



Sur les fonctions L de formes modulaires

Emmanuel Royer

► To cite this version:

Emmanuel Royer. Sur les fonctions L de formes modulaires. Mathématiques [math]. Université Paris Sud - Paris XI, 2001. Français. NNT: . tel-00001437

HAL Id: tel-00001437

<https://theses.hal.science/tel-00001437>

Submitted on 20 Jun 2002

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ORSAY
N° d'ordre : 6539

UNIVERSITÉ DE PARIS-SUD
CENTRE D'ORSAY

**SUR LES FONCTIONS L
DE FORMES MODULAIRES**

THÈSE

présentée pour l'obtention du grade de

DOCTEUR DE L'UNIVERSITÉ PARIS XI-ORSAY
spécialité : MATHÉMATIQUES

par

Emmanuel ROYER

Soutenance publique le 22 juin 2001 devant le jury composé de

Jean-Benoît BOST

Étienne FOUVRY

Henryk IWANIEC

Emmanuel KOWALSKI

Philippe MICHEL

Directeur de thèse

Président du jury

Directeur de thèse

Rapporteurs :

Emmanuel KOWALSKI

Peter SARNAK

À Solveig

*Viendras-tu ?
Es-tu loin encore ?
Prends ton temps.
Je sais que ton fardeau est lourd.
Je t'attends, je te l'ai promis.*

— Henrik Ibsen
Peer Gynt, Acte V, scène 5

Remerciements

C'est avec grand plaisir que je veux exprimer ma reconnaissance

- aux Professeurs Étienne Fouvry et Philippe Michel qui ont dirigé ma thèse. Leurs conseils et encouragements toujours répétés, leur patience et leur disponibilité ont guidé mes premiers pas dans ce monde excitant de la théorie des nombres ;
- au Professeur Henryk Iwaniec, qui lors de sa venue à Orsay et en m'invitant à *l'Institute for Advanced Study* de Princeton m'a communiqué son enthousiasme pour la théorie des fonctions L ... et a fait naître une réelle admiration ;
- au Professeur Jean-Benoît Bost : lors d'un stage de fin d'études, il m'a appris ce qu'était une forme modulaire et comment l'analyse (qu'il m'a aussi apprise) pouvait résoudre des problèmes de théorie des nombres. L'origine de cette thèse lui doit beaucoup. En acceptant de faire partie du jury, il me fait un grand plaisir et un grand honneur ;
- à Régis de la Bretèche et Karim Belabas avec qui j'ai eu de très bénéfiques discussions ;
- au Professeur Peter Sarnak qui a rapporté cette thèse ;
- au Professeur Emmanuel Kowalski qui a rapporté cette thèse et accepté de présider le jury ;
- à François Martin pour ses relectures attentives, le temps passé ensemble devant un tableau ou non... et son amitié essentielle ;
- à Wandrille Decaëns qui m'a accueilli.

Abstract

We give four contributions to the study of L -functions of modular forms. First, we prove that the Jacobian of a modular curve has a simple quotient of great dimension and rank 0 and a simple quotient of great dimension and great rank. In a second contribution we prove the 1-level density conjecture for new families of modular L -functions. Then, we study the distribution of the value at 1 of the L -function of the symmetric square of a modular form. Finally, we give, in collaboration with F.Martin, a criteria for the determination of modular forms by the special values of their L -functions.

2000 Mathematics Subject Classification

11F03, 11F11, 11F25, 11F30, 11F66, 11F67, 11G10, 11G40, 11K38, 11M41, 11N36.

Mots clés

formes modulaires, valeurs spéciales, fonctions L , conjecture de densité, jacobien, petits zéros, carré symétrique, opérateurs de Hecke.

Préface

Ce travail propose quatre contributions à l'étude des fonctions L de formes modulaires. Les méthodes utilisées sont celles de la théorie analytique des nombres et les visées sont algébriques ou géométriques.

Les deux premiers chapitres donnent un survol rapide de la théorie des formes modulaires de poids entier et des fonctions L qui sont associées à ces formes. Ils établissent les résultats nécessaires aux chapitres suivants et mettent en place les problématiques.

Le troisième chapitre porte sur l'étude du rang des facteurs des variétés jacobiniennes « privilégiées » dans le monde des formes modulaires, les variétés $J_0(N)$. Les résultats de ce chapitre sont parus au *Bulletin de la Société mathématique de France* [Roy00]. On montre qu'il existe des facteurs simples de $J_0(N)$ de grande dimension, et on quantifie cette assertion. On montre qu'on peut imposer à ces facteurs d'être de rang nul ou égal à la dimension.

Le quatrième chapitre étudie la répartition des petits zéros des fonctions L de formes modulaires. On teste une conjecture récente de Katz et Sarnak qui relie la répartition des petits zéros de fonctions L de formes modulaires à la répartition des valeurs propres de matrices unitaires. On prouve un théorème qui étaye cette conjecture. Les résultats sont à paraître à *Acta Arithmetica* [Roy01b].

Le cinquième chapitre détermine les moments, positifs et négatifs d'une fonction attachée aux formes modulaires : la valeur au bord de la bande critique de la fonction L de leur carré symétrique (ce nombre est directement relié à la norme de Petersson des formes modulaires). On donne des estimations précises des moments positifs. Les résultats sont à paraître à *Mathematische Annalen* [Roy01c].

Enfin, le dernier chapitre présente un travail effectué en collaboration avec François Martin [MR01]. On détermine le nombre de valeurs qu'il suffit de connaître de séries L attachées à une forme modulaire pour caractériser cette forme modulaire.

On donne maintenant une présentation rapide des résultats. Si N est un entier et k un entier pair, tous deux strictement positifs, $S(k, N)$ est l'espace des formes paraboliques de poids k sur le sous-groupe de congruence $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; (a, b, c, d) \in \mathbb{Z}^4, ad - bc = 1, N|c \right\}$. Les éléments de $S(k, N)$ sont les fonctions holomorphes sur le demi-plan de Poincaré vérifiant,

- 1) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ pour toute $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\Gamma_0(N)$;
- 2) $z \mapsto (\Im z)^{k/2} |f(z)|$ est bornée.

Une telle forme admet un développement de Fourier de la forme

$$f(z) = \sum_{n=1}^{+\infty} \hat{f}(n) \exp(2i\pi n z).$$

Si $N = LM$ avec L et M entiers, et si f est une forme de $S(k, M)$, la fonction $z \mapsto f(Lz)$ appartient à $S(k, N)$. Cette remarque permet de distinguer les formes nouvelles de $S(k, N)$ comme étant celles ne « provenant pas de niveau inférieur » par ce procédé (on définit cette notion plus précisément au §1.3). Pour chaque entier $n \geq 0$ on définit un opérateur, dit de Hecke, de $S(k, N)$ dans lui-même. On montre alors qu'il existe une base orthogonale $B(N)$ de l'espace des formes nouvelles de $S(k, N)$ composée de vecteurs propres de tous les opérateurs de Hecke et dont le premier coefficient de Fourier est 1. À chaque forme f de $B(N)$, on associe une fonction L définie par $L(f, s) = \sum_{n=1}^{+\infty} \hat{f}(n) n^{-s-(k-1)/2}$. Si N est sans facteur carré, on associe aussi à f une fonction L de carré symétrique définie par $L(\text{sym}^2 f, s) = \zeta^{(N)}(2s) \sum_{n=1}^{+\infty} \hat{f}(n^2) n^{-s-k+1}$.

Voici maintenant l'énoncé des résultats originaux présentés dans cette thèse.

Chapitre 3 Pour $N \geq 1$, ayant éventuellement des facteurs carrés, soit $J_0^{\text{new}}(N)$ la partie nouvelle de la jacobienne de la surface de Riemann compacte $X_0(N)$, quotient par $\Gamma_0(N)$ du demi-plan de Poincaré complété. Comme conséquence d'un théorème d'équirépartition des valeurs propres d'opérateurs de Hecke, Serre a montré que la plus grande des dimensions des facteurs $\mathbb{Q}$ -simples de $J_0^{\text{new}}(N)$ tend vers $+\infty$ lorsque N tend vers $+\infty$ [Ser97, théorème 7]. Dans un premier temps on rend effectif ce théorème d'équirépartition grâce à un calcul de discrédance. On déduit alors une version plus forte du résultat de Serre :

THÉORÈME 1

Soit p un nombre premier. Il existe une constante C_p ne dépendant que de p , strictement positive, et un entier N_p ne dépendant que de p tels que pour tout entier $N > N_p$, non divisible par p , il existe un facteur $\mathbb{Q}$ -simple, X , de la variété $J_0^{\text{new}}(N)$ dont la dimension vérifie la minoration suivante :

$$\dim X \geq C_p \sqrt{\ln \ln N}.$$

On sait, grâce à Shimura, interpréter la dimension des facteurs $\mathbb{Q}$ -simples de $J_0^{\text{new}}(N)$ en termes de degré des corps de rationalité de formes primitives de poids 2 sur $\Gamma_0(N)$. En particulier la plus grande des dimensions des facteurs $\mathbb{Q}$ -simples est donnée par le plus grand degré de ces corps de rationalité. Si on fixe un entier premier p ne divisant pas N , le degré du corps de rationalité associé à une forme f primitive relativement à N est minoré par le degré de l'extension sur $\mathbb{Q}$ engendrée par le p -ième coefficient de Fourier de $f : \mathbb{Q}(\hat{f}(p))$. Notre stratégie va donc consister à minorer le degré sur $\mathbb{Q}$ des $\hat{f}(p)$. Utilisant des techniques standard d'approximation des fonctions caractéristiques d'intervalles par des séries de Fourier, on estime la taille minimale que doit avoir un intervalle pour contenir au moins un $\hat{f}(p)/\sqrt{p}$ quand f parcourt $B(N)$. Pour cela, on a besoin d'une formule de trace, c'est-à-dire d'une moyenne des $\hat{f}(p^n)/\sqrt{p^n}$ calculée pour tout entier n avec le poids naturel $1/\text{card}B(N)$. Pour un tel poids, la formule de trace adéquate est celle d'Eichler-Selberg qu'on exprime en s'inspirant de Brumer.

Par des calculs de discrédance de sous-suites de valeurs propres d'opérateurs de Hecke associées à des formes primitives de poids 2 sur $\Gamma_0(N)$ n'annulant pas leur fonction L au point $1/2$ et en utilisant de récents développements de l'étude de ces fonctions L de formes modulaires, on renforce le théorème précédent en étudiant la dimension de facteurs $\mathbb{Q}$ -simples dont le rang (au sens algébrique de Mordell-Weil) est fixé égal à 0.

THÉORÈME 2

Soit p un nombre premier. Il existe une constante C_p ne dépendant que de p , strictement positive, et un entier N_p ne dépendant que de p tels que pour tout entier $N > N_p$, non divisible par p , il existe un facteur $\mathbb{Q}$ -simple, X , de la variété $J_0^{\text{new}}(N)$ de rang nul et dont la dimension vérifie la minoration suivante :

$$\dim X \geq C_p \sqrt{\ln \ln N}.$$

Comme précédemment, les facteurs $\mathbb{Q}$ -simples de $J_0^{\text{new}}(N)$ sont caractérisés par les corps de rationalité des formes f de $B(N)$. Mais, si on veut se restreindre aux facteurs $\mathbb{Q}$ -simples de rang 0, on doit aussi se restreindre aux corps de rationalité associés à des formes primitives dont la fonction L est d'ordre 0 au point $1/2$. (On utilise de récents travaux de Kolyvagin-Logachev et Gross-Zagier qui prouvent la

conjecture de Birch et Swinnerton-Dyer pour les fonctions L d'ordre 0 au point critique). La stratégie de la preuve est donc celle du théorème 1, à la nuance près qu'il faut trouver une formule de trace où la sommation ne se fait plus sur toutes les formes de $B(N)$ mais sur celles dont la fonction L ne s'annule pas en $1/2$. Cette formule est obtenue en insérant un facteur $L(f, \frac{1}{2})$ au poids naturel. On utilise la positivité de $L(f, \frac{1}{2})$ pour calculer une discrédance à partir de cette formule de trace tordue calculée, quant à elle, en exprimant $L(f, \frac{1}{2})$ comme série rapidement convergente, de manière à se ramener à une formule de type Eichler-Selberg.

Enfin des calculs de discrédance de même nature faisant intervenir la dérivée des fonctions L de formes modulaires permettent l'étude de facteurs $\mathbb{Q}$ -simples dont le rang et la dimension sont égaux. On prouve notamment qu'*inconditionnellement* il existe de tels facteurs dont le rang et la dimension deviennent simultanément arbitrairement grands.

THÉORÈME 3

Soit p un nombre premier. Il existe une constante C_p ne dépendant que de p , strictement positive, et un entier N_p ne dépendant que de p tels que pour tout entier $N > N_p$, non divisible par p , il existe un facteur $\mathbb{Q}$ -simple, X , de la variété $J_0^{\text{new}}(N)$ dont la dimension et le rang vérifient :

$$\text{rang } X = \dim X \geq C_p \sqrt{\ln \ln N}.$$

Ce théorème est de nouveau obtenu en utilisant les travaux récents de Kolyvagin-Logachev et Gross-Zagier sur la conjecture de Birch et Swinnerton-Dyer vraie pour les fonctions L d'ordre 1 au point critique. Il faut trouver une formule de trace où la somme se fait sur les formes de $B(N)$ dont la fonction L est d'ordre 1 en $1/2$. Il faut donc trouver un système de poids détectant les fonctions L s'annulant à l'ordre 1 en $s = \frac{1}{2}$ et assez sophistiqué pour être compatible avec la formule de trace. Ceci se fait grâce à l'insertion du facteur :

$$\left(1 - \frac{\hat{f}(p)}{p} + \frac{1}{p}\right) / \left(2\zeta^{(N)}(2) \left(1 - \frac{1}{p^2}\right) \ln \frac{\sqrt{N}}{2\pi e^\gamma} \#B(N)\right).$$

Chapitre 4 Récemment, Katz et Sarnak [KS99a] ont étudié la répartition des zéros de certaines familles de fonctions L sur la droite critique. Ils ont tiré de cette étude une conjecture — appelée *conjecture de densité* — reliant la répartition de ces zéros à la répartition des valeurs propres de groupes de symétrie. Iwaniec, Luo et Sarnak [ILS00] ont éprouvé la solidité de cette conjecture en montrant qu'elle est satisfaite (en admettant l'hypothèse de Riemann généralisée) pour les petits zéros des fonctions L des formes modulaires. On montre ici que la conjecture reste valable en considérant des sous-familles des familles considérées par Iwaniec, Luo et Sarnak caractérisées par les valeurs propres d'opérateurs d'Atkin-Lehner. Nos résultats sont donc un test supplémentaire renforçant la conjecture de densité.

Soit $F = (F(Q))$ un ensemble d'ensembles disjoints de formes modulaires indexé par un paramètre Q . À chaque forme f d'un ensemble $F(Q)$ est associé un réel c_Q appelé conducteur de f et ne dépendant que de la famille $F(Q)$ contenant f . Les zéros non triviaux de la fonction L d'une forme $f \in F(Q)$ sont notés $\frac{1}{2} + i\gamma_f$. Puisqu'on admet l'hypothèse de Riemann généralisée, on a $\gamma_f \in \mathbb{R}$. On introduit un opérateur de comptage de ces zéros

$$D(f, \phi) = \sum_{\gamma_f} \phi\left(\frac{\gamma_f}{2\pi} \ln c_Q\right)$$

où ϕ est une fonction de la classe de Schwartz $\mathcal{S}(\mathbb{R})$ de transformée de Fourier à support compact. La conjecture de densité prédit, pour certaines familles F , l'existence d'une distribution $W(F)$ telle que

$$\lim_{Q \rightarrow \infty} \frac{1}{\#F(Q)} \sum_{f \in F(Q)} D(f, \phi) = \int_{\mathbb{R}} \phi(t) W(F)(t) dt.$$

La conjecture affirme de plus que cette fonction $W(F)$ est la fonction de densité des valeurs propres (correctement normalisées) d'un groupe de symétrie.

On fixe un entier strictement positif ℓ et $\varepsilon = (\varepsilon_1, \dots, \varepsilon_\ell)$ un vecteur de $\{-1, 1\}^\ell$. Pour tout entier sans facteur carré $N = p_1 \cdots p_\ell$ ayant ℓ facteurs premiers $p_1 < \cdots < p_\ell$ on introduit le sous-ensemble des formes primitives de poids k et de niveau N défini par

$$B^\varepsilon(N) = \{f \in B(N) ; W_{p_i} f = \varepsilon_i f, 1 \leq i \leq \ell\}$$

où W_{p_i} est l'opérateur d'Atkin-Lehner associé à p_i . L'opérateur de comptage associé à une forme $f \in B^\varepsilon(N)$ est ainsi

$$D(f, \phi) = \sum_{\gamma_f} \phi\left(\frac{\gamma_f}{2\pi} \ln(k^2 N)\right)$$

où $\frac{1}{2} + i\gamma_f$ décrit les zéros non triviaux de $L(f, s)$. Pour établir le lien avec ce qui précède, on voit que Q décrit l'ensemble des entiers sans facteur carré ayant exactement ℓ facteurs premiers. Pour une fonction X de $B^\varepsilon(N)$ dans $\mathbb{C}$ on définit la moyenne harmonique de X par

$$M^\varepsilon(X) = \sum_{f \in B^\varepsilon(N)} \omega_N(f) X(f)$$

où $\omega_N(f)$ est le poids harmonique classique dans cette théorie (il est défini au paragraphe 1.7.1). On prouve alors le

THÉORÈME 4

Soit k et ℓ des entiers strictement positifs fixés avec k pair. Soit κ un réel vérifiant $0 < \kappa < 1/\ell$. L'hypothèse de Riemann est supposée vraie pour les fonctions L de Dirichlet et pour les fonctions L associées aux formes primitives de poids k . Soit $\varepsilon = (\varepsilon_1, \dots, \varepsilon_\ell)$ un vecteur de $\{-1, 1\}^\ell$. Soit ϕ une fonction paire de $\mathcal{S}(\mathbb{R})$ de transformée de Fourier à support compact dans $] -2, 2[$. On considère une suite d'entiers N sans facteur carré ayant exactement ℓ facteurs premiers $p_1, \dots, p_\ell$ tels que $N^\kappa \leq p_1 < \cdots < p_\ell$. Alors on a

$$\lim_{N \rightarrow \infty} \frac{M^\varepsilon(D(\cdot, \phi))}{M^\varepsilon(1)} = \int_{-\infty}^{\infty} W(x) \phi(x) dx$$

où W est définie par :

si $i^{k\varepsilon_1} \cdots \varepsilon_\ell = 1$ alors

$$W(x) = 1 + \frac{\sin(2\pi x)}{2\pi x}$$

si $i^{k\varepsilon_1} \cdots \varepsilon_\ell = -1$ alors

$$W(x) = 1 - \frac{\sin(2\pi x)}{2\pi x} + \delta_0(x)$$

où δ_0 est la distribution de Dirac en 0.

REMARQUE Si $f \in B^\varepsilon(N)$ alors $i^{k_{\varepsilon_1} \cdots \varepsilon_\ell}$ est le signe de l'équation fonctionnelle de $L(f, s)$. Selon que cette valeur vaut 1 ou -1 on dit que f est paire ou impaire. Le théorème montre que la distribution moyenne des petits zéros n'est gouvernée que par le signe de l'équation fonctionnelle et non par les signes des différentes composantes d'Atkin-Lehner. Cela confirme – au moins dans le domaine $] -2, 2[$ des petits zéros – la robustesse de la conjecture de densité.

Ce résultat généralise le résultat suivant dû à Iwaniec, Luo et Sarnak qui considéraient les espaces

$$B^+(N) = \{f \in B(N); W_N f = i^k f\}$$

et

$$B^-(N) = \{f \in B(N); W_N f = -i^k f\}$$

et obtenaient

THÉORÈME 5 (THEOREM 1.1 DE [ILS00])

Fixons $\phi \in \mathcal{S}(\mathbb{R})$ de transformée de Fourier à support compact dans $] -2, 2[$. Alors, lorsque N parcourt les entiers sans facteur carré

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^\pm(N)} \sum_{f \in B^\pm(N)} D(f, \phi) = \int_{-\infty}^{\infty} \phi(x) W^\pm(x) dx$$

avec

$$W^+(x) = 1 + \frac{\sin(2\pi x)}{2\pi x}$$

et

$$W^-(x) = 1 - \frac{\sin(2\pi x)}{2\pi x} + \delta_0(x).$$

Notre méthode consiste à exprimer les sommes sur $B^\varepsilon(N)$ en sommes sur $B(N)$ grâce à l'introduction de facteurs s'annulant pour les formes n'ayant pas les valeurs propres d'Atkin-Lehner recherchées. Après avoir exprimé ces valeurs propres d'Atkin-Lehner en termes de valeurs propres de Hecke, on est ramené à évaluer des formules de trace sur les formes primitives. Pour cela on utilise une formule de trace sur les formes primitives (de type Petersson) due à Iwaniec, Luo et Sarnak. On commence par montrer que la contribution des formes anciennes est négligeable si on suppose que le plus petit facteur premier du niveau croît assez vite. L'estimation de la contribution des formes nouvelles se fait par une évaluation de sommes de sommes de Kloosterman. C'est cette estimation qui requiert l'hypothèse de Riemann des séries L de Dirichlet.

On calculera rapidement la contribution des formes anciennes (c'est le seul endroit où sera nécessaire l'hypothèse de Riemann pour les fonctions L de formes primitives) puis, plus précisément celles des formes nouvelles. On pourra finalement établir un pas vers la conjecture de densité.

Chapitre 5 Soit κ un réel, $0 < \kappa \leq 1$ et $\mathcal{N}$ l'ensemble des entiers sans facteur carré N de plus petit facteur premier $p_1(N) \geq N^\kappa$. On étudie la variable aléatoire qui associe à une forme f de $B(N)$ la valeur en 1 de la fonction L associée au carré symétrique de f , soit

$$\begin{array}{ccc} L(sym^2, 1) & : & B(N) \rightarrow \mathbb{R} \\ & & f \mapsto L(sym^2 f, 1) \end{array}$$

lorsque N parcourt $\mathcal{N}$. On montre que ces variables aléatoires admettent une variable aléatoire limite $L(sym^2, 1)_\infty$ dont on calcule les moments dans le

THÉORÈME 6

Soit $n \geq 1$ un entier. Soit

$$M_n(N) = \frac{1}{\#B(N)} \sum_{f \in B(N)} L(\text{sym}^2 f, 1)^{n-1}.$$

Alors, lorsque N parcourt $\mathcal{N}$ il existe un réel M_n tel que

$$\lim_{N \rightarrow \infty} M_n(N) = M_n.$$

On définit pour tout $\mathbf{b} \in \mathbb{N}^n$ l'ensemble

$$\mathcal{E}_n(\mathbf{b}) = \left\{ \mathbf{d} \in \mathbb{N}^{n-1}; d_i \mid \left(\frac{b_1 \cdots b_i}{d_1 \cdots d_{i-1}}, b_{i+1} \right)^2, 1 \leq i \leq n-1 \right\}$$

puis pour tout $r \geq 1$ entier

$$m_n(r) = \sum_{\substack{\mathbf{b} \in \mathbb{N}^n \\ \det \mathbf{b} = r}} \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{b}) \\ \det \mathbf{d} = \det \mathbf{b}}} 1.$$

On a alors

$$M_n = \zeta(2)^{n-1} \sum_{r=1}^{+\infty} \frac{m_n(r)}{r}.$$

La variable aléatoire $L(\text{sym}^2, 1)$ admet lorsque N parcourt $\mathcal{N}$ une variable aléatoire limite $L(\text{sym}^2, 1)_\infty$ dont le moment d'ordre $n-1$ est M_n . En particulier, l'espérance de $L(\text{sym}^2, 1)_\infty$ est

$$E[L(\text{sym}^2, 1)_\infty] = \zeta(2)^2$$

et sa variance

$$\text{Var}[L(\text{sym}^2, 1)_\infty] = \zeta(2)^4 \left[\frac{\zeta(2)\zeta(3)}{\zeta(6)} - 1 \right] \approx 6,908.$$

Dans cet énoncé, et dans toute la suite, les lettres grasses telles que $\alpha, \beta, \gamma, \mathbf{b}, \mathbf{d} \dots$ désignent des vecteurs. Leurs coordonnées seront numérotées en indice, ainsi $\alpha = (\alpha_1, \dots, \alpha_m)$. Le déterminant – noté $\det$ – d'un vecteur est le produit de ses coordonnées, ainsi $\det \alpha = \alpha_1 \cdots \alpha_m$. La trace – notée tr – d'un vecteur désigne la somme de ses coordonnées, ainsi $\text{tr} \alpha = \alpha_1 + \cdots + \alpha_m$. Le produit de deux vecteurs est le vecteur de même dimension obtenu en multipliant entre elles les coordonnées de même indice, ainsi $\alpha\beta = (\alpha_1\beta_1, \dots, \alpha_m\beta_m)$. Enfin, on a fait les conventions $\mathbb{N}^0 = \{1\}$, $\mathcal{E}_1(\mathbf{b}) = \{1\}$ et $d_1 \cdots d_0 = 1$.

