulaire des courbes elliptiques définies sur \mathbb{Q} . En particulier, nous décrivons la méthode des points de Heegner pour le calcul explicite des points rationnels non triviaux lorsque le rang analytique de la courbe elliptique vaut 1. Nous étudions alors le cas des cubiques de Sylvester ($x^3 + y^3 = m$). Nous expliquons comment déterminer efficacement le degré modulaire en utilisant le carré symétrique de la série L de la courbe elliptique. Puis, nous proposons une étude des points critiques du revêtement.

En se basant sur l'analogie qui existe entre les courbes elliptiques et les corps de nombres, nous faisons une étude sur les groupes de Tate-Shafarevitch des courbes elliptiques définies sur \mathbb{Q} similaire à celle de Cohen et Lenstra sur les groupes de classes d'un corps de nombres. Enfin, l'utilisation du carré symétrique pour le calcul du degré modulaire, s'inscrit dans le cadre plus général des conjectures de Deligne sur les valeurs spéciales des séries L . Nous expliquons comment vérifier numériquement ces conjectures dans le cas des puissances symétriques des séries L de formes modulaires, et nous donnons un nombre conséquent d'exemples.

Title : Modular forms and invariants of elliptic curves defined over \mathbb{Q}

Abstract : This thesis consists of several independent parts all concerning the general setting of elliptic curves and modular forms. First, we are interested in the modular parametrization of elliptic curves defined over \mathbb{Q} . In particular, we describe the Heegner points method to compute explicitly non-trivial rational points whenever the elliptic curve has an analytic rank 1. Then, we study the family of Sylvester cubics ($x^3 + y^3 = m$). We also explain an efficient method to compute the modular degree using the symmetric square L -function associated to the elliptic curve. Then, we give a study of the critical points of the modular parametrization.

Starting with the deep analogy between elliptic curves and number fields, we make a study of Tate-Shafarevitch groups of elliptic curves defined over \mathbb{Q} similar to the one made by Cohen and Lenstra of class groups of number fields.

Finally, the use of the symmetric square L -function in order to evaluate the modular degree belongs to the more general setting of the Deligne conjectures concerning the critical values of L -functions. We explain how to verify these conjectures numerically in the case of symmetric powers of L -functions of modular forms, and we give many examples.

Thèse de **MATHÉMATIQUES PURES**

Mots-Clés :

Algorithme, conjectures de Deligne, courbe elliptique, degré modulaire, forme modulaire, groupe de Tate-Shafarevitch, point de Heegner, revêtement modulaire, point critique.

Laboratoire A2X, Université Bordeaux I,
351, Cours de la Libération 33405 TALENCE Cedex.