La preuve utilise crucialement le fait, prouvé par Gelbart et Jacquet, que la fonction $L(\text{sym}^2 f, s)$ est la fonction L d'une forme automorphe de GL_3 et la théorie de la convolution de Rankin-Selberg pour ce groupe. Par des techniques dérivées du grand crible et utilisées par Luo et Kowalski-Michel, on exprime $L(\text{sym}^2 f, 1)$ comme un polynôme de Dirichlet court en moyenne. Ce résultat est analogue et a été inspiré par les travaux de Luo [Luo99] dans le cas des formes de Maaß pour $SL(2, \mathbb{Z})$. En particulier, les moments sont les mêmes. Luo obtenait la majoration

$$\ln M_n \ll n \ln \ln n.$$

On obtient un encadrement plus précis dans le

THÉORÈME 7

Pour tout entier $n \geq 2$ on a

$$\ln M_n = 3n \ln \ln n + O(n).$$

En fait, ces techniques permettent également le calcul (inspiré par un travail ultérieur de Luo [Luo00]) des moments négatifs.

THÉORÈME 8

Soit $n \geq 1$ un entier. On définit pour tout $r \geq 1$ entier

$$m_{-n}(r) = \sum_{\substack{\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n \\ \det \mathbf{a} \mathbf{b}^2 \mathbf{c}^3 = r}} \mu(a_1 b_1 c_1) \cdots \mu(a_n b_n c_n) \mu(b_1) \cdots \mu(b_n) \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{a} \mathbf{b}) \\ \det \mathbf{a} \mathbf{b} = \det \mathbf{d}}} 1.$$

Le moment négatif d'ordre $-n - 1$ de $L(\text{sym}^2, 1)_\infty$ est donné par

$$M_{-n} = \frac{1}{\zeta(2)} \sum_{r=1}^{+\infty} \frac{m_{-n}(r)}{r}.$$

Avec les conventions déjà faites, cet énoncé reste valable pour $n = 0$.

Enfin, soit q un nombre premier, les travaux de Serre déjà cités prouvent que la variable aléatoire $f \mapsto \lambda_f(q)$ admet une variable aléatoire limite lorsque $N \rightarrow \infty$. On considère $L^{(q)}(\text{sym}^2, 1)$, la variable aléatoire obtenue de $L(\text{sym}^2, 1)$ par division par le q -ième facteur eulerien et on prouve le résultat d'indépendance

PROPOSITION 1

Soit q un nombre premier. Les variables aléatoires limites, lorsque N parcourt $\mathcal{N}$ en restant premier à q , des variables aléatoires

$$\begin{array}{ccc} \lambda(q) & : & B(N) \rightarrow \mathbb{R} \\ & & f \mapsto \lambda_f(q) \end{array}$$

et $L^{(q)}(\text{sym}^2, 1)$ sont indépendantes.

On rappelle que deux variables aléatoires sont indépendantes lorsque la fonction de distribution cumulative du couple qu'elles forment est le produit des fonctions de distribution cumulative de chacune d'elles.

Chapitre 6 Les résultats de ce chapitre ont été obtenus en collaboration avec François Martin. Soit Γ un sous-groupe de congruence de $SL(2, \mathbb{Z})$ et k un entier, on note $S(2k, \Gamma)$ l'espace des formes modulaires paraboliques de poids $2k$ sur Γ (voir le §6.3.1). Si $(\mathcal{L}_1, \dots, \mathcal{L}_n)$ est un ensemble de formes linéaires sur $S(2k, \Gamma)$, on dit que cet ensemble caractérise la forme $f \in S(2k, \Gamma)$ si on a l'implication

$$\forall g \in S(2k, \Gamma), \left\{ \begin{array}{l} \mathcal{L}_1(f) = \mathcal{L}_1(g) \\ \vdots \\ \mathcal{L}_n(f) = \mathcal{L}_n(g) \end{array} \right. \implies (f = g).$$

Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice de $SL(2, \mathbb{Z})$ et $f \in S(2k, \Gamma)$, on définit une fonction $f|_A$ sur le demi-plan de Poincaré $\mathcal{H}$ en posant

$$f|_A(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right).$$

À cette fonction, on peut associer une fonction L dont les valeurs intéressantes sont les valeurs aux entiers de $[1, 2k - 1]$ (voir §6.3.2). On s'intéresse dans ce chapitre aux formes linéaires $f \mapsto L(f|_A, \ell)$ lorsque A parcourt un ensemble de représentants du quotient $\Gamma \backslash SL(2, \mathbb{Z})$. On prouve le

THÉORÈME 9

Soit Γ un sous-groupe de congruence de $SL(2, \mathbb{Z})$ contenant $-I$ et k un entier strictement positif. Soit $f \in S(2k, \Gamma)$. Il existe un sous-ensemble $\mathcal{R}$ de $SL(2, \mathbb{Z}) \times \{1, \dots, 2k-1\}$ de cardinal

$$\frac{2k-1}{6} \nu_0(\Gamma) + \varepsilon_S(2k) \frac{\nu_2(\Gamma)}{2} + 2\varepsilon_U(2k) \frac{\nu_3(\Gamma)}{3} + \delta(k=1)$$

tel que

$$[\forall (A, \ell) \in \mathcal{R}, \forall g \in S(2k, \Gamma), L(f|_A, \ell) = L(g|_A, \ell)] \Rightarrow (f = g).$$

Dans cet énoncé, $\delta(k=1)$ vaut 1 si $k=1$ et 0 sinon. Les fonctions ε_S et ε_U sont définies par

$$\varepsilon_S(2k) = \begin{cases} 1 & \text{si } 2k \equiv 0 \pmod{4}; \\ -1 & \text{si } 2k \equiv 2 \pmod{4} \end{cases}$$

et

$$\varepsilon_U(2k) = \begin{cases} 0 & \text{si } 2k \equiv 1 \pmod{3}; \\ 1 & \text{si } 2k \equiv 0 \pmod{3}; \\ -1 & \text{si } 2k \equiv -1 \pmod{3}. \end{cases}$$

Le nombre $\nu_0(\Gamma)$ est l'indice de Γ dans $SL(2, \mathbb{Z})$. Le nombre $\nu_2(\Gamma)$ (*resp.* $\nu_3(\Gamma)$) est le nombre de points elliptiques d'ordre 2 (*resp.* d'ordre 3) de Γ . À titre d'exemple, on a

$$\nu_2(\Gamma_0(m)) = \begin{cases} 0 & \text{si } 4|m; \\ \prod_{p|m} [1 + (\frac{-1}{p})] & \text{sinon} \end{cases}$$

et

$$\nu_3(\Gamma_0(m)) = \begin{cases} 0 & \text{si } 9|m; \\ \prod_{p|m} [1 + (\frac{-3}{p})] & \text{sinon.} \end{cases}$$

[Miy89, theorem 4.2.7] Ce résultat est à comparer avec la dimension de $S(2k, \Gamma)$, [Miy89, theorem 2.5.2, lemma 4.2.6, theorem 4.2.11]

$$\dim S(2, \Gamma) = 1 + \frac{\nu_0(\Gamma)}{12} - \frac{\nu_2(\Gamma)}{4} - \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}$$

et, si $2k \geq 4$,

$$\dim S(2k, \Gamma) = \frac{2k-1}{12} \nu_0(\Gamma) + \frac{\nu_2(\Gamma)}{4} + \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}$$

où $\nu_\infty(\Gamma)$ est le nombre de pointes de Γ (voir §6.3.1).

Sans restriction sur $S(2k, \Gamma)$, on a le minoant

$$\#\mathcal{R} \geq \dim S(2k, \Gamma).$$

D'autres grandeurs que les formes linéaires utilisées ici ont été étudiées. Si $f \in S(2k, m) = S(2k, \Gamma_0(m))$, on définit, pour tout caractère χ , la fonction

$$L(f \otimes \chi, s) = \sum_{n=1}^{+\infty} \hat{f}(n) \chi(n) n^{-s}.$$

Luo et Ramakrishnan [LR97b] ont prouvé (entre autre) que l'ensemble des valeurs $L(f \otimes \chi, k)$ lorsque χ parcourt tous les caractères quadratiques de module premier à m détermine f . D'autre part, si $f \in S(2, m)$, on dit que f est associée à une

courbe elliptique si sa fonction L coïncide avec celle d'une courbe elliptique. Stark [Sta96] a prouvé que la valeur $L(f, 1)$ caractérise la forme f . On remarque qu'on a fait une grosse restriction sur $S(2, m)$ puisque, si on note $Ell(2, m)$ l'ensemble (fini) des formes de $S(2, m)$ associées à une courbe elliptique, on a pour tout $\varepsilon > 0$,

$$\frac{\#Ell(2, m)}{\dim S(2, m)} \leq C(\varepsilon)m^{-1/2+\varepsilon}$$

avec $C(\varepsilon)$ une constante ne dépendant que de ε [DK00].

Notre méthode consiste à tirer parti des relations de Manin. À chaque forme f on peut associer un polynôme appelé polynôme de périodes (voir §6.3.1). Ce polynôme vérifie des relations que l'on peut traduire en relations linéaires sur les valeurs $L(f|_A, \ell)$. Un morphisme injectif, dû à Eichler et Shimura (et Skorrupa dans la version utilisée ici) permet alors de ramener notre problème au calcul du rang d'un système linéaire (voir §6.4). Ce calcul est essentiellement un travail de combinatoire.

On déduit une autre conséquence du monomorphisme d'Eichler-Shimura, indépendante de la précédente. Pour p premier, on définit $X(p)$ comme l'ensemble des $p-1$ caractères modulo p et W_p l'involution de Fricke (voir §6.5). On a alors la

PROPOSITION 2

Soit k un entier et p un nombre premier. Soit f et g deux formes de $S(2k, \Gamma_0(p))$. On suppose que

$$\forall \ell \in [1, k], \forall \chi \in X(p), \quad L(W_p f \otimes \chi, \ell) = L(W_p g \otimes \chi, \ell),$$

$$\forall \ell \in [1, k], \quad L(W_p f, \ell) = L(W_p g, \ell)$$

et

$$\forall \ell \in [1, k], \quad L(f, \ell) = L(g, \ell).$$

Alors $f = g$.

Table des matières

Notations	xxi
1 Formes modulaires	1
1.1 L'espace des formes modulaires	1
1.2 Opérateurs de Hecke	3
1.2.1 Polynômes de Tchebychef de seconde espèce	3
1.2.2 Définition des opérateurs de Hecke	5
1.2.3 Propriétés des opérateurs de Hecke	5
1.2.4 Valeurs propres	6
1.3 Formes nouvelles et primitives	8
1.3.1 Formes anciennes et nouvelles	8
1.3.2 Formes primitives	9
1.4 Opérateurs d'Atkin-Lehner	10
1.5 Action de Galois	11
1.6 Formes signées	12
1.7 Formules de trace	13
1.7.1 Formule de Petersson	13
1.7.2 Formule de Selberg	17
2 Fonctions L	21
2.1 Présentation générale	21
2.2 Fonctions L de formes primitives	22
2.2.1 Définition	22
2.2.2 Zéros des fonctions L de formes primitives	23
2.2.3 Valeurs particulières en $\frac{1}{2}$	30
2.3 Fonction L de carré symétrique	36
2.3.1 Définition et équation fonctionnelle	36
2.3.2 La valeur particulière $L(sym^2 f, 1)$	39
2.3.3 Fonction L d'une variété	42
3 Facteurs simples de $J_0(N)$	45
3.1 Résultats	45
3.2 Choix des poids	46
3.2.1 Choix d'un poids pour la formule d'Eichler-Selberg	46
3.2.2 Choix de poids pour $L(f, \frac{1}{2})$	47
3.2.3 Choix d'un poids pour $(1 + \varepsilon_f(N))L'(f, \frac{1}{2})$	47
3.3 Discrépance des valeurs propres de Hecke	48
3.4 Comptage d'entiers algébriques	53
3.5 Preuve du théorème 3.1.1	54
3.5.1 Noyau de la preuve	54
3.5.2 Facteurs simples	55
3.5.3 Facteurs simples de rang nul	55

3.5.4	Facteurs simples de grand rang	55
4	Petits zéros	57
4.1	Résultats	57
4.2	Densité de répartition signée	61
5	Statistique de $L(sym^2, 1)$	71
5.1	Résultats	71
5.2	Préliminaires probabilistes	73
5.3	Moments	74
5.3.1	Calculs	74
5.3.2	Expression combinatoire des moments positifs	77
5.3.3	Encadrement	79
5.4	Distribution	80
5.5	Espérance et variance	81
5.6	Dépendance avec les valeurs propres de Hecke	82
6	Détermination des formes modulaires par les valeurs de fonctions L	85
6.1	Introduction	85
6.2	Lemmes combinatoires	87
6.3	Les équations de Manin	90
6.3.1	Périodes de formes modulaires	90
6.3.2	Fonctions L - Liens avec les périodes	93
6.3.3	Base du système de Manin	94
6.4	Caractérisation par les valeurs de fonctions L	100
6.4.1	Mise en équation du système	101
6.4.2	Résolution	104
6.5	Une autre application des périodes	107
A	Sommes de Kloosterman	109
B	Fonctions de Bessel	117
	Bibliographie	119

Notations

On donne ici quelques notations utilisées dans ce travail. Dans cette liste z, s sont des complexes quelconques, x, a, b des réels quelconques, m, n et N des entiers strictement positifs quelconques. Enfin, f, g et h sont des fonctions.

$\mathbb{N}$ est l'ensemble des entiers naturels *y compris 0*.

$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ est l'ensemble des entiers naturels non nuls.

$\mathbb{R}^+$ est l'ensemble des réels *positifs*, c'est-à-dire *positifs ou nuls*.

$\mathcal{P}$ est l'ensemble des nombres premiers.

$\sharp A$ est le cardinal de l'ensemble A .

$|G|$ est l'ordre du groupe G .

p est *toujours* un nombre premier.

ε est toujours un nombre réel strictement positif. Il peut être aussi petit que nécessaire et peut changer de ligne à ligne.

$s = \sigma + it$: lorsque s est un complexe, $\sigma = \Re s$ et $t = \Im s$ sont, respectivement, ses parties réelle et imaginaire.

$z = x + iy$: lorsque z est un complexe, $x = \Re z$ et $y = \Im z$ sont, respectivement, ses parties réelle et imaginaire.

$\gamma = -\Gamma'(1)$ est la constante d'Euler.

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

$$U = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad T' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

$\zeta^{(N)}$ est la fonction ζ privée de ses facteurs eulériens liés à l'entier N

$$\zeta^{(N)}(s) = \prod_{p|N} \left(1 - \frac{1}{p^s}\right) \zeta(s).$$

On ne confondra pas avec une dérivée multiple de ζ qui n'apparaît jamais ici.

$$e(z) = \exp(2i\pi z).$$

$$\delta(a, b) = \begin{cases} 1 & \text{si } a = b; \\ 0 & \text{si } a \neq b. \end{cases}$$

$m|n^\infty$ signifie que pour tout nombre premier p , si p divise m , alors p divise n .

$m||n$ signifie que m divise l'entier n et que m et $\frac{n}{m}$ sont premiers entre eux, $(m, n/m) = 1$.

$\varepsilon_N(n)$ est la fonction caractéristique des entiers premiers à N

$$\varepsilon_N(n) = \begin{cases} 1 & \text{si } (n, N) = 1; \\ 0 & \text{si } (n, N) > 1. \end{cases}$$

$\chi_N^\square$ est la fonction caractéristique des carrés premiers à N

$$\chi_N^\square(n) = \begin{cases} 1 & \text{si } (n, N) = 1 \text{ et } n \text{ est le carré d'un entier;} \\ 0 & \text{si } (n, N) > 1 \text{ ou si } n \text{ n'est pas le carré d'un entier.} \end{cases}$$

ω est la fonction nombre de diviseurs premiers sans multiplicité

$$\omega(n) = \sum_{\substack{p \in \mathcal{P} \\ p|n}} 1.$$

τ est la fonction nombre de diviseurs

$$\tau(n) = \sum_{\substack{d \in \mathbb{N} \\ d|n}} 1.$$

τ_3

$$\tau_3(n) = \#\{(i, j, k) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* ; ijk = n\}.$$

$v_p(n)$ est la valuation p -adique de n

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

$p_1(n)$ est le plus petit facteur premier de n .

μ est la fonction de Möbius

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{si } n \text{ est sans facteur carré;} \\ 0 & \text{sinon.} \end{cases}$$

Λ est la fonction de Von Mangoldt

$$\Lambda(n) = \begin{cases} \ln p & \text{s'il existe } m > 0 \text{ et } p \in \mathcal{P} \text{ tels que } n = p^m ; \\ 0 & \text{si } n = 1 \text{ ou si } n \text{ a au moins deux diviseurs premiers.} \end{cases}$$

φ est la fonction d'Euler

$$\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

$\nu(n)$

$$\nu(n) = n \prod_{\substack{p \in \mathcal{P} \\ p|n}} \left(1 + \frac{1}{p}\right).$$

Si $(m, n) = 1$ alors $\overline{m} \pmod{n}$ désigne l'inverse de m modulo n .

$$\sum_{i|n} f(i) = \sum_{\substack{i \in \mathbb{N} \\ i|n}} f(i).$$

$$\sum_{ij=n} f(i, j) = \sum_{i|n} f\left(i, \frac{n}{i}\right).$$

$$\sum_{ij|n} f(i, j) = \sum_{i|n} \sum_{j|\frac{n}{i}} f(i, j).$$

$$\sum_{(p, N)=1} f(p) = \sum_{\substack{p \in \mathcal{P} \\ (p, N)=1}} f(p).$$

Les lettres grasses telles $\mathbf{u}$, $\mathbf{v}$ désignent toujours des vecteurs. Leurs coordonnées seront numérotées en indice, ainsi $\mathbf{u} = (u_1, \dots, u_m)$. Le déterminant – noté $\det$ – d'un vecteur est le produit de ses coordonnées, ainsi $\det \mathbf{u} = u_1 \cdots u_m$. La trace – notée tr – d'un vecteur désigne la somme de ses coordonnées, ainsi $\text{tr} \mathbf{u} = u_1 + \cdots + u_m$. Le produit de deux vecteurs est le vecteur de même dimension obtenu en multipliant entre elles les coordonnées de même indice, ainsi $\mathbf{uv} = (u_1 v_1, \dots, u_m v_m)$.

$\|\cdot\|_\infty$

$$\|f\|_\infty = \sup_{x \in \mathbb{R}} |f(x)|.$$

$\mu(f)$: si μ est une mesure

$$\mu(f) = \int_{\mathbb{R}} f(x) \, d\mu.$$

$f \ll_{a,b,\dots} g$: il existe une constante C dépendant de $a, b, \dots$ telle que pour tout x (dans un domaine indiqué ou explicite)

$$|f(x)| \leq Cg(x).$$

En particulier, il est sous-entendu que g ne prend pas de valeurs strictement négatives. Le symbole $\ll$ est appelé symbole de Vinogradov.

$f = O_{a,b,\dots}(g)$ a le même sens que $f \ll_{a,b,\dots} g$.

$f \leq g + O_{a,b,\dots}(h)$: il existe une fonction ℓ telle que

- 1) $f - g \leq \ell$;
- 2) $\ell = O_{a,b,\dots}(h)$.

Chapitre 1

Formes modulaires

Dans ce premier chapitre, on rappelle les résultats connus concernant les formes modulaires dont nous aurons besoin.

1.1 L'espace des formes modulaires

Dans tout ce rapport, $\mathcal{H}$ désigne le demi-plan de Poincaré

$$\mathcal{H} = \{z \in \mathbb{C}; \Im z > 0\}$$

et $\mathcal{H}^*$ désigne le demi plan de Poincaré complété

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Pour tout entier N , on note $\Gamma_0(N)$ le sous-groupe de congruence de $SL(2, \mathbb{Z})$ défini par

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}); c \equiv 0 \pmod{N} \right\}.$$

Ce groupe contient $-I$ et on a $\Gamma_0(1) = SL(2, \mathbb{Z})$. Le groupe $\Gamma_0(N) \backslash SL(2, \mathbb{Z})$ est fini. Son cardinal [Miy89, theorem 4.2.5] est

$$\nu(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

et la fonction ν est multiplicative.

Soit k un entier pair strictement positif. Le groupe $SL(2, \mathbb{Z})$ agit sur l'espace des fonctions holomorphes sur $\mathcal{H}$ grâce à l'action

$$f|_{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}(z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right). \quad (1.1)$$

On dit que f vérifie la *condition de modularité* sur un sous-groupe Γ de $SL(2, \mathbb{Z})$ si

$$f|_M = f \quad \text{pour toute matrice } M \in \Gamma.$$

Soit $M \in SL(2, \mathbb{Z})$, on définit

$$u_M = \inf\{u \in \mathbb{N}^* ; T^u \in M^{-1}\Gamma_0(N)M\}.$$

Si une fonction f holomorphe sur $\mathcal{H}$ vérifie la condition de modularité sur $\Gamma_0(N)$ alors $f|_M$ est périodique de période u_M et elle admet un développement de Fourier de la forme

$$f|_M(z) = \sum_{n \in \mathbb{Z}} \widehat{f}_M(n) e\left(\frac{nz}{u_M}\right) \quad (1.2)$$

convergent sur $\mathcal{H}$ et uniformément convergent sur tout compact de $\mathcal{H}$. On dit que f est *holomorphe aux pointes* si

$$\widehat{f}_M(n) = 0 \quad \text{pour toute } M \in SL(2, \mathbb{Z}) \text{ et tout } n < 0.$$

Une forme holomorphe sur $\mathcal{H}$, vérifiant la condition de modularité sur $\Gamma_0(N)$ et holomorphe aux pointes est une *forme modulaire* de poids k et de niveau N . Une telle forme qui vérifie la condition supplémentaire

$$\widehat{f}_M(0) = 0 \quad \text{pour toute } M \in SL(2, \mathbb{Z})$$

est une *forme parabolique de poids k et de niveau N* .

Si $M \in SL(2, \mathbb{Z})$ et si f est parabolique on déduit du développement (1.2) et du fait que $f|_M$ vérifie la condition de modularité sur $M^{-1}\Gamma_0(N)M$ qu'il existe une constante c telle que pour tout n strictement positif on a [Miy89, corollary 2.1.6]

$$|\widehat{f}_M(n)| \leq cn^{k/2}. \quad (1.3)$$

On en déduit l'existence, pour toute $M \in SL(2, \mathbb{Z})$, de constantes c et y_0 telles que si $y \geq y_0$ alors

$$|f|_M(iy)| \leq ce^{-2\pi y/u_M} \quad (1.4)$$

[Miy89, lemma 4.3.3]. Lorsque $M \in \Gamma_0(N)$ on a $u_M = 1$ et on écrira $\widehat{f}(m)$ au lieu de $\widehat{f}_M(m)$.

De façon équivalente [Miy89, theorem 2.1.5], une *forme parabolique* de poids k et de niveau N est une fonction $f : \mathcal{H} \rightarrow \mathbb{C}$ holomorphe sur $\mathcal{H}$ qui vérifie les conditions

1) condition de modularité : pour toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ et tout $z \in \mathcal{H}$ on a

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z);$$

2) la fonction $z \mapsto (\Im z)^{k/2} |f(z)|$ est bornée sur $\mathcal{H}$.

REMARQUE 1.1 La géométrie adaptée au traitement des régions de $\mathcal{H}^*$ impliquées ici est la géométrie de Lobatchevski-Poincaré [Efi81].

REMARQUE 1.2 Il existe une notion de forme modulaire sur des groupes plus généraux et avec des conditions de modularité moins contraignantes (voir par exemple [MR97]).

On note $S(N)$ l'ensemble des formes paraboliques de poids¹ k et de niveau N . Cet ensemble est un espace vectoriel sur $\mathbb{C}$ de dimension finie vérifiant

$$\dim S(k, N) \leq \left\lfloor \frac{\nu(N)k}{12} \right\rfloor$$

(une preuve élémentaire est donnée dans [MR97], une formule exacte de la dimension est donnée dans [Miy89, theorem 2.5.3] et on donnera une formule asymptotique au corollaire 1.7.7).

On appelle *domaine fondamentale* de $\Gamma_0(N)$ un ouvert $D_0(N)$ de $\mathcal{H}$ tel que

¹On note $S(k, N)$ lorsque qu'on veut préciser le poids. Souvent, il sera sous-entendu.

- 1) pour tout $z \in \mathcal{H}$, il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ telle que $\frac{az+b}{cz+d} \in \overline{D_0(N)}$;
- 2) si deux points de $D_0(N)$ sont équivalents² modulo $\Gamma_0(N)$ alors ils sont égaux.

Si f et g sont deux formes de $S(N)$, leurs développements de Fourier en l'infini assurent la convergence de l'intégrale

$$(f, g)_N = \int_{D_0(N)} f(z) \overline{g(z)} y^k \frac{dx dy}{y^2}.$$

La condition de modularité et l'invariance de la mesure $\frac{dx dy}{y^2}$ par homographie permettent de vérifier que cette intégrale ne dépend pas du choix du domaine fondamental. Elle définit un produit hermitien sur $S(N)$ appelé *produit de Petersson*³.

1.2 Opérateurs de Hecke

1.2.1 Polynômes de Tchebychef de seconde espèce Les polynômes de Tchebychef⁴ de seconde espèce ont une grande importance pour les opérateurs de Hecke. On donne leurs propriétés en terme de représentations [BD85, §II.5]. Les seuls résultats qu'on utilisera sont (1.6) qu'on peut prendre en définition et (1.7) qui se montre aussi par des calculs aveugles.

Soit n un entier. On note E^n l'espace des polynômes complexes homogènes de degré n à deux variables⁵. C'est un espace vectoriel de dimension $n+1$. On définit une représentation⁶ D^n du groupe $SU(2, \mathbb{C})$ dans E^n par

$$\begin{aligned} D^n : SU(2, \mathbb{C}) &\rightarrow GL(E^n) \\ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} &\mapsto P(X, Y) \mapsto P(aX - \bar{b}Y, bX + \bar{a}Y). \end{aligned}$$

On montre que les représentations D^n sont irréductibles et que toute représentation irréductible de $SU(2, \mathbb{C})$ est équivalente à l'une des représentations D^n . Les caractères irréductibles de $SU(2, \mathbb{C})$ sont donc les applications

$$\begin{aligned} \chi^n : SU(2, \mathbb{C}) &\rightarrow \mathbb{C} \\ g &\mapsto \text{tr } D^n g. \end{aligned}$$

Pour toute matrice $g \in SU(2, \mathbb{C})$, la valeur de $\chi^n(g)$ ne dépend que de la classe de conjugaison de g et g est conjuguée à une matrice

$$g_\varphi = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}$$

avec $\varphi \in [0, \pi]$. Il suffit donc de calculer $\chi^n(g_\varphi)$ pour caractériser χ^n . Pour ce faire, on remarque qu'une base de E^n est donnée par les polynômes⁷

$$P_n^k(X, Y) = X^{n/2-k} Y^{n/2+k}, \quad \left(k = -\frac{n}{2}, -\frac{n}{2} + 1, \dots, \frac{n}{2} \right).$$

On a alors

$$D^n g_\varphi (P_n^k) = e^{-2ik\varphi} P_n^k$$

²Deux points z et z' de $\mathcal{H}^*$ sont dits équivalents modulo $\Gamma_0(N)$ s'il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ tel que $\frac{az+b}{cz+d} = z'$.

³On notera (f, g) plutôt que $(f, g)_N$ quand il n'y aura pas d'ambiguïté sur le niveau.

⁴Appelés ainsi en l'honneur de P.L. Tchebychef qui a introduit des polynômes semblables en 1870 dans « Sur les fonctions analogues à celles de Legendre » [Tch62].

⁵Ces polynômes sont appelés *spinours*.

⁶Appelée représentation *spinorielle*.

⁷Il se peut que $\frac{n}{2}$ et k soient demi-entiers mais $\frac{n}{2} - k$ et $\frac{n}{2} + k$ sont entiers.

ainsi

$$\chi^n g_\varphi = \sum_{k=-n/2}^{n/2} e^{-2ik\varphi} = \frac{\sin(n+1)\varphi}{\sin \varphi}. \quad (1.5)$$

C'est un polynôme en $\text{tr } g_\varphi = 2 \cos \varphi$. On note X_n ce polynôme et on l'appelle *polynôme de Tchebychef de seconde espèce*. Il est caractérisé par l'égalité

$$X_n(2 \cos \varphi) = \frac{\sin(n+1)\varphi}{\sin \varphi}. \quad (1.6)$$

On note $\widetilde{SU(2, \mathbb{C})}$ l'ensemble des classes de conjugaison de $SU(2, \mathbb{C})$. On a une bijection donnée par la trace

$$\text{tr} : \widetilde{SU(2, \mathbb{C})} \xrightarrow{\sim} [-2, 2].$$

Une paramétrisation de $SU(2, \mathbb{C})$ est donnée par

$$g(\theta_1, \theta_2, \theta_3) = \begin{pmatrix} A(\theta_1, \theta_2, \theta_3) & B(\theta_1, \theta_2, \theta_3) \\ -\overline{B}(\theta_1, \theta_2, \theta_3) & \overline{A}(\theta_1, \theta_2, \theta_3) \end{pmatrix}$$

avec

$$A(\theta_1, \theta_2, \theta_3) = \cos \theta_3 + i \sin \theta_3 \cos \theta_2,$$

$$B(\theta_1, \theta_2, \theta_3) = \sin \theta_3 \sin \theta_2 \cos \theta_1 + i \sin \theta_3 \sin \theta_2 \sin \theta_1$$

et $\theta_1 \in [0, 2\pi]$, $\theta_2 \in [0, \pi]$ et $\theta_3 \in [0, \pi]$. Pour cette paramétrisation, la mesure de Haar de $SU(2, \mathbb{C})$ est

$$\mu_{SU(2, \mathbb{C})} = \frac{1}{2\pi^2} \sin^2 \theta_3 \sin \theta_2 \, d\theta_1 \, d\theta_2 \, d\theta_3.$$

Si f est une fonction centrale sur $SU(2, \mathbb{C})$, elle définit une fonction sur $\widetilde{SU(2, \mathbb{C})}$ de sorte qu'il existe $\tilde{f} : [-2, 2] \rightarrow \mathbb{C}$ telle que

$$f(g(\theta_1, \theta_2, \theta_3)) = \tilde{f}(\text{tr } g(\theta_1, \theta_2, \theta_3)).$$

On a $\text{tr } g(\theta_1, \theta_2, \theta_3) = 2 \cos \theta_3$ donc après intégration sur θ_1 et θ_2 on trouve

$$\begin{aligned} \int_{SU(2, \mathbb{C})} f \, d\mu_{SU(2, \mathbb{C})} &= \\ \frac{1}{\pi} \int_{\text{tr } g(\theta_1, \theta_2, \theta_3) = -2}^{\text{tr } g(\theta_1, \theta_2, \theta_3) = 2} \tilde{f}(\text{tr } g(\theta_1, \theta_2, \theta_3)) \sqrt{1 - \frac{1}{4} \text{tr}^2 g(\theta_1, \theta_2, \theta_3)} \, d\text{tr } g(\theta_1, \theta_2, \theta_3). \end{aligned}$$

Ainsi, l'image par l'application tr de la mesure de Haar de $SU(2, \mathbb{C})$ est la mesure de Sato-Tate sur $[-2, 2]$ donnée par

$$d\mu_\infty(x) = \frac{1}{\pi} \sqrt{1 - \frac{x^2}{4}} \, dx.$$

Les relations d'orthogonalité des caractères irréductibles donnent

$$\int_{SU(2, \mathbb{C})} \chi^n \chi^m \, d\mu_{SU(2, \mathbb{C})} = \delta(m, n)$$

ce qui s'exprime encore

$$\int_{-2}^2 X_n X_m \, d\mu_\infty = \delta(m, n). \quad (1.7)$$

On note que cette relation caractérise la mesure $d\mu_\infty$. En effet on vérifie par calcul que

$$X_n = xX_{n-1} - X_{n-2} \quad (1.8)$$

de sorte que la famille $(X_n)_{n \in \mathbb{N}}$ est échelonnée par rapport au degré. Elle forme donc une base de $\mathbb{R}[X]$. Par densité de $\mathbb{R}[X]$ dans l'espace des fonctions continues de $[-2, 2]$ dans $\mathbb{R}$ la relation (1.7) caractérise μ_∞ parmi les mesures positives de masse 1. On déduit aussi de (1.7) que pour tout $n \geq 0$

$$X^n = \sum_{i=0}^n h_n(i) X_i \quad (1.9)$$

avec

$$h_n(i) = \frac{2^{n+1}}{\pi} \int_0^\pi \cos^n \varphi \sin(i+1)\varphi \sin \varphi \, d\varphi. \quad (1.10)$$

On déduit de (1.5) que

$$\max_{x \in [-2, 2]} |X_n(x)| = X_n(2) = n+1. \quad (1.11)$$

On aura besoin d'une suite de mesures μ_q dont μ_∞ est limite, et définie pour tout réel $q \geq 1$ par

$$d\mu_q = \frac{q+1}{\pi} \frac{\sqrt{1-x^2/4}}{(q^{1/2} + q^{-1/2})^2 - x^2} dx$$

On a, pour tout $n \geq 0$ entier

$$\int_{-2}^2 X_n d\mu_q = \begin{cases} q^{-n/2} & \text{si } n \text{ est pair;} \\ 0 & \text{sinon.} \end{cases} \quad (1.12)$$

1.2.2 Définition des opérateurs de Hecke On définit sur l'espace des formes modulaires des opérateurs linéaires qui stabilisent $S(N)$, commutent entre eux et sont presque tous autoadjoints pour le produit scalaire de Petersson. On verra que ce « presque tous » est à l'origine de la théorie des formes nouvelles développée par Atkin et Lehner.

Soit $n \in \mathbb{N}$, on définit l'opérateur de Hecke⁸ T_n par

$$T_n : f \mapsto \frac{1}{n} \sum_{\substack{ad=n \\ (a,N)=1}} a^k \sum_{b=0}^{d-1} f\left(\frac{az+b}{d}\right).$$

On montre [Iwa97, theorem 6.16] que si f est une forme modulaire (resp. parabolique) il en est de même pour $T_n f$.

1.2.3 Propriétés des opérateurs de Hecke Les opérateurs de Hecke vérifient une relation de multiplicativité donnée par

$$T_m T_n = \sum_{\substack{d|(m,n) \\ (d,N)=1}} d^{k-1} T_{mn/d^2} \quad (1.13)$$

pour tous $m, n \geq 1$ [Iwa97, theorem 6.6]. Par utilisation de la relation de Möbius on vérifie que la relation (1.13) s'inverse en

$$T_{mn} = \sum_{\substack{d|(m,n) \\ (d,N)=1}} \mu(d) d^{k-1} T_{m/d} T_{n/d}. \quad (1.14)$$

⁸Hecke a établi les propriétés essentielles de ces opérateurs déjà utilisés par Hurwitz [Hec37].

Il en résulte que l'application arithmétique $n \mapsto T_n$ est multiplicative et que les opérateurs T_p avec $p \in \mathcal{P}$ suffisent à construire tous les opérateurs de Hecke. En particulier, si $(p, N) = 1$ et $n \geq 2$ on déduit de (1.14) la relation

$$\frac{1}{p^{n(k-1)/2}} T_{p^n} = \frac{1}{p^{(k-1)/2}} T_p \frac{1}{p^{(n-1)(k-1)/2}} T_{p^{n-1}} - \frac{1}{p^{(n-2)(k-1)/2}} T_{p^{n-2}}$$

ce qui prouve après comparaison avec la relation de récurrence (1.8) que pour tout $n \geq 0$ on a

$$X_n \left(\frac{1}{p^{(k-1)/2}} T_p \right) = \frac{1}{p^{n(k-1)/2}} T_{p^n} \quad (1.15)$$

puisque c'est vrai pour $n \in \{0, 1\}$.

L'action des opérateurs de Hecke sur les coefficients des formes paraboliques est donnée [Iwa97, proposition 6.3] dans la

PROPOSITION 1.2.1
Si

$$f(z) = \sum_{n=1}^{+\infty} \hat{f}(n) e(nz)$$

est une forme de $S(N)$ alors le m -ième coefficient de Fourier de la forme $T_n f$ est donné par

$$\widehat{T_n f}(m) = \sum_{\substack{d|(m,n) \\ (d,N)=1}} d^{k-1} \hat{f}\left(\frac{mn}{d^2}\right).$$

Enfin, les opérateurs de Hecke sont presque tous autoadjoints [Iwa97, theorem 6.20] au sens où, pour $(n, N) = 1$ on a

$$(T_n f, g) = (f, T_n g) \quad (1.16)$$

pour toutes $f, g \in S(N)$.

1.2.4 Valeurs propres Si $t_f(n)$ est la valeur propre de l'opérateur T_n associée au vecteur propre $f \in S(N)$ on note

$$\lambda_f(n) = \frac{1}{n^{(k-1)/2}} t_f(n).$$

L'équation (1.13) implique que pour tout p premier et tout entier $n \geq 0$ un vecteur propre de T_p est vecteur propre de T_{p^n} . Si de plus p ne divise pas N , (1.15) montre que

$$X_n(\lambda_f(p)) = \lambda_f(p^n), \quad (p, N) = 1. \quad (1.17)$$

On déduit de cette relation et de (1.9) la relation

$$\lambda_f(p)^n = \sum_{i=0}^n h_n(i) \lambda_f(p^i), \quad (p, N) = 1$$

avec $h_n(i)$ défini en (1.10). Si f est vecteur propre de tous les opérateurs T_d pour $d|mn$, l'équation (1.13) donne

$$\lambda_f(m) \lambda_f(n) = \sum_{\substack{d|(m,n) \\ (d,N)=1}} \lambda_f\left(\frac{mn}{d^2}\right). \quad (1.18)$$

Si $p|N$ et $n \geq 0$ on obtient

$$\lambda_f(p^n) = \lambda_f(p)^n. \quad (1.19)$$

Les valeurs propres des opérateurs de Hecke caractérisent les coefficients de Fourier des vecteurs propres. Ainsi, d'après la relation (1.13) et la proposition 1.2.1 avec $m = 1$ on a la

PROPOSITION 1.2.2

Soit

$$f(z) = \sum_{n=1}^{+\infty} \hat{f}(n) e(nz)$$

une forme de $S(N)$ vecteur propre de tous les opérateurs T_p pour p appartenant à P un ensemble donné de nombres premiers. On pose

$$T_p f = t_f(p) f.$$

Si n est un entier dont les facteurs premiers sont dans P alors f est un vecteur propre de T_n associé à la valeur propre $t_f(n)$ et on a

$$\hat{f}(n) = \hat{f}(1) t_f(n).$$

D'après (1.14) et (1.16), la famille d'opérateurs

$$\{T_n, (n, N) = 1\}$$

est une famille d'opérateurs normaux qui commutent deux à deux. Pour de telles familles, on a la⁹

PROPOSITION 1.2.3

Soit $\mathcal{E}$ un espace hermitien sur $\mathbb{C}$ et $\mathcal{F}$ une famille d'opérateurs normaux commutant deux à deux. Alors il existe une base orthonormale $\mathcal{B}$ de $\mathcal{E}$ formée de vecteurs propres de tous les opérateurs de $\mathcal{F}$.

On en déduit la

PROPOSITION 1.2.4

Il existe une base orthonormale de l'espace $S(N)$ formée de vecteurs propres de tous les opérateurs de Hecke T_n tels que $(n, N) = 1$.

La majoration des valeurs propres des opérateurs de Hecke a fait l'objet de recherches qui ont culminé¹⁰ avec les travaux de Deligne¹¹ [Del74, théorème 8.2]. Il prouve la

PROPOSITION 1.2.5

Soit p un nombre premier ne divisant pas N . Soit $t(p)$ une valeur propre de l'opérateur de Hecke T_p . Alors

$$|t(p)| \leq 2p^{(k-1)/2}.$$

Avec les notations du paragraphe 1.2.3 cette proposition entraîne¹²

$$|\lambda_f(p)| \leq 2$$

⁹Une preuve de cette proposition se trouve dans [Gan66, théorème 9.11].

¹⁰Ces recherches ne sont pas terminées dans le cas de formes modulaires plus générales que celles présentées ici.

¹¹Dans le cas du poids 2, ce résultat est dû à Eichler [Eic54], Shimura [Shi58] et Igusa [Igu59].

¹²On verra au paragraphe 3.1 que cette majoration est optimale.

pour $(p, N) = 1$ et f vecteur propre de T_p . On déduit de (1.17) et (1.11) que

$$|\lambda_f(p^n)| \leq n + 1.$$

Par multiplicativité on a alors

$$|\lambda_f(n)| \leq \tau(n), \quad (n, N) = 1. \quad (1.20)$$

Pour prouver la proposition 1.2.5, on montre qu'on peut écrire

$$\lambda_f(p) = \alpha_f(p) + \alpha_f(p)^{-1}, \quad (p, N) = 1$$

avec $|\alpha_f(p)| = 1$. Cette équation se généralise en

$$\lambda_f(p^i) = \frac{\alpha_f(p)^{i+1} - \alpha_f(p)^{-i-1}}{\alpha_f(p) - \alpha_f(p)^{-1}} \quad (p, N) = 1 \quad (1.21)$$

grâce à (1.18).

On utilisera aussi le théorème sur la nature algébrique des valeurs propres de Hecke dû à Shimura [Shi71, theorem 3.48]

THÉORÈME 1.2.6

Soit N et n deux entiers naturels. Les valeurs propres de l'opérateur de Hecke T_n agissant sur les formes paraboliques de niveau N sont des entiers algébriques.

1.3 Formes nouvelles et primitives

tous d'écrire est ensemble, éléments

1.3.1 Formes anciennes et nouvelles La proposition (1.2.2) permet d'affirmer que si f est vecteur propre de tous les opérateurs T_n , $(n, N) = 1$ alors

$$\widehat{f}(n) = \widehat{f}(1)t_f(n), \quad (n, N) = 1. \quad (1.22)$$

Cela ne suffit pas à dire¹³ que $\widehat{f}(1) \neq 0$. On peut même trouver des formes f vecteurs propres de tous les opérateurs T_n , $(n, N) = 1$ telles que $\widehat{f}(1) = 0$.

Soit L et M des entiers tels que $LM = N$. Soit $f \in S(M)$ et $f_L : z \mapsto f(Lz)$. On vérifie alors [Miy89, lemma 4.6.2] que pour tout $n \geq 0$ entier

$$\begin{cases} f_L \in S(N) \\ T_n f = t_f(n)f \Rightarrow T_n f_L = t_f(n)f_L \\ \widehat{f_L}(1) = 0. \end{cases}$$

On définit l'espace des *formes anciennes* par rapport à N comme

$$S^a(N) = \text{Vect}\{f_L ; f \in S(M), LM|N, M \neq N\}.$$

Cet espace est stable par tous les opérateurs T_n , $(n, N) = 1$ [Miy89, lemma 4.6.10].

On définit l'espace des formes *nouvelles* par rapport à N comme l'orthogonal de $S^a(N)$ dans $S(N)$:

$$S^n(N) = S^a(N)^\perp.$$

Le théorème d'Atkin-Lehner [Miy89, theorem 4.6.8] affirme

¹³On voudrait le dire pour construire des formes dont les coefficients sont les valeurs propres de Hecke.

THÉORÈME 1.3.1

Soit $f \in S(N)$ telle que

$$(n, N) = 1 \Rightarrow \widehat{f}(n) = 0.$$

Alors

$$f \in S^a(N).$$

On en déduit, (grâce à (1.22)) que si $f \in S^n(N)$ et si f est vecteur propre de tous les opérateurs de Hecke T_n , $(n, N) = 1$ alors $\widehat{f}(1) \neq 0$. Si g est une autre forme de $S^n(N)$ de mêmes valeurs propres on a

$$\left(g - \frac{\widehat{g}(1)}{\widehat{f}(1)}f\right)(n) = 0, \quad (n, N) = 1$$

et donc

$$g - \frac{\widehat{g}(1)}{\widehat{f}(1)}f \in S^n(N) \cap S^a(N)$$

de sorte que

$$g = \frac{\widehat{g}(1)}{\widehat{f}(1)}f.$$

L'ensemble des vecteurs propres des opérateurs T_n , $(n, N) = 1$ associés à un système de valeurs propres est donc une droite. Cela explique qu'on appelle aussi le théorème d'Atkin-Lehner théorème de multiplicité 1.

PROPOSITION 1.3.2

Soit $f \in S^n(N)$ avec $\widehat{f}(1) = 1$ et $T_n f = t(n)f$ pour tous $(n, N) = 1$. Si $g \in S^n(N)$ et $T_n g = t(n)g$ pour tous $(n, N) = 1$ alors $g \in \mathbb{C}f$.

1.3.2 Formes primitives Si f est vecteur propre de tous les opérateurs de Hecke T_n avec $(n, N) = 1$ et si $f \in S^n(N)$ on pose

$$f^{nor} = \frac{f}{\widehat{f}(1)}.$$

L'ensemble $B(N)$ des formes f^{nor} lorsque f parcourt une base orthogonale de $S^n(N)$ de vecteurs propres de tous les T_n , $(n, N) = 1$ est appelé ensemble des formes *primitives* de niveau N . Cet ensemble est une base orthogonale de $S^n(N)$. Elle est unique au sens où l'on a¹⁴ la

PROPOSITION 1.3.3

Soit $f \in S^n(N)$ telle que

$$1) \forall (n, N) = 1, \exists t(n) \in \mathbb{C}; T_n f = t(n)f;$$

$$2) \widehat{f}(1) = 1$$

alors $f \in B(N)$.

Démonstration – On pose $B(N) = \{f_1, \dots, f_g\}$. Soit f comme dans l'énoncé. On a

$$f = \sum_{i=1}^g \nu_i f_i$$

¹⁴Cette caractérisation prouve l'égalité des notions de forme primitive et de *forme de Hecke normalisée*.

avec $(\nu_i)_{1 \leq i \leq g} \in \mathbb{C}^g$. Puisque $f \neq 0$, on fixe j tel que $\nu_j \neq 0$. D'une part, les formes f_i étant vecteurs propres de T_n on a

$$T_n f = \sum_{i=1}^g \nu_i t_i(n) f_i$$

et d'autre part, f étant aussi vecteur propre de T_n on a

$$T_n f = \sum_{i=1}^g \nu_i t(n) f_i.$$

On a donc l'égalité $\nu_j t_j(n) = \nu_j t(n)$ puis $t(n) = t_j(n)$ de sorte que par la proposition 1.3.2 on a $f \in \mathbb{C} f_j$ puis $f = f_j$ car $\hat{f}(1) = \hat{f}_j(1) = 1$. $\square$

Enfin, la restriction $(n, N) = 1$ est superflue grâce à la

PROPOSITION 1.3.4

Soit $f \in B(N)$ alors f est vecteur propre de tous les opérateurs de Hecke et, pour tout entier $n \in \mathbb{N}^$ on a*

$$T_n f = \hat{f}(n) f.$$

La première partie de cet énoncé résulte de la commutativité des opérateurs de Hecke et de la proposition 1.3.2. La seconde partie résulte de la proposition 1.2.2.

On peut exprimer toute forme en fonction de formes primitives de niveau plus petit, en effet par définition, on a

$$S(N) = \bigoplus_{LM=N} \bigoplus_{f \in B(M)} \text{Vect}\{f_t, \ell|L\}. \quad (1.23)$$

1.4 Opérateurs d'Atkin-Lehner

Soit M un diviseur de N tel que $M \parallel N$. On définit sur $S(N)$ l'opérateur

$$W(M) : f \mapsto \left[z \mapsto M^{k/2} (Nz + Md)^{-k} f\left(\frac{Maz + b}{Nz + Md}\right) \right]$$

où

$$\begin{cases} (a, b, d) \in \mathbb{Z}^3 \\ d \equiv 1 \pmod{N/M} \\ M^2 ad - bN = M. \end{cases} \quad (1.24)$$

Un tel triplet existe et tous les triplets vérifiant (1.24) conduisent à la même définition de $W(M)$ [AL70, lemma 9]. Ces opérateurs sont multiplicatifs : si $M_1 \parallel M$, $M_2 \parallel M$ et $(M_1, M_2) = 1$ alors

$$W(M_1 M_2) = W(M_1) W(M_2).$$

Ce sont des isométries sur $S(N)$ stabilisant $S^n(N)$, qui commutent avec les opérateurs de Hecke T_n , $(n, N) = 1$ et sont autoadjointes [AL70, lemma 25]. On déduit de la proposition 1.3.4 que si $f \in B(N)$ alors il existe $\varepsilon_f(M) \in \mathbb{C}$ tel que

$$W(M) f = \varepsilon_f(M) f, \text{ avec } \varepsilon_f(M) \in \{-1, 1\}.$$

Si M est sans facteur carré, la valeur propre $\varepsilon_f(M)$ est reliée aux valeurs propres des opérateurs de Hecke par

$$\varepsilon_f(M) = \mu(M) \hat{f}(M) M^{1-k/2} = \mu(M) \sqrt{M} \lambda_f(M). \quad (1.25)$$

Enfin

$$p^2|N \Rightarrow \hat{f}(p) = 0. \quad (1.26)$$

Ces faits sont développés par exemple dans [Kna92, §IX.7]. On résume dans la proposition suivante les propriétés des coefficients de Fourier d'une forme primitive.

PROPOSITION 1.4.1

Soit $f \in B(N)$, soit m et n des entiers, soit p un nombre premier. On a

$$1) \quad \hat{f}(n) = t_f(n) = n^{(k-1)/2} \lambda_f(n);$$

2)

$$\hat{f}(n)\hat{f}(m) = \sum_{\substack{d|(m,n) \\ (d,N)=1}} d^{k-1} \hat{f}\left(\frac{mn}{d^2}\right);$$

$$3) \quad \text{s'il existe } p|n \text{ tel que } p^2|N \text{ alors } \hat{f}(n) = 0;$$

$$4) \quad \text{si } n \parallel N, \hat{f}(n) = \mu(n)n^{k/2-1} \varepsilon_f(n) \text{ avec } \varepsilon_f(n) \in \{-1, 1\};$$

$$5) \quad \hat{f}(n) \in \overline{\mathbb{Q}} \cap \mathbb{R};$$

$$6) \quad |\lambda_f(n)| \leq \tau(n).$$

second point résulte (1.13). Le troisième point est conséquence de quatrième point est (1.25). Le cinquième caractère autoadjoint des opérateurs T_n , $(n, N) = 1$. quatrième points et de la majoration de Deligne (1.20).

1.5 Action de Galois

Soit f un vecteur propre de tous les opérateurs de Hecke T_p où p décrit $\mathcal{P}$, on peut définir, grâce au théorème 1.2.6 le corps $\mathbb{Q}(f)$ comme le corps engendré par toutes les valeurs propres $t_p(f)$, $p \in \mathcal{P}$. C'est une extension algébrique de $\mathbb{Q}$ de degré fini [Shi71, theorem 3.48]. On peut alors donner la

DÉFINITION 1.5.1

Soit $\sigma \in \text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ et $f \in B(N)$. On pose

$$f^\sigma(z) = \sum_{n=1}^{+\infty} \sigma(\hat{f}(n)) e(nz).$$

Shimura [Shi72, proposition 1.2] a prouvé la

PROPOSITION 1.5.2

Soit $f \in B(N)$ et $\sigma \in \text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ alors $f^\sigma \in B(N)$.

On a un moyen de calculer le cardinal de l'orbite $\text{orbite}(f)$ sous $\text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ d'une forme primitive f grâce à la

PROPOSITION 1.5.3

Soit $f \in B(N)$ alors $\#\text{orbite}(f) = [\mathbb{Q}(f) : \mathbb{Q}]$.

Démonstration – Soit $f \in B(N)$. On a une bijection

$$\begin{array}{ccc} \text{Gal}(\mathbb{Q}(f)/\mathbb{Q}) & \xrightarrow{\sim} & \text{orbite}(f) \\ \sigma & \mapsto & f^\sigma. \end{array}$$

La surjectivité est évidente. Pour l'injectivité, deux morphismes de même image ont mêmes valeurs en les coefficients de f qui engendrent $\mathbb{Q}(f)$ et sont donc égaux.

On a alors $\# \text{orbite}(f) = \# \text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ puis, grâce au théorème fondamental de la théorie de Galois $\# \text{orbite}(f) = [\mathbb{Q}(f) : \mathbb{Q}]$. $\square$

En particulier, $[\mathbb{Q}(f) : \mathbb{Q}] \leq \dim S^n(N)$. D'autre part, Shimura a prouvé que $\mathbb{Q}(f)$ est totalement réel [Shi72, proposition 1.3]. Autrement dit, pour tout $n \in \mathbb{N}$ et tout $\sigma \in \text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ on a $\sigma(\hat{f}(n)) \in \mathbb{R}$. On résume ces propriétés dans le

THÉORÈME 1.5.4

Soit $f \in B(N)$. Le corps $\mathbb{Q}(f)$ engendré sur $\mathbb{Q}$ par les coefficients de Fourier de f est une extension algébrique totalement réelle et de degré fini de $\mathbb{Q}$. Son degré vérifie

$$[\mathbb{Q}(f) : \mathbb{Q}] = \# \text{orbite}(f) \leq \dim S^n(N).$$

1.6 Formes signées

Soit $\ell \in \mathbb{N}^*$. Si N est un entier sans facteur carré ayant exactement ℓ facteurs carrés on écrit

$$N = p_1 \cdots p_\ell, \quad p_1 < \cdots < p_\ell.$$

Grâce à la proposition 1.4.1, si $f \in B(N)$ alors $W(p_i)f = \varepsilon_f(p_i)f$ et, en posant

$$\varepsilon_f(N) = \varepsilon_f(p_1) \cdots \varepsilon_f(p_\ell). \quad (1.27)$$

on a $W(N)f = \varepsilon_f(N)f$.

DÉFINITION 1.6.1

Soit $N = p_1 \cdots p_\ell$ un entier avec $p_1 < \cdots < p_\ell$ premiers. On appelle signature de $f \in B(N)$ le vecteur $\varepsilon_f = (\varepsilon_f(p_1), \dots, \varepsilon_f(p_\ell))$ de $\{-1, 1\}^\ell$

Si on fixe $\varepsilon \in \{-1, 1\}^\ell$ on peut alors étudier les formes de signature ε .

DÉFINITION 1.6.2

Soit $N = p_1 \cdots p_\ell$ un entier avec $p_1 < \cdots < p_\ell$ premiers. Soit $\varepsilon \in \{-1, 1\}^\ell$. On définit l'ensemble des formes de signature ε et de niveau N par

$$B^\varepsilon(N) = \{f \in B(N); \varepsilon_f = \varepsilon\}.$$

La fonction caractéristique de $B^\varepsilon(N)$ est

$$\delta^\varepsilon(f) = \frac{1}{2^\ell} \prod_{i=1}^{\ell} [1 + \varepsilon_i \varepsilon_f(p_i)].$$

Grâce à (1.25), elle se récrit

$$\delta^\varepsilon(f) = \frac{1}{2^\ell} + \frac{1}{2^\ell} \sum_{i=1}^{\ell} (-1)^i \sum_{1 \leq j_1 < \cdots < j_i \leq \ell} \prod_{r \in \{j_1, \dots, j_i\}} \varepsilon_r \sqrt{p_r} \lambda_f(p_r). \quad (1.28)$$

On pose la

DÉFINITION 1.6.3

Soit N un entier sans facteur carré. On appelle ensemble des formes paires de niveau N l'ensemble

$$B^+(N) = \{f \in B(N); i^k \varepsilon_f(N) = +1\}.$$

et ensemble des formes impaires de niveau N l'ensemble

$$B^-(N) = \{f \in B(N); i^k \varepsilon_f(N) = -1\}.$$

La fonction caractéristique des formes paires (*resp.* impaires) est

$$\delta^+(f) = \frac{1}{2} + i^k \frac{\mu(N)\sqrt{N}}{2} \lambda_f(N)$$

resp.

$$\delta^-(f) = \frac{1}{2} - i^k \frac{\mu(N)\sqrt{N}}{2} \lambda_f(N).$$

On donne des estimations de la taille de ces ensembles au corollaire 1.7.8.

1.7 Formules de trace

1.7.1 Formule de Petersson Les formules de trace évaluent des sommes de valeurs propres d'opérateurs de Hecke. Elles expriment des relations « d'orthogonalité » entre ces valeurs¹⁵.

Petersson a établi une formule¹⁶ de ce type : celle-ci s'applique à des formes de norme 1 et elle fait donc apparaître un facteur de normalisation

$$\omega_N(f) = \frac{\Gamma(k-1)}{(4\pi)^{k-1}(f, f)_N}$$

dès que l'on somme sur une base orthogonale¹⁷. Ce facteur est appelé *facteur harmonique* (d'où les notions de somme harmonique, moyenne harmonique...). On choisit $H(N)$ une base orthogonale¹⁸ de $S(N)$.

THÉORÈME 1.7.1

Soit m et n des entiers strictement positifs

$$\sum_{f \in H(N)} \omega_N(f) \frac{\hat{f}(m)\hat{f}(n)}{(mn)^{(k-1)/2}} = \delta(m, n) + 2\pi i^k \sum_{r=1}^{+\infty} \frac{S(m, n, rN)}{rN} J_{k-1} \left(\frac{4\pi\sqrt{mn}}{rN} \right).$$

REMARQUE 1.3 La preuve repose sur le fait qu'on peut exprimer les coefficients de Fourier de f en fonction du produit de Petersson de f contre des séries dites de Poincaré qui engendrent $S(N)$. On trouvera les détails dans [Iwa97, §3.3].

Énoncée sous cette forme, la formule n'est utilisable que pour une base orthogonale de $S(N)$. On voudrait l'utiliser pour une base orthogonale de formes nouvelles. Lorsqu'il n'y a pas de formes anciennes, c'est immédiat : c'est par exemple le cas si $k \leq 10$ et N est premier. Un cas plus général a été donné par Iwaniec, Luo et Sarnak. Pour l'énoncer, on introduit l'opérateur Δ_N défini pour tous entiers strictement positifs m et n par

$$\Delta_N(m, n) = \delta(m, n) + 2\pi i^k \sum_{r=1}^{+\infty} \frac{S(m, n, rN)}{rN} J_{k-1} \left(\frac{4\pi\sqrt{mn}}{rN} \right). \quad (1.29)$$

On a alors le

¹⁵En fait, d'orthogonalité approchée. Les considérer comme de vraies relations d'orthogonalité peut conduire à manquer des phénomènes importants. Voir, par exemple [KMV00a].

¹⁶Les notions nécessaires concernant les sommes de Kloosterman $S(m, n; c)$ et les fonctions de Bessel J_{k-1} sont rappelées en annexe.

¹⁷En particulier, les formes primitives forment une base orthogonale du sous-espace $S^n(N)$ qui n'est pas normée.

¹⁸On prêtera attention au fait qu'on choisit une base de *toutes* les formes de $S(N)$ et pas uniquement des formes nouvelles.

THÉORÈME 1.7.2 (PROPOSITION 2.8 DE [ILS00])

Soit N un entier sans facteur carré. Soit f une forme de $B(N)$. Soit m et n deux entiers strictement positifs tels que $(m, N) = 1$ et $(n, N^2) | N$ alors

$$\sum_{f \in B(N)} \omega_N(f) \lambda_f(m) \lambda_f(n) = \frac{1}{N} \sum_{LM=N} \frac{\mu(L)M}{\nu((n, L))} \sum_{\ell | L^\infty} \frac{1}{\ell} \Delta_M(m\ell^2, n).$$

REMARQUE 1.4 À la place du poids harmonique $\omega_N(f)$, Iwaniec, Luo et Sarnak utilisent un poids qu'ils notent $Z_N(1, f)/Z(1, f)$. On déduit notre proposition grâce à leurs équations¹⁹ (2.36) et (2.50) qui donnent pour $f \in B(N)$ la formule

$$\frac{Z_N(1, f)}{Z(1, f)} = \frac{N(k-1)}{12} \omega_N(f). \quad (1.30)$$

REMARQUE 1.5 Le point de départ de la preuve, est la décomposition (1.23). Si $N = LM$ est sans facteur carré, on définit pour chaque forme $f \in B(M)$ et chaque diviseur d de L une forme

$$f_d(z) = \left(\frac{d}{\rho_f(d)} \right)^{1/2} \sum_{c \equiv d} \frac{\mu(c)}{\nu(c)} \lambda_f(c) \ell^{(k-1)/2} f(\ell z)$$

où

$$\rho_f(d) = \prod_{p|d} \left[1 - p \left(\frac{\lambda_f(p)}{p+1} \right)^2 \right].$$

L'ensemble $\{f_d, d|L\}$ est une base orthogonale de $\text{Vect}\{z \mapsto f(\ell z), \ell|L\}$ qu'on sait normaliser (voir le lemme 2.3.2). On en déduit le

LEMME 1.7.3 (LEMMA 2.7 DE [ILS00])

Soit N un entier sans facteur carré et m et n deux entiers strictement positifs tels que $(m, n, N) = 1$ et $(mn, N^2) | N$ alors

$$\Delta_N(m, n) = \sum_{LM=N} \sum_{f \in B(M)} \frac{\omega_M(f)}{\nu(L)\rho_f(L)} \frac{\lambda_f(m)\lambda_f(n)}{\nu((mn, L))}.$$

REMARQUE 1.6 Là encore, le poids d'[ILS00] est $Z_N(1, f)/Z(1, f)$. Mais, toujours grâce à leurs équations (2.36) et (2.50), on a pour $f \in B(M)$ la formule

$$\frac{Z_N(1, f)}{Z(1, f)} = \frac{N(k-1)}{12} \frac{\omega_M(f)}{\nu(L)\rho_f(L)}.$$

Le théorème 1.7.2 résulte alors du lemme 1.7.3 par inversion de Möbius.

On déduit du théorème 1.7.2 grâce à la majoration de Weil-Esternmann (A.13) l'estimation

LEMME 1.7.4 (COROLLARY 2.10 DE [ILS00])

Soit N un entier sans facteur carré et m et n deux entiers strictement positifs tels que $(m, N) = 1$ et $(n, N^2) | N$ alors

$$\begin{aligned} \sum_{f \in B(N)} \omega_N(f) \lambda_f(m) \lambda_f(n) &= \frac{\varphi(N)}{N} \delta(m, n) \\ &+ O\left(k^{-\frac{5}{6}} (mn)^{\frac{1}{4}} N^{-1} (n, N)^{-\frac{1}{2}} \tau(N)^2 \tau_3((m, n)) \ln(2mnN)\right). \end{aligned}$$

¹⁹Les méthodes utilisées pour prouver ces équations sont celles exposées au paragraphe 2.3.2.

On déduit de ce lemme que

$$\sum_{f \in B(N)} \omega_N(f) = 1 + O\left(\frac{2^{\omega(N)}}{p_1(N)}\right) \quad (1.31)$$

où $p_1(N)$ est le plus petit diviseur premier de N . Si N parcourt une suite d'entiers telle que $p_1(N) = o(2^{\omega(N)})$ alors (1.31) donne un opérateur de moyenne. Kowalski et Michel [KM99] puis Iwaniec, Luo et Sarnak [ILS00] ont montré comment enlever ce facteur harmonique. Ils prouvent notamment la

PROPOSITION 1.7.5 (PROPOSITIONS 2.11 ET 2.13 DE [ILS00])

Soit N un entier sans facteur carré et n un entier strictement positif tel que $(n, N^2) | N$. Alors

$$\begin{aligned} \sum_{f \in B(N)} \lambda_f(n) &= \frac{k-1}{12} \sum_{LM=N} \frac{\nu(L)M}{\nu((n, L))} \sum_{(m, M)=1} \frac{\Delta_M(m^2, n)}{m} \\ &= \frac{k-1}{12} \frac{\varphi(N)}{\sqrt{n}} \chi_N^\square(n) + O((n, N)^{-1/2} n^{1/6} (kN)^{2/3}). \end{aligned}$$

Choisissant $n = 1$ on déduit le

COROLLAIRE 1.7.6

Si N est sans facteur carré

$$\sharp B(N) = \dim S^n(N) = \frac{k-1}{12} \varphi(N) + O((kN)^{2/3}).$$

On déduit de (1.23) que

$$\dim S(N) = \sum_{LM|N} \tau(L) \sharp B(M).$$

Puisque N est sans facteur carré, on a $\tau * \varphi(N) = \nu(N)$ d'où l'on déduit le

COROLLAIRE 1.7.7

Si N est sans facteur carré

$$\begin{aligned} \dim S(N) &= \frac{k-1}{12} \nu(N) + O(k^{2/3} 2^{\omega(N)} \sigma_{2/3}(N)) \\ &= \frac{k-1}{12} \nu(N) + O((kN)^{2/3} N^\varepsilon) \end{aligned}$$

pour tout $\varepsilon > 0$, la constante ne dépendant que de ce ε .

Compte-tenu de (1.28), on déduit alors du lemme 1.7.4 les cardinaux des ensembles de formes signées dans le

COROLLAIRE 1.7.8

Soit N un entier pair sans facteur carré et $\varepsilon \in \{-1, 1\}^{\omega(N)}$. Alors

$$\sharp B^\varepsilon(N) = \frac{1}{2^{\omega(N)}} \frac{k-1}{12} \varphi(N) + O((k^4 N^5)^{1/6}),$$

$$\sharp B^+(N) = \frac{k-1}{24} \varphi(N) + O((k^4 N^5)^{1/6})$$

et

$$\sharp B^-(N) = \frac{k-1}{24} \varphi(N) + O((k^4 N^5)^{1/6}).$$

Les constantes sont absolues.

Soit une application $X : B(N) \rightarrow \mathbb{C}$ on définit la ε -moyenne harmonique de X par

$$M^\varepsilon(X) = \sum_{f \in B^\varepsilon} \omega_N(f) X(f).$$

On déduit de (1.28) que

$$M^\varepsilon(X) = \frac{1}{2^\ell} \left(M^h(X) + \sum_{i=1}^{\ell} \sum_{1 \leq j_1 < \dots < j_i \leq \ell} (-1)^{i \varepsilon_{j_1} \dots \varepsilon_{j_i}} \times \sqrt{p_{j_1} \dots p_{j_i}} M^h(\lambda_f(p_{j_1}) \dots \lambda_f(p_{j_i}) X) \right) \quad (1.32)$$

où M^h est la moyenne harmonique

$$M^h(X) = \sum_{f \in B(N)} \omega_N(f) X(f).$$

Les formules d'Iwaniec, Luo et Sarnak permettent aussi de calculer des formules de traces sur les formes signées.

PROPOSITION 1.7.9

Soit N un entier sans facteur carré. On considère la suite $p_1 < \dots < p_\ell$ de ses diviseurs premiers, ε un vecteur de $\{-1, 1\}^\ell$ et k un entier strictement positif. Alors pour tout entier $m \geq 2$ vérifiant $(m, N) = 1$ on a

$$\sum_{f \in B^\varepsilon(N)} \omega_N(f) \lambda_f(m) \ll_k \tau(N)^2 N^{-\frac{3}{4}} \ln(2N^2 m) m^{\frac{1}{4}}$$

la constante impliquée ne dépendant que de k .

Démonstration – Pour un entier i tel que $0 \leq i \leq \ell$, une suite $\mathbf{j} = (j_1, \dots, j_\ell)$ telle que $0 \leq j_1 < \dots < j_i \leq \ell$ on définit $N_{\mathbf{j}} = 1$ si $i = 0$ et $N_{\mathbf{j}} = p_{j_1} \dots p_{j_i}$ sinon. On a $N_{\mathbf{j}} | N$ et $(N_{\mathbf{j}}, m) = 1$. On utilise alors (1.32) pour conclure. $\square$

La taille harmonique des ensembles de formes de poids N et de signature ε est alors donnée par le

LEMME 1.7.10

Soit N un entier sans facteur carré ayant ℓ facteurs premiers distincts. On considère ε un vecteur de $\{-1, 1\}^\ell$ et k un entier strictement positif. Alors

$$\sum_{f \in B^\varepsilon(N)} \omega_N(f) = \frac{1}{2^\ell} \frac{\varphi(N)}{N} + O_k \left(\frac{\tau(N)^2 \ln N}{N} \right)$$

où la constante ne dépend que de k .

Démonstration – Cela résulte de (1.32) avec $X = 1$ à qui on applique le lemme 1.7.4 pour d'une part $m = n = 1$ et d'autre part $m = 1$ et $n = p_{j_1} \dots p_{j_i}$ où $p_1, \dots, p_\ell$ sont les diviseurs premiers de N . $\square$

1.7.2 Formule de Selberg Il existe une formule de trace, sans facteur harmonique, due à Selberg. Elle est moins utile car le terme d'erreur est plus important. On en aura besoin lorsque $k = 2$ dans la forme suivante due à Brumer [Bru95b]²⁰.

THÉORÈME 1.7.11 (PROPOSITION 2.8 DE [BRU95B])

Soit la fonction multiplicative α définie sur les premiers p par

$$\alpha(p) = \alpha(p^2) = -1, \quad \alpha(p^3) = 1 \text{ et } \alpha(p^r) = 0 \text{ si } r \geq 4.$$

On définit les fonctions β et γ par

$$\beta(m) = \begin{cases} \mu(a) & \text{si } m = a^2 ; \\ 0 & \text{sinon ;} \end{cases}$$

et

$$\gamma(m) = m \sum_{d|m} \frac{\alpha(d)}{d}.$$

Alors, pour tous entiers N, ℓ et m strictement positifs tels que $(N, m) = 1$ et $\ell || N$ on a la majoration

$$\begin{aligned} \mathrm{tr} T_m W_\ell|_{S^n(2, N)} &= \frac{1}{12} \chi_N^\square(m) \beta(\ell) \gamma\left(\frac{N}{\ell}\right) \\ &\quad + O((m + m^{1/2} N^{1/2}) \tau(N)^3 \tau(m) \ln^2(4mN)). \end{aligned}$$

Choisissant $m = \ell = 1$ on obtient le

COROLLAIRE 1.7.12

Soit N un entier, on a

$$\sharp B(2, N) = \dim S^n(2, N) = \frac{\gamma(N)}{12} + O(N^{1/2} \tau(N)^3 \ln^2(4N)).$$

REMARQUE 1.7 Ce résultat est plus précis que celui du corollaire 1.7.6 mais ne le contredit évidemment pas ; en effet, si N est sans facteur carré, $\gamma(N) = \varphi(N)$. On en déduit en particulier que pour tout $\varepsilon > 0$ on a

$$N^{1-\varepsilon} \ll_\varepsilon \sharp B(2, N) \ll N. \quad (1.33)$$

REMARQUE 1.8 Lorsque $k > 2$, la formule de Selberg (que nous n'utiliserons pas ici) donne (voir [Ser97, §§4 et 5])

$$\dim S(k, N) = \frac{k-1}{12} \nu(N) + O(N^{1/2+\varepsilon})$$

et

$$\dim S^n = \frac{k-1}{12} \gamma(N) + O(N^{1/2+\varepsilon})$$

avec des constantes ne dépendant que d' ε et γ défini au théorème 1.7.11.

On déduit du théorème 1.7.11 la

PROPOSITION 1.7.13

Pour tous entiers strictement positifs N et m on a la majoration :

$$\sum_{f \in B(2, N)} \varepsilon_f(N) \lambda_f(m) \ll (m^{1/2} + N^{1/2})(mN)^\varepsilon.$$

La constante impliquée par le symbole de Vinogradov ne dépend que de ε .

²⁰Pour les poids supérieurs, on peut se reporter à [Ser97].

Démonstration – Dans le cas où m et N sont premiers entre eux la somme impliquée dans notre proposition n'est autre que la trace de $\frac{1}{\sqrt{m}}T_m W_N$ car les opérateurs autoadjoints W_N et T_m commutent et sont simultanément diagonalisables. Notre démarche va donc consister à nous ramener au résultat de Brumer. On écrit $m = m_1 m_2$ avec

$$m_1 = \prod_{\substack{p|m \\ p \nmid N}} p^{v_p(m)} \quad \text{et} \quad m_2 = \prod_{p|(m,N)} p^{v_p(m)}. \quad (1.34)$$

Grâce à (1.19) on a

$$\lambda_f(m_2) = \prod_{p|(m,N)} \lambda_f(p)^{v_p(m)}.$$

Lorsqu'il existe p divisant m tel que p^2 divise N on a $\lambda_f(m_2) = 0 = \lambda_f(m)$ grâce à la proposition 1.4.1 et la proposition 1.7.13 est prouvée. On suppose désormais que si $p|(m, N)$ alors $p \nmid N$. Sous cette hypothèse on a grâce à la proposition 1.4.1

$$\lambda_f(m_2) = \prod_{\substack{p|m \\ p \nmid N}} \left(-p^{-1/2} \varepsilon_f(p) \right)^{v_p(m)}. \quad (1.35)$$

On a alors, grâce à (1.18) et (1.35)

$$\lambda_f(m) = m_2^{-1/2} \lambda_f(m_1) \prod_{\substack{p|m \\ p \nmid N}} \left(-\varepsilon_f(p) \right)^{v_p(m)}. \quad (1.36)$$

On écrit $N = N_1 N_2 N_3$ avec

$$N_1 = \prod_{\substack{p|N \\ p \nmid m}} p^{v_p(m)}, \quad N_2 = \prod_{\substack{p|N \\ p|m \\ v_p(m) \text{ pair}}} p \quad \text{et} \quad N_3 = \prod_{\substack{p|N \\ p|m \\ v_p(m) \text{ impair}}} p.$$

Alors, puisque $\varepsilon_f(p) \in \{-1, 1\}$ on a

$$\varepsilon_f(N_2 N_3) \prod_{\substack{p|N \\ p|m}} \varepsilon_f(p)^{v_p(m)} = \varepsilon_f(N_2).$$

Ainsi

$$\varepsilon_f(N) \lambda_f(m) = \pm m_2^{-1/2} \varepsilon_f(N_1 N_2) \lambda_f(m_1). \quad (1.37)$$

On a $(m_1, N_1 N_2) = 1$. Les opérateurs autoadjoints T_{m_1} et $W_{N_1 N_2}$ commutent donc et la sommation de (1.37) sur $B(2, N)$ donne

$$\pm \sum_{f \in B(2, N)} \varepsilon_f(N) \lambda_f(m) = m^{-1/2} \text{tr } W_{N_1 N_2} T_{m_1}|_{S^n(2, N)}. \quad (1.38)$$

On conclut grâce au théorème 1.7.11. $\square$

On en déduit aussi la

PROPOSITION 1.7.14

Pour tout entier m et N et tout réel $\varepsilon > 0$ on a la majoration :

$$\frac{1}{\sqrt{m}} \text{tr } T_m|_{S^n(2, N)} - \sharp B(2, N) \chi_N^\square(m) m^{-1/2} \ll (m^{1/2} + N^{1/2})(mN)^\varepsilon.$$

La constante impliquée ne dépend que de ε .

Démonstration – • Si $(m, N) = 1$, le théorème 1.7.11 donne

$$\frac{1}{\sqrt{m}} \operatorname{tr} T(m)|_{S^n(2, N)} - \frac{m^{-1/2}}{12} \chi_N^\square(m) \gamma(N) \ll_\varepsilon (m^{1/2} + N^{1/2})(Nm)^\varepsilon \quad (1.39)$$

On obtient le résultat grâce au corollaire 1.7.12.

• Si $(m, N) > 1$, on décompose $m = m_1 m_2$ comme en (1.34). On a alors comme en (1.36) :

$$\lambda_f(m) = \pm \lambda_f(m_1) \varepsilon_f(N') m_2^{-1/2}$$

avec

$$N' = \prod_{\substack{p \parallel N \\ p \mid m \\ v_p(m) \text{ impair}}} p.$$

On a alors :

$$\frac{1}{\sqrt{m}} \operatorname{tr} T(m)|_{S^n(2, N)} = m^{-1/2} \operatorname{tr} T(m_1) W_{N'}|_{S^n(2, N)}.$$

Puisque $(m_1, N) = 1$, $N' \parallel N$ et $\beta(N') = 0$ le théorème 1.7.11 permet de conclure. $\square$

Chapitre 2

Fonctions L

Dans ce deuxième chapitre, on rappelle les résultats connus concernant les fonctions L de formes modulaires dont on aura besoin.

La théorie des fonctions L permet de coder et décoder des informations de nature arithmétique ou géométrique à l'aide des outils de l'analyse complexe. La liste des résultats obtenus par cette théorie est très longue. Citons uniquement le résultat récent de Cogdell, Piatetski-Shapiro et Sarnak prouvé par des techniques fines d'étude des fonctions L [IS00].

THÉORÈME

Soit K un corps de nombres totalement réel d'anneau des entiers O_K . Soit $n \in O_K$ sans facteur carré. Si n est assez grand et représentable partout localement comme somme de trois carrés alors il est représentable comme somme de trois carrés de O_K .

2.1 Présentation générale

Soit ϖ un objet de nature arithmético-géométrique¹ lié à un corps de nombres K . On suppose qu'à chaque idéal premier $\mathfrak{p}$ de l'anneau des entiers $\mathcal{O}_K$ de K est lié un objet $\varpi_{\mathfrak{p}}$ issu de ϖ . La fonction L de ϖ est définie par le produit eulérien

$$L(\varpi, s) = \prod_{\mathfrak{p}} L(\varpi_{\mathfrak{p}}, s)$$

où $L(\varpi_{\mathfrak{p}}, s)^{-1}$ est un polynôme en $N(\mathfrak{p})^{-s}$, $N(\mathfrak{p})$ étant la norme de $\mathfrak{p}$. On suppose qu'il existe un entier d_{ϖ} tel que chacun de ces polynômes est de degré inférieur ou égal à d_{ϖ} avec égalité sauf en un nombre fini de $\mathfrak{p}$.

On suppose que le produit converge et définit une fonction holomorphe pour $\Re s > 1$. Il peut se développer en une somme sur les idéaux entiers

$$L(\varpi, s) = \sum_{\mathfrak{n}} \lambda_{\varpi}(\mathfrak{n}) N(\mathfrak{n})^{-s}.$$

La fonction $L(\varpi, s)$ est donc définie par les propriétés locales de ϖ . On espère que ces propriétés locales sont reliées entre elles de façon non triviale grâce à une équation fonctionnelle. Pour exprimer cette équation on introduit un facteur *à la place infinie*

$$L(\varpi_{\infty}, s) = \prod_{j=1}^{d_{\varpi}} \Gamma_{\infty}(s - \mu_{j, \varpi})$$

¹On pourrait aussi présenter les fonctions L de façon purement analytique. C'est la démarche suivie dans l'axiomatique de Selberg [Sel92].

où les nombres $\{\mu_{j,\varpi}\}_{1 \leq j \leq d_\varpi}$ sont déterminés par ϖ et la fonction Γ_∞ est donnée par

$$\Gamma_\infty(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right).$$

On suppose que l'objet ϖ détermine aussi un objet (dit objet *dual*) $\tilde{\varpi}$, un réel q_ϖ appelé *conducteur* et un complexe de norme 1 appelé (abusivement) *signe* de l'équation fonctionnelle et noté ε_ϖ de sorte que

$$L(\varpi_\infty, s)L(\varpi, s) = \varepsilon_\varpi q_\varpi^{-s+1/2} L(\tilde{\varpi}_\infty, 1-s)L(\tilde{\varpi}, 1-s)$$

Enfin, on suppose disposer d'un prolongement méromorphe de $L(\varpi, s)$ à $\mathbb{C}$. On a alors l'inégalité de Lindelöf

$$L\left(\varpi, \frac{1}{2} + it\right) \ll_\varepsilon [(|t| + 1)^{d_\varpi} (\lambda_\varpi + 1) q_\varpi]^{1/4+\varepsilon}$$

la constante ne dépendant que de ε . On a posé

$$\lambda_\varpi = \left[\sum_{j=1}^{d_\varpi} |\mu_{j,\varpi}|^2 \right]^{1/2}.$$

Pour T assez grand, on a

$$\begin{aligned} \#\{\rho; L(\varpi, \rho) = 0, 0 \leq \Re \rho \leq 1, 0 \leq \Im \rho \leq T\} \\ = \frac{d_\varpi}{2\pi} T \ln T + c_\varpi T + O(\ln T) \end{aligned} \quad (2.1)$$

pour une constante c_ϖ . Un problème de la théorie des nombres est l'hypothèse de Riemann généralisée.

CONJECTURE 2.1.1

Les zéros de la fonction $L(\varpi_\infty, s)L(\varpi, s)$ sont tous de partie réelle $\frac{1}{2}$.

Cette conjecture aux multiples conséquences est qualifiée par Iwaniec et Sarnak de « quintessence de ce qu'une bonne conjecture devrait être ».

2.2 Fonctions L de formes primitives

2.2.1 Définition Soit k un entier fixé dans toute la suite. Soit $N \geq 1$ un entier et $f \in B(N)$. À tout nombre premier p on associe le facteur $L(f_p, s)$ défini par

$$L(f_p, s) = \begin{cases} (1 - \lambda_f(p)p^{-s} + p^{-2s})^{-1} & \text{si } (p, N) = 1; \\ (1 - \lambda_f(p)p^{-s})^{-1} & \text{si } p|N. \end{cases}$$

On prolonge à l'ensemble des nombres premiers la fonction α_f (définie page 8) et on définit la fonction β_f en posant

$$L(f_p, s) = (1 - \alpha_f(p)p^{-s})^{-1} (1 - \beta_f(p)p^{-s})^{-1}$$

pour tout premier. On a donc

$$\alpha_f(p) = \lambda_f(p) = -\varepsilon_f(p)p^{-1/2} \text{ si } p|N$$

et

$$\beta_f(p) = \begin{cases} \alpha_f(p)^{-1} & \text{si } (p, N) = 1; \\ 0 & \text{si } p|N. \end{cases}$$

On a alors $d_f = 2$ et la fonction L de f est donnée par

$$L(f, s) = \prod_p L(f_p, s). \quad (2.2)$$

Grâce à la majoration de Deligne (1.20) ce produit converge pour $\Re s > 1$. Grâce à la relation de multiplicativité (1.18) ce produit se développe en la série

$$\begin{aligned} L(f, s) &= \sum_{n=1}^{+\infty} \widehat{f}(n) n^{(k-1)/2} n^{-s} \\ &= \sum_{n=1}^{+\infty} \lambda_f(n) n^{-s}. \end{aligned} \quad (2.3)$$

On introduit le facteur à la place infinie

$$\begin{aligned} L(f_\infty, s) &= \Gamma_\infty\left(s + \frac{k-1}{2}\right) \Gamma_\infty\left(s + \frac{k-1}{2} + 1\right) \\ &= 2(2\pi)^{-(k-1)/2} (2\pi)^{-s} \Gamma\left(s + \frac{k-1}{2}\right) \end{aligned}$$

grâce à la relation de Legendre. Si $\Re s > 1$, une intégration terme à terme donne

$$L(f_\infty, s) L(f, s) = 2 \int_0^{+\infty} f(iv) v^{s+(k-1)/2} \frac{dv}{v} \quad (2.4a)$$

$$\begin{aligned} &= 2 \int_1^{+\infty} f(iv) v^{s+(k-1)/2} \frac{dv}{v} \\ &\quad + 2i^k \int_1^{+\infty} f|_S(iv) v^{-s+(k-1)/2} \frac{dv}{v}. \end{aligned} \quad (2.4b)$$

Grâce à (1.4) et (2.4b) on peut alors prolonger $L(f_\infty, s)L(f, s)$ – et donc $L(f, s)$ – en fonction entière. D'autre part, si f est primitive, $(\sqrt{N}z)^{-k} f(-1/Nz) = \varepsilon_f(N) f(z)$ et grâce à (2.4a) on obtient l'équation fonctionnelle

$$L(f_\infty, s) L(f, s) = i^k \varepsilon_f(N) N^{-s+1/2} L(f_\infty, 1-s) L(f, 1-s) \quad (2.5)$$

où $\varepsilon_f(N)$ est la valeur propre d'Atkin-Lehner associée à f . Le conducteur de f est donc N .

REMARQUE 2.1 L'équation (2.3) définit $L(f, s)$ pour toute forme parabolique. On obtient encore une série convergente pour $\Re s > 1$. On associe alors à f l'objet dual $W(N)f$ et le même facteur à l'infini pour obtenir une équation fonctionnelle qui n'est plus symétrique. Cette série ne se développe plus en produit eulérien.

2.2.2 Zéros des fonctions L de formes primitives On déduit de (2.4a)

$$\overline{L(f, s)} = L(f, \bar{s}). \quad (2.6)$$

Les zéros de $L(f, s)$ sont donc symétriques par rapport à l'axe réel. Grâce à l'équation fonctionnelle (2.5), ils sont aussi symétriques par rapport à l'axe $\Re s = \frac{1}{2}$. Soit p un nombre premier. Puisque $\lambda_f(p)$ est réel, les racines de $1 - \lambda_f(p)X + X^2$ sont complexes conjuguées et donc de norme 1. Ainsi, lorsque $\Re s > 0$, $1 - \lambda_f(p)p^{-s} + p^{-2s} \neq 0$ et grâce à son développement eulérien (2.2), la fonction $L(f, s)$ n'a pas de zéro dans la région $\Re s > 1$. Grâce à l'équation fonctionnelle (2.5), on déduit que les

zéros dans la bande $\Re s < 0$ sont les points $-n - \frac{k-1}{2}$, $n \in \mathbb{N}$. Ces zéros sont appelés *zéros triviaux*. Ainsi, tous les zéros non triviaux de $L(f, s)$ sont dans la *bande critique* $0 \leq \Re s \leq 1$.

L'hypothèse de Riemann permet d'évaluer des moyennes sur les nombres premiers des coefficients d'une forme primitive. On aura besoin de la

PROPOSITION 2.2.1

Supposons vraie l'hypothèse de Riemann pour les fonctions L de formes primitives. Soit N un entier et $f \in B(N)$. Soit $Q \geq 2$. On a

$$\sum_{p \leq Q} \frac{\lambda_f(p) \ln p}{\sqrt{p}} \ll \ln^3(kNQ).$$

La constante ne dépend ni de Q ni de N ni de k .

Démonstration – La fonction $L'(f, s)/L(f, s)$ est holomorphe sur $\Re s > 1/2$. Par dérivation logarithmique de (2.2) on a

$$-\frac{L'(f, s)}{L(f, s)} = \sum_{n=1}^{+\infty} b_f(n) \Lambda(n) n^{-s} \quad (\Re s > 1) \quad (2.7)$$

avec

$$b_f(n) = \begin{cases} 0 & \text{si } \Lambda(n) = 0; \\ \alpha_f(p)^m + \alpha_f(p)^{-m} & \text{si } n = p^m \text{ avec } (p, N) = 1 \text{ et } m > 0; \\ \lambda_f(p^m) & \text{si } n = p^m \text{ avec } p|N \text{ et } m > 0. \end{cases}$$

On évalue déjà

$$\sum_{p \leq Q} \lambda_f(p) \ln p = \sum_{p \leq Q} b_f(p) \Lambda(p).$$

Grâce à l'équation fonctionnelle et à l'inégalité de Phragmén-Lindelöf on a, pour $\sigma > 1/2$ et $t \geq 2$ l'inégalité

$$\ln |L(f, \sigma + it)| \leq O(\ln(|t|kN)). \quad (2.8)$$

Puisque la fonction $\omega \mapsto L(f, 2+it+\omega)/L(f, 2+it)$ est holomorphe pour $|\omega| < 3/2$ et prend la valeur 1 en 0, on choisit F une détermination holomorphe du logarithme de cette fonction telle que $F(0) = 0$. On a $\Re F(\omega) = \ln |L(f, 2+it+\omega)| - \ln |L(f, 2+it)|$. Grâce au développement eulérien (2.2) et à la majoration de Deligne (1.20) on a

$$-\ln |L(f, 2+it)| \leq \sum_{p \in \mathcal{P}} \ln \left(1 + \frac{9}{4p^2} \right) = O(1).$$

Ainsi, avec (2.8) on a

$$\Re F(\omega) \leq O(\ln(|t|kN)).$$

Par le lemme de Borel-Carathéodory [Ten95, §II.3.6, corollaire 11.1] on déduit pour tout $\varepsilon \in]0, 1/2[$ l'inégalité

$$F(\omega) \ll \frac{3}{\varepsilon} \ln(|t|kN), \quad |\omega| < \frac{3}{2} - \varepsilon.$$

On en déduit

$$\frac{L'(f, \sigma + it)}{L(f, \sigma + it)} \ll \frac{3}{\varepsilon} \ln(|t|kN), \quad \frac{1}{2} + \varepsilon \leq \sigma < 2$$

grâce à l'inégalité de Cauchy. Pour $Q \geq 2$, $T \geq 2$ et $\kappa = 1 + \ln^{-1} Q$, la seconde formule de Perron effective [Ten95, §II.2.2, corollaire 2.1] donne alors

$$\sum_{n \leq Q} b_f(n) \Lambda(n) = -\frac{1}{2i\pi} \int_{\kappa-iT}^{\kappa+iT} \frac{L'(f, s)}{L(f, s)} Q^s \frac{ds}{s} + O\left(\left(1 + \frac{Q}{T} \ln(QT)\right) \ln Q\right).$$

Si $\mathcal{C}$ est le chemin formé des droites reliant les points

$$\kappa - iT, \frac{1}{2} + \ln^{-1} Q - iT, \frac{1}{2} + \ln^{-1} Q + iT, \kappa + iT$$

le théorème des résidus donne

$$\sum_{n \leq Q} b_f(n) \Lambda(n) = -\frac{1}{2i\pi} \int_{\mathcal{C}} \frac{L'(f, s)}{L(f, s)} Q^s \frac{ds}{s} + O\left(\left(1 + \frac{Q}{T} \ln(QT)\right) \ln Q\right).$$

On choisit $\varepsilon = 1/\ln(kNQ)$. La contribution des lignes horizontales de $\mathcal{C}$ est en $O(QT^{-1} \ln(TN) \ln(kNQ))$ et celle de la verticale en $O(Q^{1/2} \ln(TN) \ln(kNQ))$ d'où, après avoir choisi $Q = T$ on trouve

$$\sum_{n \leq Q} b_f(n) \Lambda(n) \ll Q^{1/2} \ln^2(kNQ).$$

Or

$$\sum_{n \leq Q} b_f(n) \Lambda(n) = \sum_{p \leq Q} b_f(p) \ln p + \sum_{j=2}^{\ln Q / \ln 2} \sum_{p \leq Q^{1/j}} b_f(p^j) \ln p$$

d'où

$$\sum_{p \leq Q} \lambda_f(p) \ln(p) = \sum_{p \leq Q} b_f(p) \ln p \ll Q^{1/2} \ln^2(kNQ).$$

On obtient le résultat énoncé par intégration par parties

$$\begin{aligned} \sum_{p \leq Q} \lambda_f(p) \frac{\ln p}{\sqrt{t}} &= \left[\frac{1}{\sqrt{p}} \sum_{p \leq t} \lambda_f(p) \ln p \right]_2^Q \\ &\quad + \int_2^Q t^{-3/2} \sum_{p \leq t} \lambda_f(p) \ln p \, dt = O(\ln^3(kNQ)). \end{aligned}$$

□

Soit $\phi \in \mathcal{S}(\mathbb{R})$ paire² et de transformée de Fourier

$$\widehat{\phi}(\xi) = \int_{\mathbb{R}} \phi(x) e(-x\xi) \, dx$$

à support compact $[-R, R]$. On définit pour tout complexe s la fonction

$$\Phi(s) = \int_{\mathbb{R}} \widehat{\phi}(x) e(xs) \, dx.$$

Grâce au théorème d'inversion de Fourier, on a

$$\Phi|_{\mathbb{R}} = \phi.$$

²On dit que ϕ est une fonction de Schwartz, ce qu'on note $\phi \in \mathcal{S}(\mathbb{R})$, si ϕ est infiniment dérivable sur $\mathbb{R}$ et si, pour tous entiers n et ℓ , $0 \leq n \leq \ell$, $x \mapsto (1+x^2)^\ell \phi^{(n)}(x)$ est bornée sur $\mathbb{R}$.

Puisque $\hat{\phi}$ est infiniment dérivable à support compact alors Φ est entière et, pour tout n entier positif on a [Rud95, théorème 7.22] la majoration

$$|\Phi(s)| \ll_n (1 + |s|)^{-n} e^{R|\Im s|}. \quad (2.9)$$

Puisque Φ est un prolongement de ϕ , on la note ϕ . Soit alors $f \in B(N)$. On note $\{\rho_f = \beta_f + i\gamma_f\}$ la suite des zéros non triviaux de $L(f, s)$ répétés avec multiplicité. On introduit l'opérateur de comptage

$$D(f, \phi) = \sum_{\rho_f} \phi \left(\left(\beta_f - \frac{1}{2} + i\gamma_f \right) \frac{\ln(k^2 N)}{2i\pi} \right).$$

REMARQUE 2.2 Si l'on suppose vraie l'hypothèse de Riemann pour $L(f, s)$, cet opérateur devient

$$D(f, \phi) = \sum_{\rho_f} \phi \left(\gamma_f \frac{\ln(k^2 N)}{2\pi} \right).$$

D'après (2.9) on a

$$\phi \left(\left(\beta_f - \frac{1}{2} + i\gamma_f \right) \frac{\ln(k^2 N)}{2i\pi} \right) \ll (1 + |\gamma_f|)^{-2}$$

de sorte que

$$D(f, \phi) \ll \sum_{n \in \mathbb{N}^*} n^{-2} \#\{\gamma_f \in [n, n+1]\} \ll 1$$

grâce à (2.1), les constantes ne dépendant que de k et N .

L'évaluation de l'opérateur de comptage se fait grâce à la formule de Riemann³ donnée dans la

PROPOSITION 2.2.2

Soit $\phi \in \mathcal{S}(\mathbb{R})$ paire et de transformée de Fourier à support compact. Elle se prolonge en une fonction entière toujours notée ϕ . Soit $f \in B(k, N)$. On a

$$\begin{aligned} D(f, \phi) &= \hat{\phi}(0) + \frac{1}{2} \phi(0) - \sum_{\substack{p \in \mathcal{P} \\ (p, N)=1}} \lambda_f(p) \hat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} \\ &\quad - \sum_{\substack{p \in \mathcal{P} \\ (p, N)=1}} \lambda_f(p^2) \hat{\phi} \left(\frac{2 \ln p}{\ln(k^2 N)} \right) \frac{2 \ln p}{p \ln(k^2 N)} + O \left(\frac{\ln \ln(3N)}{\ln(k^2 N)} \right). \end{aligned}$$

REMARQUE 2.3 L'intérêt de cette formule est de ramener un dénombrement des zéros – délicat puisqu'on ne les connaît pas – à une évaluation de sommes finies de coefficients de formes primitives. Cette dernière évaluation est d'autant plus délicate que le support de $\hat{\phi}$ est grand.

Démonstration –⁴ On pose

$$G(s) = \phi \left(\left(s - \frac{1}{2} \right) \frac{\ln(k^2 N)}{2i\pi} \right).$$

³Appelée ainsi parce que Riemann a prouvé une formule de même type pour la fonction ζ [Rie59].

⁴Une preuve d'un résultat semblable dans le cas général du paragraphe 2.1 est donnée par Rudnick et Sarnak dans [RS96, proposition 2.1].

On veut évaluer

$$D(f, \phi) = \sum_{\rho_f} G(\rho_f).$$

Grâce à (2.9) on a

$$s^2 G(s) \ll_{k,N} 1 \quad |\sigma| \leq 3 \quad (2.10)$$

et par parité de ϕ on a

$$G(s) = G(1-s).$$

Soit $M > 2$. On note $\mathcal{R}_M$ le rectangle dont les sommets sont les points $2 - iM$, $2 + iM$, $-1 + iM$ et $-1 - iM$. On note $\mathcal{F}_M$ la frontière de ce rectangle. On note

$$\Lambda(s) = N^{s/2} L(f_\infty, s) L(f, s).$$

Les zéros de cette fonction sont les zéros non triviaux de $L(f, s)$ et, par (2.5) on a

$$\Lambda(s) = i^k \varepsilon_f(N) \Lambda(1-s).$$

On applique la formule des résidus à $G(s) \frac{\Lambda'(s)}{\Lambda(s)}$ pour obtenir ⁵

$$\sum_{\rho \in \mathcal{R}_M} G(\rho) = \frac{1}{2i\pi} \int_{\mathcal{F}_M} G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds.$$

Par symétrie $s \mapsto 1-s$ on a

$$\int_{2-iM}^{2+iM} G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds - \int_{-1-iM}^{-1+iM} G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds = \int_{2-iM}^{2+iM} 2G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds.$$

On montre maintenant que

$$\lim_{M \rightarrow +\infty} \int_{2-iM}^{2+iM} G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds = 0. \quad (2.11)$$

Par (2.10) on a

$$\begin{aligned} \int_M^{+\infty} \left| G(2+it) \frac{\Lambda'(2+it)}{\Lambda(2+it)} \right| dt &\ll_{k,N} \int_M^{+\infty} \left| \frac{L'(f_\infty, 2+it)}{L(f_\infty, 2+it)} + \frac{L'(f, 2+it)}{L(f, 2+it)} \right| \frac{dt}{t^2} \\ &\quad + O_N\left(\frac{1}{M}\right). \end{aligned}$$

Grâce à la formule de Stirling on a

$$\frac{L'(f_\infty, 2+it)}{L(f_\infty, 2+it)} \ll_{k,N} \ln |t|$$

d'où

$$\lim_{M \rightarrow +\infty} \int_M^{+\infty} \left| \frac{L'(f_\infty, 2+it)}{L(f_\infty, 2+it)} \right| \frac{dt}{t^2} = 0.$$

Avec (2.7) on a

$$\frac{L'(f, 2+it)}{L(f, 2+it)} \ll \sum_{n=1}^{+\infty} |b_f(n) \Lambda(n)| n^{-2} \ll 1$$

d'où

$$\lim_{M \rightarrow +\infty} \int_M^{+\infty} \left| \frac{L'(f, 2+it)}{L(f, 2+it)} \right| \frac{dt}{t^2} = 0.$$

⁵en notant ρ au lieu de ρ_f .

On a alors prouvé (2.11). On prouve ensuite

$$\lim_{M \rightarrow +\infty} \int_{-1+iM}^{2+iM} G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds = 0.$$

Là encore, par (2.10) et la majoration de Stirling il suffit de prouver

$$\lim_{M \rightarrow +\infty} \int_{-1}^2 \left| \frac{L'(f, \sigma + iM)}{L(f, \sigma + iM)} \frac{d\sigma}{M^2} \right| = 0. \quad (2.12)$$

Grâce à l'expression de $L(f, s)$ en produit de Hadamard, on a [Brü95a] l'estimation

$$\frac{L'(f, \sigma + iM)}{L(f, \sigma + iM)} = \sum_{|\gamma - M| < 1} \frac{1}{\sigma + iM - \rho} + O(\ln M).$$

D'après (2.1), il existe deux zéros $\rho_1 = \beta_1 + i\gamma_1$ et $\rho_2 = \beta_2 + i\gamma_2$ tels que $M - 1 < \gamma_1 < \gamma_2 < M + 1$, $|\gamma_2 - \gamma_1| \gg \ln^{-1} M$ et aucun autre zéro n'a d'ordonnée comprise entre γ_1 et γ_2 . En remplaçant M par M' de sorte que $\gamma_1 < M' < \gamma_2$, on modifie M d'au plus 2 et pour tout zéro tel que $|M' - \gamma| < 1$ on a $|\sigma + iM' - \rho| \gg \ln^{-1} M'$. Ainsi, en remplaçant M par M' (qu'on renote M) on a

$$\frac{L'(f, \sigma + iM)}{L(f, \sigma + iM)} \ll \ln^2 M.$$

On en déduit (2.12) puis

$$D(f, \phi) = \frac{1}{2i\pi} \int_{(2)} 2G(s) \frac{\Lambda'(s)}{\Lambda(s)} ds.$$

Grâce au développement eulérien de $L(f, s)$ on a

$$\frac{\Lambda'(s)}{\Lambda(s)} = \ln(\sqrt{N}/2\pi) + \frac{\Gamma'}{\Gamma} \left(s + \frac{k-1}{2} \right) - \sum_p \left(\sum_{j=1}^{+\infty} (\alpha_f(p)^j + \beta_f(p)^j) p^{-js} \right) \ln p$$

d'où

$$D(f, \phi) = \sum_{\mathcal{P} \cup \{\infty\}} H(p)$$

avec

$$H(p) = -2 \sum_{j=1}^{+\infty} (\alpha_f(p)^j + \beta_f(p)^j) F(p^j) \ln p,$$

$$F(y) = \frac{1}{2i\pi} \int_{(1/2)} G(s) y^{-s} ds = \frac{1}{\sqrt{y} \ln(k^2 N)} \hat{\phi} \left(\frac{\ln y}{\ln(k^2 N)} \right)$$

et

$$H(\infty) = 2F(1) \ln(\sqrt{N}/2\pi) + \frac{1}{2i\pi} \int_{(2)} 2 \frac{\Gamma'}{\Gamma} \left(s + \frac{k-1}{2} \right) G(s) ds.$$

On a donc

$$\begin{aligned} D(f, \phi) &= 2 \frac{\ln(\sqrt{N}/2\pi)}{\ln(k^2 N)} \hat{\phi}(0) + 2 \int_{\mathbb{R}} \frac{\Gamma'}{\Gamma} \left(\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) \phi(x) \frac{dx}{\ln(k^2 N)} \\ &\quad - 2 \sum_p \sum_{j=1}^{+\infty} (\alpha_f(p)^j + \beta_f(p)^j) \hat{\phi} \left(\frac{j \ln p}{\ln(k^2 N)} \right) p^{-j/2} \frac{\ln p}{\ln(k^2 N)}. \end{aligned}$$

Par parité de ϕ on a

$$\int_{\mathbb{R}} \frac{\Gamma'}{\Gamma} \left(\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) \phi(x) \frac{dx}{\ln(k^2 N)} = \int_0^{+\infty} \left(\frac{\Gamma'}{\Gamma} \left(\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) + \frac{\Gamma'}{\Gamma} \left(-\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) \right) \phi(x) \frac{dx}{\ln(k^2 N)}.$$

On a, pour $\Re(z) > 0$ et $y \in \mathbb{R}$ la formule

$$\frac{\Gamma'}{\Gamma}(z) - \frac{\Gamma'}{\Gamma}(y) = \sum_{k=0}^{+\infty} \left(\frac{1}{y+k} - \frac{1}{z+k} \right).$$

(Elle se montre, pour $z > 0$ par utilisation du produit de Gauss de Γ^{-1} et prolongement analytique.) Elle implique

$$\frac{\Gamma'}{\Gamma} \left(\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) + \frac{\Gamma'}{\Gamma} \left(-\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) - 2 \frac{\Gamma'}{\Gamma} \left(\frac{k}{2} \right) = O \left(\frac{x^2}{k^2 \ln^2(k^2 N)} \right).$$

Ainsi, puisque par parité $\hat{\phi}(0) = 2 \int_0^{+\infty} \phi$, on a

$$\int_{\mathbb{R}} \frac{\Gamma'}{\Gamma} \left(\frac{2i\pi x}{\ln(k^2 N)} + \frac{k}{2} \right) \phi(x) \frac{dx}{\ln(k^2 N)} = \frac{\Gamma'}{\Gamma} \left(\frac{k}{2} \right) \frac{\hat{\phi}(0)}{\ln(k^2 N)} + O \left(\frac{1}{k^2 \ln^3(k^2 N)} \right).$$

Or $\frac{\Gamma'}{\Gamma} \left(\frac{k}{2} \right) = \ln k + O(1)$ donc la contribution du facteur infini est

$$H(\infty) = \hat{\phi}(0) + O \left(\frac{1}{\ln(k^2 N)} \right).$$

On estime enfin la contribution des facteurs $L(f_p, s)$. On a

$$\begin{aligned} & 2 \sum_p \sum_{j=1}^{+\infty} (\alpha_f(p)^j + \beta_f(p)^j) \hat{\phi} \left(\frac{j \ln p}{\ln(k^2 N)} \right) p^{-j/2} \frac{\ln p}{\ln(k^2 N)} \\ &= 2 \sum_p \sum_{j=3}^{+\infty} (\alpha_f(p)^j + \beta_f(p)^j) \hat{\phi} \left(\frac{j \ln p}{\ln(k^2 N)} \right) p^{-j/2} \frac{\ln p}{\ln(k^2 N)} \\ &\quad + 2 \sum_p \lambda_f(p) \hat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) p^{-1/2} \frac{\ln p}{\ln(k^2 N)} \\ &\quad + 2 \sum_p (\lambda_f(p^2) - \chi_0(p)) \hat{\phi} \left(\frac{2 \ln p}{\ln(k^2 N)} \right) p^{-1} \frac{\ln p}{\ln(k^2 N)} \end{aligned}$$

où χ_0 est la caractère trivial modulo N . On a

$$\begin{aligned} & \sum_p \sum_{j=3}^{+\infty} (\alpha_f(p)^j + \beta_f(p)^j) \hat{\phi} \left(\frac{j \ln p}{\ln(k^2 N)} \right) p^{-j/2} \frac{\ln p}{\ln(k^2 N)} \\ & \ll \frac{1}{\ln(k^2 N)} \sum_p \ln p \frac{p^{-3/2}}{1 - p^{-1/2}} \ll \frac{1}{\ln(k^2 N)} \end{aligned}$$

puis, grâce à la proposition 1.4.1 on a

$$\sum_{p|N} \lambda_f(p) \hat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) p^{-1/2} \frac{\ln p}{\ln(k^2 N)} \ll \frac{1}{\ln(k^2 N)} \sum_{p|N} \frac{\ln p}{p} \ll \frac{\ln \ln(3N)}{\ln(k^2 N)}$$

et

$$\sum_{p|N} \lambda_f(p^2) \hat{\phi}\left(\frac{2 \ln p}{\ln(k^2 N)}\right) p^{-1} \frac{\ln p}{\ln(k^2 N)} \ll \frac{1}{\ln(k^2 N)}.$$

Si

$$\text{Li}(t) = \int_2^t \frac{dx}{\ln x}$$

le théorème des nombres premiers sous sa forme

$$\#\{p \in \mathcal{P} ; p \leq t\} = \text{Li}(t) + O(e^{-c\sqrt{\ln t}})$$

donne

$$2 \sum_{(p,N)=1} \hat{\phi}\left(\frac{2 \ln p}{\ln(k^2 N)}\right) \frac{\ln p}{p \ln(k^2 N)} = - \int_2^{+\infty} f'(t) \text{Li}(t) dt + O(I_1) + O\left(\frac{1}{\ln(k^2 N)}\right)$$

avec

$$f(t) = \hat{\phi}\left(\frac{2 \ln t}{\ln(k^2 N)}\right) \frac{2 \ln t}{t \ln(k^2 N)}$$

puis

$$I_1 = \int_2^{+\infty} t |f'(t)| e^{-c\sqrt{\ln t}} dt \ll \frac{1}{\ln(k^2 N)}.$$

Or

$$-2 \int_2^{+\infty} f'(t) \text{Li}(t) dt = \int_2^{+\infty} f(t) \frac{dt}{\ln t} = \frac{\phi(0)}{2} + O\left(\frac{1}{\ln(k^2 N)}\right)$$

d'où le résultat. $\square$

2.2.3 Valeurs particulières en $\frac{1}{2}$ D'après (2.5) si f est impaire alors $L(f, \frac{1}{2}) = 0$ de sorte que pour toute forme primitive f , paire ou impaire on a

$$(1 - i^k \varepsilon_f(N)) L\left(f, \frac{1}{2}\right) = 0. \quad (2.13)$$

Lorsque $f \in B(2, N)$, l'annulation de la valeur $L(f, \frac{1}{2})$ est liée au rang du groupe des points rationnels d'une variété abélienne (voir le paragraphe 2.3.3). Il est donc intéressant d'étudier cette annulation. Grâce à l'équation (2.6), $L(f, x)$ est réel lorsque x est réel. De plus, le développement eulérien de $L(f, s)$ assure que $L(f, x) > 0$ pour $x \in]1, +\infty[$. On en déduit, par continuité de $x \mapsto L(f, x)$ que, si l'hypothèse de Riemann est vraie, alors $L(f, \frac{1}{2}) \geq 0$. Il est remarquable que ce résultat soit prouvé *sans recourir à l'hypothèse de Riemann* suite à des travaux commencés par Waldspurger et achevés par Guo [Guo96]. Pour insister sur le caractère remarquable de ce résultat, on rappelle que pour un caractère de Dirichlet quadratique χ on ne sait pas prouver que $L(\chi, \frac{1}{2}) \geq 0$. D'autre part, si f est impaire les travaux de Gross et Zagier [GZ86] prouvent que si $L(f, \frac{1}{2}) = 0$ alors $L'(f, \frac{1}{2}) \geq 0$. On résume ce résultat dans le

THÉORÈME 2.2.3

Soit $f \in B(2, N)$ alors

$$L\left(f, \frac{1}{2}\right) \geq 0$$

et

$$L\left(f, \frac{1}{2}\right) = 0 \Rightarrow L'\left(f, \frac{1}{2}\right) \geq 0.$$

REMARQUE 2.4 Si $f \in B(k, N)$, la première partie du théorème reste vraie.

On conjecture que, en moyenne asymptotique, $L(f, \frac{1}{2}) \neq 0$ si f est paire et $L'(f, \frac{1}{2}) \neq 0$ si f est impaire. Autrement dit, l'ordre de $L(f, s)$ en $s = \frac{1}{2}$ ne serait gouverné que par le signe $\varepsilon_f(N)$. Cela est prédit par la conjecture de Katz et Sarnak que nous expliquons ici. Pour tout entier $j \geq 1$, Katz et Sarnak définissent sur $\mathbb{R}$ deux mesures⁶ $\nu(+, j)$ et $\nu(-, j)$ [KS99a, proposition 7.5.5] de probabilités, supportées dans $\mathbb{R}^+$ et absolument continues par rapport à la mesure de Lebesgue. Si l'hypothèse de Riemann est vérifiée pour $L(f, s)$ avec f primitive, ces zéros non triviaux sont de la forme $\frac{1}{2} + i\gamma_f$ avec

$$0 \leq \gamma_{f,1} \leq \gamma_{f,2} \leq \dots$$

On a listé les zéros avec multiplicité. Si f est impaire, le zéro $\frac{1}{2}$ est listé avec multiplicité moins 1⁷. La conjecture prévoit que pour tout $j \geq 1$ et pour toute fonction $h : \mathbb{R} \rightarrow \mathbb{C}$ continue à support compact on ait

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^\pm(N)} \sum_{f \in B^\pm(N)} h\left(\gamma_{f,j} \frac{\ln(k^2 N)}{2\pi}\right) = \int_{\mathbb{R}} h d\nu(\pm, j). \quad (2.14)$$

On choisit pour tout réel $0 < t < 1$ une fonction continue $h_t : \mathbb{R} \rightarrow [0, 1]$ à support dans $[-t, t]$ et telle que $h_t(0) = 1$. On a $h_t \geq \delta_0$ et donc

$$\frac{1}{\#B^+(N)} \sum_{f \in B^+(N)} h_t\left(\gamma_{f,1} \frac{\ln(k^2 N)}{2\pi}\right) \geq \frac{1}{\#B^+(N)} \#\left\{f \in B^+(N); L\left(f, \frac{1}{2}\right) = 0\right\}.$$

Lorsque $N \rightarrow \infty$ puis $t \rightarrow 0$ on déduit de (2.14)

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^+(N)} \#\left\{f \in B^+(N); L\left(f, \frac{1}{2}\right) = 0\right\} = 0.$$

De même

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^-(N)} \#\left\{f \in B^-(N); L'\left(f, \frac{1}{2}\right) = 0\right\} = 0.$$

Ces faits sont exposés dans [KS99a, introduction]. Iwaniec, Luo et Sarnak ont prouvé (en supposant l'hypothèse de Riemann des fonctions L des formes primitives, mais aussi des caractères de Dirichlet) que

$$\liminf_{N \rightarrow \infty} \frac{1}{\#B^+(N)} \#\left\{f \in B^+(N); L\left(f, \frac{1}{2}\right) \neq 0\right\} > \frac{9}{16} \quad (2.15a)$$

et

$$\liminf_{N \rightarrow \infty} \frac{1}{\#B^-(N)} \#\left\{f \in B^-(N); L'\left(f, \frac{1}{2}\right) \neq 0\right\} > \frac{15}{16}. \quad (2.15b)$$

Iwaniec et Sarnak prouvent – inconditionnellement – la minoration (2.15a) avec $\geq \frac{1}{2}$ au lieu de $> \frac{9}{16}$. Kowalski et Michel prouvent – inconditionnellement – la minoration (2.15b) avec $\geq \frac{7}{8}$ au lieu de $> \frac{15}{16}$. Ils montrent avec VanderKam qu'au moins 99 % des formes primitives annulent leur fonction L en $\frac{1}{2}$ à un ordre inférieur ou égal à 4 [KMV00b]. Le lecteur est invité à se reporter à la remarque 2.10 pour des tests numériques sur cette conjecture.

Les travaux de Gross et Zagier [GZ86, corollary (1.3)] permettent aussi de prouver que si l'ordre de la fonction L d'une forme primitive est inférieur ou égal à 1, alors il est stable par action de Galois. Autrement dit, on a la

⁶Ce sont les limites, lorsque N tend vers $+\infty$ des mesures de localisation de la j^e (resp. $j+1^e$) phase propre de $SO(2N)$ (resp. $SO(2N+1)$) lorsqu'on les ordonne dans $[0, \pi]$.

⁷Autrement dit, on ne compte que les zéros non « évidents ».

PROPOSITION 2.2.4

Soit $f \in B(2, N)$. Alors

$$L\left(f, \frac{1}{2}\right) \neq 0 \quad \text{si et seulement si} \quad L\left(f^\sigma, \frac{1}{2}\right) \neq 0 \quad \forall \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

et

$$\text{ord}_{s=1/2} L(f, s) = 1 \quad \text{si et seulement si} \quad \text{ord}_{s=1/2} L(f^\sigma, s) = 1 \quad \forall \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

On conjecture qu'il n'existe que deux orbites de formes primitives de tailles non négligeables, une constituée de formes paires et l'autre de formes impaires. Est-ce que deux formes paires (resp. impaires) appartiennent à la même orbite? Des évaluations numériques de Brumer [Bru95b, §§6 et 8] montrent que pour environ 88 % des nombres premiers N inférieurs à 10000, il n'y a qu'une orbite d'ordre pair dans $B(2, N)$. Pour les 12 % de nombres premiers restant, il semble y avoir une orbite beaucoup plus grosse que les autres. Nos résultats (voir le chapitre 3) montrent la

PROPOSITION 2.2.5

Soit p un nombre premier. Il existe une constante C_p strictement positive et un entier N_p tels que pour tout entier $N > N_p$ non divisible par p il existe $f^+ \in B^+(2, N)$ et $f^- \in B^-(2, N)$ telles que

$$\# \text{ orbite } f^+ \geq C_p \sqrt{\ln \ln N}$$

et

$$\# \text{ orbite } f^- \geq C_p \sqrt{\ln \ln N}.$$

REMARQUE 2.5 Compte-tenu des dimensions de $B^+(2, N)$ et $B^-(2, N)$ (voir le paragraphe 1.7) et des calculs de Brumer, on s'attend à pouvoir remplacer $\sqrt{\ln \ln N}$ par une puissance positive de N .

Les calculs sur les valeurs de $L(f, \frac{1}{2})$ et $L'(f, \frac{1}{2})$ se font par leur expression en séries courtes grâce au⁸

LEMME 2.2.6

Soit V et W les fonctions définies par

$$V(y) = \frac{1}{2i\pi\Gamma(\frac{k}{2})} \int_{(2)} \Gamma\left(s + \frac{k}{2}\right) y^{-s} \frac{ds}{s}$$

et

$$W(y) = \frac{1}{2i\pi\Gamma(\frac{k}{2})} \int_{(2)} \Gamma\left(s + \frac{k}{2}\right) y^{-s} \frac{ds}{s^2}.$$

Pour tout réel $A > 0$, ces fonctions vérifient

$$|V(y)| \ll y^{-A} \quad \text{et} \quad |W(y)| \ll y^{-A}$$

les constantes dépendant de A .

Pour $f \in B(N)$ on a

$$L\left(f, \frac{1}{2}\right) = (1 + i^k \varepsilon_f(N)) \sum_{\ell=1}^{+\infty} \frac{\lambda_f(\ell)}{\sqrt{\ell}} V\left(\frac{2\pi\ell}{\sqrt{N}}\right)$$

et

$$(1 - i^k \varepsilon_f(N)) L'\left(f, \frac{1}{2}\right) = 2(1 - i^k \varepsilon_f(N)) \sum_{\ell=1}^{+\infty} \frac{\lambda_f(\ell)}{\sqrt{\ell}} W\left(\frac{2\pi\ell}{\sqrt{N}}\right).$$

⁸Ce lemme est le point de départ de l'étude des problèmes d'annulation de $L(f, \frac{1}{2})$ et $L'(f, \frac{1}{2})$.

Démonstration – Soit $M > 0$. On note $\mathcal{F}_M$ la frontière du rectangle défini par les angles $1 + iM$, $-1 + iM$, $-1 - iM$ et $1 - iM$. On note

$$\Lambda(s) = (2\pi)^{k/2} N^{(2s-1)/4} L(f_\infty, s) L(f, s) / 2.$$

Le théorème des résidus donne alors

$$\frac{1}{2i\pi} \int_{\mathcal{F}_M} \Lambda\left(s + \frac{1}{2}\right) \frac{ds}{s} = \Gamma\left(\frac{k}{2}\right) L\left(f, \frac{1}{2}\right).$$

Or

$$\begin{aligned} - \int_{-1-iM}^{-1+iM} \Lambda\left(s + \frac{1}{2}\right) \frac{ds}{s} + \int_{1-iM}^{1+iM} \Lambda\left(s + \frac{1}{2}\right) \frac{ds}{s} \\ = (1 + i^k \varepsilon_f(N)) \int_{1-iM}^{1+iM} \Lambda\left(s + \frac{1}{2}\right) \frac{ds}{s} \end{aligned}$$

grâce à l'équation fonctionnelle (2.5). D'autre part

$$\int_{1-iM}^{1+iM} \Lambda\left(s + \frac{1}{2}\right) \frac{ds}{s} = \sum_{\ell=1}^{+\infty} \frac{\lambda_f(\ell)}{\sqrt{\ell}} \int_{1-iM}^{1+iM} \Gamma\left(s + \frac{k}{2}\right) \left(\frac{2\pi\ell}{\sqrt{N}}\right)^{-s} \frac{ds}{s}.$$

Il reste à faire tendre M vers l'infini. Cela se fait par les mêmes méthodes que celles utilisées dans la preuve de la proposition 2.2.2. La majoration $V(y) \ll y^{-A}$ résulte du déplacement de contour de la ligne $\Re s = 2$ vers la ligne $\Re s = A$ et de la majoration de Stirling.

Pour l'expression de $L'(f, \frac{1}{2})$ on considère

$$I = \frac{1}{2i\pi} \int_{(1)} \Lambda\left(s + \frac{1}{2}\right) \frac{ds}{s^2}.$$

Comme précédemment on a

$$(1 - i^k \varepsilon_f(N)) I = \operatorname{Rés}_{s=0} s^{-2} \Lambda\left(s + \frac{1}{2}\right).$$

On multiplie par $\frac{1}{2}(1 - \varepsilon_f(N)) \in \{0, 1\}$ et on utilise (2.13) pour trouver

$$\frac{1}{2}(1 - i^k \varepsilon_f(N))^2 I = (1 - i^k \varepsilon_f(N)) I = \frac{1}{2} \Gamma\left(\frac{k}{2}\right) (1 - i^k \varepsilon_f(N)) L'\left(f, \frac{1}{2}\right).$$

Le développement de Λ permet de conclure. $\square$

On peut alors énoncer pour les formes de $B(2, N)$ deux formules de traces tordues respectivement par $L(f, \frac{1}{2})$ et $L'(f, \frac{1}{2})$. Pour cela, il est nécessaire d'évaluer la somme et la dérivée de

$$g(m, s) = \sum_{\ell=1}^{+\infty} \ell^{-1-s} \sum_{d|(\ell, m)} d\chi_N^\square\left(\frac{\ell m}{d^2}\right)$$

pour m une puissance de premier et $s = 0$.

LEMME 2.2.7

Pour tout nombre premier p premier à N , tout entier positif ou nul n et tout complexe s tel que $\Re s > -1/2$ on a :

$$\begin{aligned} g(p^{2n}, s) &= \left(1 + \left(1 + \frac{1}{p}\right) \frac{1 - p^{-2ns}}{1 - p^{-2s}} p^{-2s}\right) \zeta^{(N)}(2 + 2s) \\ g(p^{2n+1}, s) &= \left(1 + \frac{1}{p}\right) \frac{1 - p^{-2(n+1)s}}{1 - p^{-2s}} p^{-s} \zeta^{(N)}(2 + 2s). \end{aligned}$$

En particulier :

$$g(p^n, 0) = \zeta^{(N)}(2) \begin{cases} \frac{n}{2} \left(1 + \frac{1}{p}\right) + 1 & \text{si } n \text{ est pair;} \\ \frac{n+1}{2} \left(1 + \frac{1}{p}\right) & \text{sinon.} \end{cases}$$

Enfin :

$$g'(p^n, 0) = 2 \frac{\zeta^{(N)'}(2)}{\zeta^{(N)}(2)} g(p^n, 0) + e(p, n)$$

où $e(p, n)$ est définie par :

$$e(p, n) = -\zeta^{(N)}(2) \left(1 + \frac{1}{p}\right) \ln p \begin{cases} \frac{n}{2} \left(\frac{n}{2} + 1\right) & \text{si } n \text{ est pair;} \\ \left(\frac{n+1}{2}\right)^2 & \text{sinon.} \end{cases}$$

LEMME 2.2.8

Soit p un nombre premier. La fonction $g(p^n, s)$ possède les propriétés suivantes :

1) pour $\Re s \in]-1/2, +\infty[$:

$$\left| \frac{g(p^n, s)}{\zeta^{(N)}(2 + 2s)} \right| \ll_\varepsilon \begin{cases} 1 & \text{si } \Re s > \varepsilon; \\ p^{n/2} & \text{sinon;} \end{cases}$$

2) pour $n > 0$:

$$\begin{aligned} \left(1 + \frac{1}{p}\right) g(p^n, 0) p^{-n/2} - \frac{1}{p^{1/2}} g(p^{n-1}, 0) p^{-(n-1)/2} - \\ \frac{1}{p^{1/2}} g(p^{n+1}, 0) p^{-(n+1)/2} = \left(1 - \frac{1}{p^2}\right) \zeta^{(N)}(2) \mu_p(X_n); \end{aligned}$$

3) pour $n > 0$:

$$\begin{aligned} \left(1 + \frac{1}{p}\right) g'(p^n, 0) p^{-n/2} - \frac{1}{p^{1/2}} g'(p^{n-1}, 0) p^{-(n-1)/2} - \\ \frac{1}{p^{1/2}} g'(p^{n+1}, 0) p^{-(n+1)/2} = 2 \zeta^{(N)'}(2) \left(1 - \frac{1}{p^2}\right) \mu_p(X_n) + \\ \zeta^{(N)}(2) \left(1 + \frac{1}{p}\right) \ln(p) k(p, n) p^{-n/2} \end{aligned}$$

avec :

$$k(p, n) = \begin{cases} \frac{n}{2p} + \frac{1}{p} - \frac{n}{2} & \text{si } n \text{ est pair;} \\ -\frac{n+1}{2} \left(1 - \frac{1}{p}\right) & \text{sinon.} \end{cases}$$

Démonstration – Les points 2) et 3) se font par simple calcul à partir du lemme 2.2.7 et de la relation (1.12). On démontre 1). On a la majoration suivante :

$$\left| \frac{1 - p^{-2(n+1)s}}{1 - p^{-2s}} \right| \leq \sum_{k=0}^n p^{-2k \Re s}. \quad (2.16)$$

Ainsi, lorsque $\Re s > \varepsilon$ on déduit de (2.16) :

$$\left| \frac{g(p^{2n+1}, s)}{\zeta(2 + 2s)} \right| \leq 2 \frac{1 - p^{-2(n+1)\varepsilon}}{1 - p^{-2\varepsilon}} \leq \frac{2}{1 - 2^{-2\varepsilon}}.$$

Lorsque $\Re s > -1/2$ on déduit de même :

$$\left| \frac{g(p^{2n+1}, s)}{\zeta(2+2s)} \right| \leq 2 \frac{p^{n+1} - 1}{p - 1} p^{1/2} \leq 4 \frac{p^{n+1}}{p} p^{1/2} = 4p^{(2n+1)/2}.$$

car $p^{1-2\varepsilon} - 1 > p^{1-2\varepsilon}/4$ pour ε assez petit. Le principe de calcul est le même pour $2n$. $\square$

On obtient alors une formule de trace tordue par $L(f, 1/2)$ dans la

PROPOSITION 2.2.9

Pour tout entier strictement positif N , tout nombre premier p ne divisant pas le niveau N et tout entier positif ou nul n nous avons :

$$\frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} L\left(f, \frac{1}{2}\right) \lambda_f(p^n) = \zeta^{(N)}(2) f(p^n, 0) p^{-n/2} + O_\varepsilon(p^{n(1+\varepsilon)/2} N^{-1/4+\varepsilon}).$$

La fonction $f(p^n, 0)$ est donnée par :

$$f(p^n, 0) = \begin{cases} \frac{n}{2} \left(1 + \frac{1}{p}\right) + 1 & \text{si } n \text{ est pair;} \\ \frac{n+1}{2} \left(1 + \frac{1}{p}\right) & \text{sinon.} \end{cases}$$

Démonstration – Grâce au lemme 2.2.6 et aux propositions 1.7.14 et 1.7.13 on a :

$$\begin{aligned} \sum_{f \in B(2, N)} L\left(f, \frac{1}{2}\right) \lambda_f(p^n) &= \\ \sum_{\ell \leq N^{1/2+\varepsilon}} V\left(\frac{2\pi\ell}{\sqrt{N}}\right) \ell^{-1/2} \sum_{f \in B(2, N)} (1 + i^k \varepsilon_f(N)) \lambda_f(\ell) \lambda_f(p^n) + O_\varepsilon(p^{n(1+\varepsilon)/2} N^{-1}). \end{aligned}$$

Puis grâce de nouveau aux propositions 1.7.14 et 1.7.13 et réintégration des $\ell > N^{1/2+\varepsilon}$ qui interviennent de façon négligeable, cette quantité devient :

$$\#B(2, N) p^{-n/2} \sum_{\ell=0}^{\infty} V(2\pi\ell N^{-1/2}) \ell^{-1} \sum_{d|(\ell, p^n)} d\chi_N^\square\left(\frac{\ell p^n}{d^2}\right) + O_\varepsilon(p^{n(1+\varepsilon)/2} N^{3/4+\varepsilon}).$$

Enfin le résultat s'obtient par déformation de contour sur V vers la ligne $\Re s = -1/2 + \varepsilon$ et utilisation des lemmes 2.2.8 et 2.2.7. $\square$

On a de même une formule de trace tordue par $(1 - i^k \varepsilon_f(N)) L'(f, 1/2)$ dans la

PROPOSITION 2.2.10

Pour tout entier strictement positif N , tout nombre premier p ne divisant pas le niveau N et tout entier positif ou nul n on a

$$\begin{aligned} \frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} (1 - i^k \varepsilon_f(N)) L'(f, 1/2) \lambda_f(p^n) &= \\ 2 \left(\ln \frac{\sqrt{N}}{2\pi e^\gamma} f(p^n, 0) + \hat{f}(p^n, 0) \right) \zeta^{(N)}(2) p^{-n/2} + O_\varepsilon(p^{n(1+\varepsilon)/2} N^{-1/4+\varepsilon}). \end{aligned}$$

La fonction $f(p^n, 0)$ est donnée par

$$f(p^n, 0) = \begin{cases} \frac{n}{2} \left(1 + \frac{1}{p}\right) + 1 & \text{si } n \text{ est pair;} \\ \frac{n+1}{2} \left(1 + \frac{1}{p}\right) & \text{sinon.} \end{cases}$$

La fonction $\widehat{f}(p^n, 0)$ est donnée par

$$\widehat{f}(p^n, 0) = f(p^n, 0) \begin{cases} \left(\frac{2\zeta^{(N)'}(2)}{\zeta^{(N)}(2)} - \left(1 + \frac{1}{p}\right)^{\frac{\frac{n}{2}(\frac{n}{2}+1)\ln p}{1+(1+\frac{1}{p})^{\frac{n}{2}}}} \right) & \text{si } n \text{ est pair;} \\ \left(\frac{2\zeta^{(N)'}(2)}{\zeta^{(N)}(2)} - \frac{(n+1)}{2} \ln p \right) & \text{sinon.} \end{cases}$$

Démonstration – La méthode est la même que celle utilisée pour prouver la proposition 2.2.9. $\square$

2.3 Fonction L de carré symétrique

Dans tout ce paragraphe, M est un entier sans facteur carré.

2.3.1 Définition et équation fonctionnelle La fonction L de carré symétrique d'une forme $f \in B(M)$ est définie pour $\Re s > 1$ par

$$L(sym^2 f, s) = \zeta^{(M)}(2s) \sum_{n=1}^{+\infty} \lambda_f(n^2) n^{-s}.$$

Pour $\Re(s) > 1$, la fonction $L(sym^2 f, s)$ admet le développement eulérien

$$L(sym^2 f, s) = \prod_{p \in \mathcal{P}} L(sym_p^2 f, s)$$

où $L(sym_p^2 f, s)$ est définie par

$$L(sym_p^2 f, s) = (1 - \alpha_f(p)^2 p^{-s})^{-1} (1 - \alpha_f(p) \beta_f(p) p^{-s})^{-1} (1 - \beta_f(p)^2 p^{-s})^{-1}.$$

On définit

$$L(sym_\infty^2 f, s) = \pi^{-3s/2} \Gamma\left(\frac{s+1}{2}\right) \Gamma\left(\frac{s+k-1}{2}\right) \Gamma\left(\frac{s+k}{2}\right).$$

Shimura a prouvé que la fonction $L(sym_\infty^2 f, s) L(sym^2 f, s)$ admet un prolongement méromorphe qui est holomorphe sauf en d'éventuels pôles simples en $s = 0$ et $s = 1$ [Shi75, theorem 1]. D'autre part, on définit

$$L(f \times f, s) = \zeta^{(M)}(2s) \sum_{n=1}^{\infty} \lambda_f(n)^2 n^{-s}. \quad (2.17)$$

Grâce à (1.21), cette fonction a pour développement eulérien

$$L(f \times f, s) = \prod_{p \in \mathcal{P}} (1 - \alpha_f(p)^2 p^{-s})^{-1} (1 - \alpha_f(p) \beta_f(p) p^{-s})^{-2} (1 - \beta_f(p)^2 p^{-s})^{-1}.$$

On en déduit

$$L(f \times f, s) = \zeta^{(M)}(s) L(sym^2 f, s). \quad (2.18)$$

Rankin (voir aussi le corollaire 2.3.4) a prouvé que $L(f \times f, s)$ avait un pôle simple en 1 et était holomorphe ailleurs. En particulier, $\zeta^{(M)}$ ayant un pôle simple en 1, $L(sym^2 f, s)$ n'en a pas⁹. Li [Li75, §4] a prouvé que la fonction

$$\Phi^+(s) = \prod_{p|M} (1 - p^{-s})^{-1} \left(\frac{\sqrt{M}}{2\pi} \right)^{2s} \Gamma(s) \Gamma(s+k-1) L(f \times f, s)$$

⁹Si $M = 1$, $\zeta^{(M)}(0) = \zeta(0) \neq 0$ et on déduit de (2.18) que $L(sym^2 f, s)$ n'a pas de pôle en 0. Mais si $M \neq 1$ alors $\zeta^{(M)}(0) = 0$.

vérifie l'équation fonctionnelle $\Phi^+(s) = \Phi^+(1-s)$. Grâce à la formule de duplication de Legendre, on peut récrire

$$\Phi^+(s) = \frac{2^{k-3}}{\pi} \xi(s) M^s L(\text{sym}_\infty^2 f, s) L(\text{sym}^2 f, s)$$

où

$$\xi(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Supposons, par l'absurde, que $L(\text{sym}^2 f, s)$ ait un pôle en $s = 0$. Alors Φ^+ aurait un pôle double en 0 et donc en 1 et $L(\text{sym}^2 f, s)$ aurait un pôle en 1; on a vu que ce n'était pas le cas. On déduit alors de $\xi(s) = \xi(1-s)$ et du fait que $L(\text{sym}_\infty^2 f, s) L(\text{sym}^2 f, s)$ est entière l'équation fonctionnelle valable sur $\mathbb{C}$ donnée par

$$L(\text{sym}_\infty^2 f, s) L(\text{sym}^2 f, s) = (M^2)^{-s+1/2} L(\text{sym}_\infty^2 f, 1-s) L(\text{sym}^2 f, 1-s).$$

REMARQUE 2.6 Pourquoi ce terme « carré symétrique » ? La réponse est donnée par l'introduction d'une nouvelle structure qui permet de voir les fonctions L de Dirichlet et de formes primitives comme des cas particuliers d'une même définition générale. On esquisse cette généralisation (voir [Gel97] et [Bum98, §§1.8 et 3.3]). On note $\mathbb{A}$ l'anneau des adèles de $\mathbb{Q}$, c'est le sous anneau de

$$\prod_{p \in \mathcal{P} \cup \{\infty\}} \mathbb{Q}_p$$

formé des (x_p) avec $x_p \in \mathbb{Z}_p$ pour presque tout¹⁰ $p \in \mathcal{P}$. L'injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ permet de considérer le morphisme d'anneaux injectif

$$\begin{array}{ccc} i_p & : & \mathbb{Q} \hookrightarrow \mathbb{A} \\ x & \longmapsto & (x_p)_{p \in \mathcal{P} \cup \{\infty\}} \end{array}$$

puisque $x \in \mathbb{Z}_p$ pour tout p ne divisant pas le dénominateur de x . On muni $\mathbb{A}$ d'une topologie en donnant à un point (x_p) de $\mathbb{A}$ la base de voisinage constituée des ensembles $\prod_p \Omega_p$ où Ω_p est un ouvert de $\mathbb{Q}_p$ contenant x_p et, pour presque tout p , contenu dans $\mathbb{Z}_p$. Pour cette topologie $\mathbb{A}$ est localement compact, $\mathbb{Q}$ est discret dans $\mathbb{A}$ et $\mathbb{A}/\mathbb{Q}$ est compact¹¹ [Hum80, §4.2]. Si $GL(n, \mathbb{Q})$ (resp. $GL(n, \mathbb{A})$) est l'ensemble des matrices $n \times n$ à coefficients dans $\mathbb{Q}$ (resp. $\mathbb{A}$) de déterminant non nul (resp. inversible dans $\mathbb{A}$), l'inclusion i_p permet de voir $GL(n, \mathbb{Q})$ comme un sous-groupe discret de $GL(n, \mathbb{A})$. Puisque $\mathbb{A}$ est un groupe additif localement compact commutatif, il a une mesure de Haar. Soit $Z(\mathbb{A}) = \{aI_n; a \in \mathbb{A}^\times\}$ où I_n est la matrice identité de $GL(n, \mathbb{A})$ et $\mathbb{A}^\times$ est le groupe des éléments inversibles de $\mathbb{A}$. On montre que $Z(\mathbb{A})GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A})$ est de volume fini pour la mesure de Haar [JL70, §10]. Soit ω un caractère unitaire de $\mathbb{A}^\times / \mathbb{Q}^\times$. On définit l'espace des *formes automorphes paraboliques*

$$L_0^2(GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A}), \omega)$$

comme étant l'espace des fonctions mesurables sur $GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A})$ telles que

1)

$$f(zI_n g) = \omega(z) f(g), \quad \forall z \in \mathbb{A}^\times, \forall g \in GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A})$$

¹⁰C'est-à-dire tous sauf un nombre fini.

¹¹La situation topologique de $\mathbb{Q}$ dans $\mathbb{A}$ est donc semblable à celle de $\mathbb{Z}$ dans $\mathbb{R}$.

2)

$$\int_{Z(\mathbb{A})GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A})} |f(g)|^2 dg < \infty$$

3)

$$\int_{(\mathbb{A}/\mathbb{Q})^{r(n-r)}} f\left(\begin{pmatrix} I_r & x \\ 0 & I_{n-r} \end{pmatrix}\right) dx = 0, \quad \forall g \in GL(n, \mathbb{A}), \forall r \in [1, n[.$$

Cette espace est invariant par la représentation régulière à droite

$$\begin{array}{ccc} GL(n, \mathbb{A}) & \longrightarrow & \text{End}\left(L_0^2\left(GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A}), \omega\right)\right) \\ g & \longmapsto & \left(f \longmapsto (g' \longmapsto f(g'g))\right) \end{array}$$

et il se décompose en somme directe infinie de sous-espaces irréductibles invariants [Bum98, theorem 3.3.2]. Une représentation de $GL(n, \mathbb{A})$ s'écrit $\varpi = \otimes_p \varpi_p$ avec ϖ_p représentation de $GL(n, \mathbb{Q}_p)$ (c'est un résultat de Gel'fand, Graev et Pyatetskii-Shapiro, voir [Fla79]). S'il existe un caractère ω tel qu'une représentation ϖ de $GL(n, \mathbb{A})$ soit isomorphe à la représentation régulière à droite sur l'un des sous-espaces invariants de $L_0^2(GL(n, \mathbb{Q}) \backslash GL(n, \mathbb{A}), \omega)$ on dit que ϖ est une *représentation automorphe parabolique* de $GL(n, \mathbb{A})$. L'intérêt, pour nous, d'introduire cette notion est qu'il existe une application bijective entre $B(N)$ et un sous-ensemble des représentations automorphes paraboliques. Godement et Jacquet ont associé à une représentation automorphe parabolique ϖ de $GL(n, \mathbb{A})$ une fonction $L(\varpi, s)$. Cette fonction est donnée par

$$L(\varpi, s) = \prod_p L(\varpi_p, s)$$

où, sauf pour un nombre fini de premiers et ∞ , $L(\varpi_p, s)$ est de la forme

$$L(\varpi_p, s) = (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_n(p)p^{-s})^{-1}.$$

Dans le cas où $n = 2$, si ϖ correspond à la forme primitive f_ϖ alors $L(f_\varpi, s) = L(\varpi, s)$. Si ϖ est une représentation de $GL(2, \mathbb{A})$ et si r est un entier positif, on conjecture qu'il existe une représentation automorphe parabolique $\varpi^{(r)}$ de $GL(r+1, \mathbb{A})$ dont la série L , notée $L(\varpi^{(r)}, s)$ est donnée par

$$\prod_p (1 - \alpha_1(p)^r p^{-s})^{-1} (1 - \alpha_1(p)^{r-1} \alpha_2(p) p^{-s})^{-1} \cdots (1 - \alpha_2(p)^r p^{-s})^{-1}.$$

Dans le cas $r = 2$, si on note f pour f_ϖ , on a (avec les notations de la page 22)

$$L(\varpi, s) = \prod_p (1 - \alpha_f(p)p^{-s})^{-1} (1 - \beta_f(p)p^{-s})^{-1}.$$

D'après un résultat de Jacquet, la fonction $\varpi^{(2)}$ est le carré symétrique $\text{sym}^2 \varpi$ de ϖ et, on remarque que si f est la forme primitive f_ϖ alors

$$L(\text{sym}^2 f_\varpi, s) = L(\text{sym}^2 \varpi, s)$$

d'où la notion du carré symétrique d'une forme primitive.

2.3.2 La valeur particulière $L(sym^2 f, 1)$ Un intérêt de l'étude de $L(sym^2 f, 1)$ est que l'on peut relier cette valeur à la norme de Petersson de f grâce au

LEMME 2.3.1

Soit $f \in B(M)$, on a $(f, f)_M = \frac{\Gamma(k)}{2^{2k-1}\pi^{k+1}} ML(sym^2 f, 1)$.

Si $N = LM$ et si $\ell|L$ on a vu au paragraphe 1.3.1 que si $f \in B(M)$ alors $f_\ell \in S(N)$. Le lemme 2.3.1 est une conséquence du

LEMME 2.3.2

Soit M et L des entiers sans facteur carré et premiers entre eux. Soit $\ell_1|L$ et $\ell_2|L$. On pose $N = LM$ et $\ell = \ell_1\ell_2(\ell_1, \ell_2)^{-2}$. Soit $f \in B(M)$, on a

$$(\ell_1\ell_2)^{k/2}(f_{\ell_1}, f_{\ell_2})_N = \lambda_f(\ell)\ell^{1/2}\nu(\ell)^{-1} \frac{\Gamma(k)}{2^{2k-1}\pi^{k+1}} \frac{\nu(N)M}{\nu(M)} L(sym^2 f, 1).$$

REMARQUE 2.7 Ce lemme est dû à Abbes et Ullmo dans le cas du poids 2 et a été généralisé par Iwaniec, Luo et Sarnak. La base de la preuve est la méthode de déroulement de Rankin et Selberg.

Démonstration – On définit

$$\Gamma_\infty = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z} \right\}$$

puis la série d'Eisenstein¹²

$$E(z, s) = \sum_{\Gamma_\infty \backslash \Gamma_0(N)} (\Im \gamma z)^s.$$

La fonction $s \mapsto E(z, s)$ a priori holomorphe pour $\Re s > 1$ se prolonge en une fonction méromorphe. Sur $\Re s > \frac{1}{2}$ le seul pôle est $s = 1$. Il est simple et de résidu

$$\text{Rés}_{s=1} E(z, s) = \frac{3}{\pi \nu(N)}$$

[Miy89, corollary 7.2.11 et 7.2.17]. Soit $F(s) = (E(z, s)f(\ell_1 z), f(\ell_2 z))_N$, on a

$$\text{Rés}_{s=1} F(s) = \frac{3}{\pi \nu(N)} (f_{\ell_1}, f_{\ell_2})_N. \quad (2.19)$$

D'autre part,

$$\begin{aligned} F(s) &= \int_{D_0(N)} E(z, s) f(\ell_1 z) \bar{f}(\ell_2 z) y^{k-2} dx dy \\ &= \sum_{\Gamma_\infty \backslash \Gamma_0(N)} \int_{\gamma D_0(N)} y^{s+k-2} f(\ell_1 z) \bar{f}(\ell_2 z) dx dy \end{aligned}$$

après changement $z \mapsto \gamma^{-1}z$ et utilisation de l'invariance modulaire. Un domaine fondamental de Γ_∞ étant $0 < \Re z < 1$, $\Im z > 0$, on en déduit¹³

$$F(s) = \int_{y=0}^{+\infty} y^{s+k-2} \int_{x=0}^1 f(\ell_1 z) \bar{f}(\ell_2 z) dx dy.$$

¹²Miyake étudie plutôt la fonction $E_{0,N}^*(z, s) = (\Im z)^{-s} E(z, s)$. Dans [Miy89], il définit cette fonction (contrairement à ce qu'indique l'index) en (7.2.60) et (7.2.61) page 290.

¹³C'est cette méthode de calcul qu'on appelle méthode de déroulement : elle revient à « dérouler » $D_0(N)$ dans le domaine fondamental de Γ_∞ .

On a, par utilisation du développement de Fourier de f , l'égalité

$$F(s) = \sum_{n_1=0}^{+\infty} \sum_{n_2=0}^{+\infty} \lambda_f(n_1) \lambda_f(n_2) (n_1 n_2)^{(k-1)/2} \\ \times \int_0^{+\infty} y^{s+k-2} \exp(2\pi(n_2 \ell_2 + n_1 \ell_1)y) dy \int_0^1 e((n_1 \ell_1 - n_2 \ell_2)x) dx$$

puis

$$F(s) = (4\pi)^{-s-k+1} \Gamma(s+k-1) (\ell_1 \ell_2)^{(1-k)/2} \sum_{n_1 \ell_1 = n_2 \ell_2} \lambda_f(n_1) \lambda_f(n_2) (n_1 \ell_1)^{-s}.$$

On définit deux entiers sans facteur carré et premiers entre eux

$$\ell' = \frac{\ell_1}{(\ell_1, \ell_2)} \text{ et } \ell'' = \frac{\ell_2}{(\ell_1, \ell_2)}.$$

La bijection

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\sim} & \{(n_1, n_2) \in \mathbb{N}^2; n_1 \ell_1 = n_2 \ell_2\} \\ n & \mapsto & (n\ell'', n\ell') \end{array}$$

permet d'écrire

$$F(s) = (4\pi)^{-s-k+1} \Gamma(s+k-1) (\ell_1 \ell_2)^{(1-k)/2} \left(\frac{\ell_1 \ell_2}{(\ell_1, \ell_2)} \right)^{-s} \\ \times \sum_{n=1}^{+\infty} \lambda_f(n\ell'') \lambda_f(n\ell') n^{-s}.$$

On pose, pour $(a, b) = 1$,

$$F(a, b; s) = \sum_{n=1}^{+\infty} \lambda_f(na) \lambda_f(nb) n^{-s}.$$

On a alors

$$\begin{aligned} F(a, b; s) &= \sum_{n=1}^{+\infty} n^{-s} \sum_{\substack{d|(na, nb) \\ (d, M)=1}} \lambda_f\left(\frac{n^2 ab}{d^2}\right) \\ &= \sum_{n=1}^{+\infty} n^{-s} \sum_{\substack{d|n \\ (d, M)=1}} \lambda_f\left(\frac{n^2 ab}{d^2}\right) \end{aligned}$$

ainsi $F(a, b; s)$ ne dépend que du produit ab et en particulier si $\ell = \ell' \ell''$,

$$F(\ell', \ell''; s) = \sum_{n=1}^{+\infty} \lambda_f(n\ell) \lambda_f(n) n^{-s}.$$

En écrivant $n = mr$ avec $(m, \ell) = 1$ et $r|\ell^\infty$ on a

$$F(\ell', \ell''; s) = \sum_{(m, \ell)=1} \lambda_f(m)^2 m^{-s} \sum_{r|\ell^\infty} \lambda_f(r\ell) \lambda_f(r) r^{-s}.$$

Décomposant $\ell = p_1 \cdots p_{\omega(\ell)}$, on a

$$\sum_{r|\ell^\infty} \lambda_f(r\ell) \lambda_f(r) r^{-s} = \sum_{\nu_1=0}^{+\infty} \cdots \sum_{\nu_{\omega(\ell)}=0}^{+\infty} \lambda_f(p_1^{\nu_1+1} \cdots p_{\omega(\ell)}^{\nu_{\omega(\ell)}+1}) \lambda_f(p_1^{\nu_1} \cdots p_{\omega(\ell)}^{\nu_{\omega(\ell)}}) (p_1^{\nu_1} \cdots p_{\omega(\ell)}^{\nu_{\omega(\ell)}})^{-s}$$

puis, par multiplicativité de λ_f ,

$$F(\ell', \ell''; s) = \sum_{(m, \ell)=1} \lambda_f(m)^2 m^{-s} \prod_{p|\ell} \sum_{\nu=0}^{+\infty} \lambda_f(p^{\nu+1}) \lambda_f(p^\nu) p^{-\nu s}.$$

Grâce à (1.14) et puisque $(\ell, M) = 1$, on a pour tout $p|\ell$,

$$\sum_{\nu=0}^{+\infty} \lambda_f(p^{\nu+1}) \lambda_f(p^\nu) p^{-\nu s} = \lambda_f(p) \sum_{\nu=0}^{+\infty} \lambda_f(p^\nu)^2 p^{-\nu s} - \frac{1}{p^s} \sum_{\nu=0}^{+\infty} \lambda_f(p^{\nu+1}) \lambda_f(p^\nu) p^{-\nu s}.$$

Puisque ℓ est sans facteur carré, on déduit de la multiplicativité de λ_f que

$$F(\ell', \ell''; s) = \lambda_f(\ell) \prod_{p|\ell} \left(1 + \frac{1}{p^s}\right)^{-1} \sum_{n=1}^{+\infty} \lambda_f(n)^2 n^{-s}.$$

Puis, grâce à (2.18)

$$F(\ell', \ell''; s) = \lambda_f(\ell) \prod_{p|\ell} \left(1 + \frac{1}{p^s}\right)^{-1} \frac{\zeta^{(M)}(s)}{\zeta^{(M)}(2s)} L(\text{sym}^2 f, s).$$

On calcule alors

$$\text{Rés}_{s=1} F(s) = \lambda_f(\ell) \ell^{1/2} \nu(\ell)^{-1} (\ell_1 \ell_2)^{-k/2} \frac{\Gamma(k)}{(4\pi)^k} \frac{M}{\zeta(2) \nu(M)} L(\text{sym}^2 f, 1).$$

On conclut à l'aide de (2.19). $\square$

Au cours de la preuve ci-dessus, on a montré la

PROPOSITION 2.3.3

Soit M un entier sans facteur carré et $f \in B(M)$. On a

$$L(f \times f, s) = \frac{(4\pi)^{s+k-1}}{\Gamma(s+k-1)} (\zeta^{(M)}(2s) E(z, s), E(z, s))_M$$

Comme $\zeta^{(M)}(2s) E(z, s)$ est méromorphe avec un pôle unique et simple en $s = 1$ [Miy89, (7.2.62) et corollary 7.2.11], on a le

COROLLAIRE 2.3.4

Soit M un entier sans facteur carré et $f \in B(M)$. La fonction $\Gamma(s+k-1) L(f \times f, s)$ est méromorphe avec un unique pôle en $s = 1$. Ce pôle est simple.

Enfin, il est utile de contrôler la taille de $L(\text{sym}^2 f, 1)$, et, notamment grâce aux travaux de Golfeld, Hoffstein et Lieman [GHL94] on a

$$L(\text{sym}^2 f, 1) + L(\text{sym}^2 f, 1)^{-1} \ll \ln(kN). \quad (2.20)$$

La minoration de $L(\text{sym}^2 f, 1)^{-1}$ résulte de l'absence de zéro de Siegel pour la fonction $L(\text{sym}^2 f, s)$ lorsque f n'est pas issue de GL_1 . C'est notamment le cas lorsque le niveau de f est sans facteur carré, seul cas pour lequel (dans ce travail) on a défini $L(\text{sym}^2 f, s)$. Pour tout entier $n \geq 0$ et tout vecteur $\mathbf{b} \in \mathbb{N}^n$, on définit l'ensemble

$$\mathcal{E}_n(\mathbf{b}) = \left\{ \mathbf{d} \in \mathbb{N}^{n-1}; d_i \mid \left(\frac{b_1 \cdots b_i}{d_1 \cdots d_{i-1}}, b_{i+1} \right)^2, 1 \leq i \leq n-1 \right\}$$

avec les conventions $\mathbb{N}^0 = \{1\}$, $\mathcal{E}_1(\mathbf{b}) = \{1\}$, $\mathcal{E}_0(1) = \{1\}$ et $d_1 \cdots d_0 = 1$. On a alors

$$L(\text{sym}^2 f, s)^n = \sum_{r=1}^{+\infty} \rho_f^{(+n)}(r) r^{-s}$$

avec

$$\rho_f^{(+n)}(r) = \sum_{\substack{\mathbf{a}, \mathbf{b} \in \mathbb{N}^n \\ \det \mathbf{a}^2 \mathbf{b} = r \\ (a_1, N) = \cdots = (a_n, N) = 1}} \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{b}) \\ (d_1, N) = \cdots = (d_n, N) = 1}} \lambda_f \left[\left(\frac{b_1 \cdots b_n}{d_1 \cdots d_{n-1}} \right)^2 \right].$$

Enfin, par comparaison des développements eulériens pour tout s tel que $\Re s > 1$, on a

$$L(\text{sym}^2 f, s)^{-1} = \sum_{r=1}^{+\infty} \rho_f^-(r) r^{-s}$$

avec $\rho_f^-(r)$ défini par

$$\rho_f^-(r') \rho_f^-(r'') \quad \text{si } r = r' r'', r' \mid N^\infty, (r'', N) = 1$$

et

$$\begin{cases} \mu(r) r^{-1} & \text{si } r \mid N^\infty; \\ \mu(abc) \mu(b) \lambda_f(a^2 b^2) & \text{si } (r, N) = 1 \text{ et } r = ab^2 c^3 \text{ avec } \mu(abc) \neq 0; \\ 0 & \text{si } (r, N) = 1 \text{ et } r \text{ a un facteur bicarré.} \end{cases}$$

On a alors, pour tout $n \geq 0$ entier

$$L(\text{sym}^2 f, s)^{-n} = \sum_{r=1}^{+\infty} \rho_f^{(-n)}(r) r^{-s}$$

avec, si $(r, N) = 1$, la définition

$$\begin{aligned} \rho_f^{(-n)}(r) = & \sum_{\substack{\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n \\ \det \mathbf{a} \mathbf{b}^2 \mathbf{c}^3 = r}} \mu(a_1 b_1 c_1) \cdots \mu(a_n b_n c_n) \mu(b_1) \cdots \mu(b_n) \\ & \times \sum_{\mathbf{d} \in \mathcal{E}_n(\mathbf{a} \mathbf{b})} \lambda_f \left[\left(\frac{a_1 \cdots a_n b_1 \cdots b_n}{d_1 \cdots d_{n-1}} \right)^2 \right]. \end{aligned}$$

Pour tout r et tout $\varepsilon > 0$, $\rho_f^{(\pm n)}(r) \ll r^\varepsilon$ avec une constante dépendant de ε et n .

2.3.3 Fonction L d'une variété Soit C une variété projective non singulière sur $\mathbb{Q}$. Lorsque p est un nombre premier tel que la réduction modulo p de C est une variété non singulière sur $\mathbb{F}_p$ on dit que p est un *bon* nombre premier (ou encore que p a *bonne réduction* en p). Dans le cas contraire, p est un *mauvais* nombre premier (la variété a *mauvaise réduction*). Si p est un bon nombre premier, on note C_p la réduction de C modulo p et N_n le nombre de points de C à coordonnées dans $\mathbb{F}_{p^n}$.

On sait alors, d'après l'hypothèse de Riemann pour les corps finis que si g est le genre de C , il existe des entiers algébriques $\alpha_1(p), \dots, \alpha_{2g}(p)$ tels que

$$N_n = 1 + p^n - \sum_{i=1}^{2g} \alpha_i(p)^n$$

et pour tout $1 \leq i \leq 2g$, $|\alpha_i(p)| = \sqrt{p}$. On définit alors

$$L(C_p, s)^{-1} = \left(1 - \frac{\alpha_1(p)}{\sqrt{p}} p^{-s}\right) \cdots \left(1 - \frac{\alpha_{2g}(p)}{\sqrt{p}} p^{-s}\right).$$

Lorsque p est un mauvais nombre premier, la définition de $L(C_p, s)$ est plus compliquée. On définit la fonction L de C par

$$L(C, s) = \prod_{p \in \mathcal{P}} L(C_p, s).$$

Les résultats de Wiles, Taylor, Diamond, Conrad et Breuil prouvent qu'il existe un entier N et une forme primitive de poids 2 et de niveau N telle que $L(E, s) = L(f, s)$. Plus généralement, on sait [Roh97, §3.7] grâce aux travaux de Shimura [Shi71, §7.5] que pour toute forme primitive f de poids 2 et de niveau N il existe une variété abélienne sur $\mathbb{Q}$ notée $A_{\overline{f}}$, ne dépendant que de la classe de conjugaison galoisienne de f telle¹⁴ que

$$L(A_{\overline{f}}, s) = \prod_{g \in \text{orbite } f} L(g, s).$$

D'après les travaux de Ribet [Rib80, corollary (4.2)] ces variétés sont simples sur $\mathbb{Q}$. La dimension de $A_{\overline{f}}$ est le cardinal de l'orbite de f

$$\dim A_{\overline{f}} = \# \text{ orbite } f = [\mathbb{Q}(f) : \mathbb{Q}]. \quad (2.21)$$

D'après le théorème de Weil, on a

$$A_{\overline{f}}(\mathbb{Q}) \simeq A_{\overline{f}}^{\text{tors}} \oplus \mathbb{Z}^{\text{rang } A_{\overline{f}}}.$$

La conjecture (faible) de Birch et Swinnerton-Dyer affirme que

$$\text{ord}_{s=1/2} L(A_{\overline{f}}, s) = \text{rang } A_{\overline{f}}$$

et on a alors aisément

$$\text{rang } A_{\overline{f}} = \sum_{g \in \text{orbite } f} \text{ord}_{s=1/2} L(g, s).$$

Dans le cas précis des variétés $A_{\overline{f}}$, cette conjecture est partiellement démontrée grâce aux travaux de Kolyvagin, Logatchev, Gross et Zagier

THÉORÈME 2.3.5

Soit $f \in B(2, N)$

1) si $\text{ord}_{s=1/2} L(f, s) = 0$ alors $\text{rang } A_{\overline{f}} = 0$;

2) si $\text{ord}_{s=1/2} L(f, s) = 1$ alors $\text{rang } A_{\overline{f}} = \# \text{ orbite } f = \dim A_{\overline{f}}$.

¹⁴Il faut là les travaux de Carayol suivant Deligne, Ihara, Langlands. Voir par exemple [Roh97, theorem 5].

Ainsi, on peut calculer le rang de $A_{\overline{f}}$ à partir de l'ordre d'annulation de $L(f, s)$ au point critique $\frac{1}{2}$ et de la taille de l'orbite de f .

REMARQUE 2.8 Ce théorème utilise la stabilité de l'ordre d'annulation par conjugaison galoisienne vue à la proposition (2.2.4).

REMARQUE 2.9 À partir des variétés $A_{\overline{f}}$ on définit

$$J_0(N)^{\text{new}} = \prod_{\text{orbite } f, f \in B(N)} A_{\overline{f}}.$$

C'est la *partie nouvelle* de la jacobienne de $X_0(N)$.

REMARQUE 2.10 La conjecture de Katz et Sarnak, et ses conséquences, vues au paragraphe 2.2.3 impliquent

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^+(2, N)} \#\{f \in B^+(2, N) ; \text{rang } A_{\overline{f}} \neq 0\} = 0$$

et

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^-(2, N)} \#\{f \in B^-(2, N) ; \text{rang } A_{\overline{f}} \neq \dim A_{\overline{f}}\} = 0.$$

Ainsi, en moyenne limite, le rang des facteurs simples de $J_0(N)^{\text{new}}$ est borné. Cela ne dit rien sur le rang des facteurs pris individuellement comme on le verra au chapitre 3. Si on définit $Ell(N)$ (*resp.* $Ell^+(N)$, $Ell^-(N)$) le sous-ensemble des formes f de $B(2, N)$ (*resp.* $B^+(2, N)$, $B^-(2, N)$) telles que $A_{\overline{f}}$ est une courbe elliptique, l'équivalent de la conjecture de Katz et Sarnak affirme qu'en moyenne asymptotique, il n'y a pas de courbes elliptiques de grand rang (voir [Roy01a]). Néanmoins, des calculs numériques tendraient à montrer qu'il existe une proportion non nulle de courbes elliptiques E telles que l'ordre de leur fonction L en $\frac{1}{2}$ ¹⁵ dépasse 2. Les travaux de Zagier et Kramarz [ZK87] donnent l'existence d'une famille de courbes elliptiques E_m vérifiant

$$\frac{\#\{1 \leq m \leq x; m \text{ sans cube, } E_m \text{ paire, } \text{ord}_{s=1} L(E_m, 1) \geq 2\}}{\#\{1 \leq m \leq x; m \text{ sans cube, } E_m \text{ paire}\}} \approx 0, 2$$

pour¹⁶ tout $x \leq 70000$. Brumer et Mac Guinness [BM90] ont construit une famille de 310716 courbes elliptiques dont les fonctions L admettent la répartition par ordre d'annulation en $\frac{1}{2}$ suivante

ordre	0	1	2	3	4
%	30, 04	46, 08	19, 80	3, 82	0, 26

et Fermigier, après Mestre, [Fer96] a donné des méthodes de construction de courbes elliptiques dont l'ordre d'annulation de la fonction L en $\frac{1}{2}$ est grand. Si la conjecture de Katz et Sarnak est vérifiée, cette conclusion serait due au fait que les calculs numériques se font sur des ensembles finis de nombres. Cependant, il y a une différence analytique entre la conjecture de Katz et Sarnak sur $B(2, N)$ et celle sur $Ell(N)$. Grâce aux travaux de Brumer et Silvermann [BS96] (voir aussi [DK00, proposition 1]) l'ensemble $Ell(N)$ est asymptotiquement négligeable devant $B(2, N)$: on a pour tout $\varepsilon > 0$

$$\frac{\#Ell(N)}{\#B(2, N)} \ll N^{-1/2+\varepsilon}$$

la constante dépendant de ε .

¹⁵En fait, les calculs sont faits sur le rang des courbes. Sous la conjecture de Birch et Swinnerton-Dyer, ce rang est aussi l'ordre d'annulation en $1/2$ de la fonction L associée.

¹⁶Une courbe paire est une courbe dont la forme modulaire associée est paire.

Chapitre 3

Facteurs simples de $J_0(N)$

Ce troisième chapitre porte sur l'étude du rang des facteurs des variétés $J_0(N)$. Les résultats de ce chapitre sont parus au *Bulletin de la Société mathématique de France* [Roy00].

3.1 Résultats

Dans ce chapitre, on prouve le

THÉORÈME 3.1.1

Soit p un nombre premier, il existe $C_p \in \mathbb{R}^+$ et $N_p \in \mathbb{N}$ ne dépendant que de p telles que pour tous entiers $N > N_p$ il existe des facteurs $\mathbb{Q}$ -simples X , X^0 et X^1 de $J_0(N)^{\text{new}}$ tels que

- 1) $\dim X \geq C_p \sqrt{\ln \ln N}$;
- 2) $\dim X^0 \geq C_p \sqrt{\ln \ln N}$ et $\text{rang } X^0 = 0$;
- 3) $\text{rang } X^1 = \dim X^1 \geq C_p \sqrt{\ln \ln N}$.

En particulier, il existe des facteurs $\mathbb{Q}$ -simples de $J_0(N)^{\text{new}}$ de rang arbitrairement grand¹. Ce résultat ne dit rien sur les courbes elliptiques puisqu'on a supprimé la condition de dimension qui définit les courbes elliptiques. Le premier point du théorème a été obtenu de façon indépendante et par une méthode qui ne semble pas s'adapter aux autres points par De Jong [DJ].

On sait par (2.21) que si $f \in B(2, N)$, la dimension du facteur simple $A_{\overline{f}}$ est le degré du corps $\mathbb{Q}(f)$ sur $\mathbb{Q}$. En particulier, le facteur de plus grande dimension est donné par la forme de corps $\mathbb{Q}(f)$ de plus haut degré. En adaptant une méthode due à Serre, on cherche, après avoir fixé p à maximiser le degré de $\lambda_f(p)$ lorsque f parcourt $B(2, N)$. Pour le point 1), le sous-ensemble considéré est $B(2, N)$ lui-même. Pour les points 2) et 3), on utilise le théorème 2.3.5. Les sous-ensembles considérés sont alors

$$B^0(2, N) = \left\{ f \in B(2, N) ; L\left(f, \frac{1}{2}\right) \neq 0 \right\}$$

et

$$B^1(2, N) = \{f \in B(2, N) ; \text{ord}_{s=1/2} L(f, s) = 1\}.$$

On évalue la discrétion $D(N)$ des nombres $\lambda_f(p) \in [-2, 2]$ lorsque f parcourt $B(2, N)$ (*resp.* $B^0(2, N)$, $B^1(2, N)$). On sait alors que dans chaque intervalle de

¹L'existence de variétés jacobiniennes simples de grand rang est déjà connue. Voir, par exemple [ST99].

longueur² $4/D(N)$ il y a une valeur $\lambda_f(p)$. Cette remarque permet de compter le nombre de valeurs distinctes de $\lambda_f(p)\sqrt{p}$. Puisque les nombres $\lambda_f(p)\sqrt{p}$ sont des entiers algébriques, d'après le théorème 1.2.6, on en déduit une minoration de leur degré.

Le calcul de discrédance est fait par des méthodes d'analyse de Fourier. On prouve notamment (voir la proposition 3.3.2) la

PROPOSITION 3.1.2

Soit p un nombre premier et $\varepsilon > 0$. Il existe $N_p > 0$ dépendant de ε et p tel que si $N > N_p$ ne divise pas p et si I est un intervalle de longueur

$$\mu_p(I) \geq \frac{p^\varepsilon}{(\ln N)^{1-\varepsilon}}$$

alors il existe $f \in B(2, N)$ – resp. $f^0 \in B^0(2, N)$, $f^1 \in B^1(2, N)$ – telle que

$$\lambda_f(p) \in I, \lambda_{f^0}(p) \in I, \lambda_{f^1}(p) \in I.$$

Il résulte de cette proposition que l'ensemble

$$\bigcup_{N \in \mathbb{N}} \{\lambda_f(p), f \in B(2, N)\}$$

est dense dans $[-2, 2]$ ce qui nous a fait dire page 7 que la majoration de Deligne était optimale.

3.2 Choix des poids

Le but de ce paragraphe est de trouver des poids sur $B(2, N)$, c'est-à-dire des fonctions

$$\Omega_N^p : B(2, N) \rightarrow \mathbb{R}^+$$

qui s'annulent sur les complémentaires des ensembles $B^0(2, N)$ ou $B^1(2, N)$. Ainsi, ces poids « sélectionnent » les formes de $B^0(2, N)$ ou $B^1(2, N)$. Ils permettent de calculer des discrédances et on les cherche de sorte que

$$\sum_{f \in B(2, N)} \Omega_N^p(f) \lambda'_f(p^n) = \mu_p(X_n) + \text{reste}.$$

3.2.1 Choix d'un poids pour la formule d'Eichler-Selberg Si p est premier à N , on a $\chi_N^\square(p^n)p^{-n/2} = \chi_1^\square(p^n)p^{-n/2} = \mu_p(X_n)$ grâce à (1.12). Ainsi, la proposition 1.7.14 donne compte-tenu de (1.33) la

PROPOSITION 3.2.1

Pour tout nombre premier p ne divisant pas le niveau N , tout entier positif ou nul n , tout réel ε strictement positif on a

$$\frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} \lambda_f(p^n) = \mu_p(X_n) + O_\varepsilon \left((p^{n/2}N^{-1} + N^{-1/2})(p^n N)^\varepsilon \right).$$

²En fait, la longueur pour μ_p .

3.2.2 Choix de poids pour $L(f, \frac{1}{2})$ On effectue le même travail pour la formule de trace tordue par $L(f, \frac{1}{2})$.

PROPOSITION 3.2.2

Pour tout entier strictement positif N et tout nombre premier p ne divisant pas N soit la fonction Ω_N^p définie sur $B(2, N)$ par la formule suivante

$$\Omega_N^p(f) = \frac{L^p(f, \frac{1}{2})}{\sum_{f \in B(2, N)} L^p(f, \frac{1}{2})}$$

avec

$$L^p\left(f, \frac{1}{2}\right) = \left(1 - \frac{\lambda_f(p)}{p^{1/2}} + \frac{1}{p}\right) L\left(f, \frac{1}{2}\right).$$

C'est un poids, c'est-à-dire que pour toute forme f de $B(2, N)$ on a

$$\Omega_N^p(f) \geq 0.$$

De plus pour tout entier positif ou nul n la formule de trace suivante est vraie

$$\sum_{f \in B(2, N)} \Omega_N^p(f) \lambda_f(p^n) = \mu_p(X_n) + O_\varepsilon\left((p^n N^{-1/2})^{1/2} (p^n N)^\varepsilon\right)$$

Démonstration – La positivité est conséquence de la positivité de $L(f, \frac{1}{2})$ vue au théorème 2.2.3 et de la proposition 1.2.5 qui donne

$$1 - \frac{\lambda_f(p)}{\sqrt{p}} + \frac{1}{p} \geq \frac{1}{p} \left(\sqrt{p} - 1\right)^2 > 0.$$

On prouve désormais la formule de trace. Si $n = 0$ on a grâce à la proposition 2.2.9

$$\frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} L^p\left(f, \frac{1}{2}\right) = \zeta^{(N)}(2) \left(1 - \frac{1}{p^2}\right) + O_\varepsilon\left(p^\varepsilon N^{-1/4+\varepsilon}\right). \quad (3.1)$$

Si $n \geq 1$, la relation de multiplicativité de Hecke (1.18), et la proposition 2.2.9 donnent

$$\begin{aligned} \frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} L^p\left(f, \frac{1}{2}\right) \lambda_f(p^n) &= \zeta^{(N)}(2) \left(1 - \frac{1}{p^2}\right) \mu_p(X_n) \\ &\quad + O_\varepsilon\left((p^n N^{-1/2})^{1/2} (p^n N)^\varepsilon\right). \end{aligned}$$

Le report de (3.1) dans cette égalité permet de conclure. $\square$

3.2.3 Choix d'un poids pour $(1 + \varepsilon_f(N)) L'(f, \frac{1}{2})$ De même qu'on a prouvé la proposition 3.2.2 on prouve la proposition suivante qui propose un choix de poids pour $(1 + \varepsilon_f(N)) L'(f, \frac{1}{2})$.

PROPOSITION 3.2.3

Pour tout entier strictement positif N , tout nombre premier p ne divisant pas le niveau N , soit le poids $\Omega_N^p(f)$ sur $B(2, N)$ défini par la formule suivante

$$\Omega_N^p(f) = \frac{(1 + \varepsilon_f(N)) L'^p\left(f, \frac{1}{2}\right)}{\sum_{f \in B(2, N)} (1 + \varepsilon_f(N)) L'^p\left(f, \frac{1}{2}\right)}$$

avec

$$L'^p \left(f, \frac{1}{2} \right) = \left(1 - \frac{\lambda_f(p)}{p^{1/2}} + \frac{1}{p} \right) L' \left(f, \frac{1}{2} \right).$$

Pour tout entier positif ou nul n la formule de trace suivante est vraie

$$\sum_{f \in B(2, N)} \Omega_N^p(f) \lambda_f(p^n) = \mu_p(X_n) + O_\varepsilon \left(\frac{(n+1)^2 p^{-n/2+\varepsilon}}{\ln N} + (p^n N^{-1/2})^{1/2} (p^n N)^\varepsilon \right).$$

Démonstration – La positivité est conséquence, outre de la positivité du p -ème facteur eulérien, du théorème 2.2.3 et de (2.13). On prouve la formule de trace. Si $n = 0$ on a grâce à la proposition 2.2.10

$$\begin{aligned} \frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} (1 + \varepsilon_f(N)) L'^p \left(f, \frac{1}{2} \right) &= 2 \left(1 - \frac{1}{p^2} \right) \zeta^{(N)}(2) \ln \frac{\sqrt{N}}{2\pi e^\gamma} \\ &\times \left(1 + O \left(\frac{\ln p}{p \ln N} + p^\varepsilon N^{-1/4+\varepsilon} \right) \right). \end{aligned} \quad (3.2)$$

Si $n \geq 1$ on calcule

$$\begin{aligned} \frac{1}{\#B(2, N)} \sum_{f \in B(2, N)} (1 + \varepsilon_f(N)) L'^p \left(f, \frac{1}{2} \right) \lambda_f(p^n) &= 2 \zeta^{(N)}(2) \ln \frac{\sqrt{N}}{2\pi e^\gamma} E(p, n) + \\ &2 \zeta^{(N)}(2) \hat{E}(p, n) + O_\varepsilon \left(p^{n(1+\varepsilon)/2} N^{-1/4+\varepsilon} \right). \end{aligned} \quad (3.3)$$

Dans cette équation,

$$E(p, n) = (f(p^n, 0) - f(p^{n-1}, 0)) p^{-n/2} + (f(p^n, 0) - f(p^{n+1}, 0)) p^{-n/2-1}$$

et

$$\hat{E}(p, n) = (\hat{f}(p^n, 0) - \hat{f}(p^{n-1}, 0)) p^{-n/2} + (\hat{f}(p^n, 0) - \hat{f}(p^{n+1}, 0)) p^{-n/2-1}.$$

Ces fonctions ont été calculées et grâce au lemme 2.2.8 on a

$$E(p, n) = \left(1 - \frac{1}{p^2} \right) \mu_p(X_n) \quad (3.4a)$$

$$\hat{E}(p, n) \ll n^2 p^{-n/2+\varepsilon}. \quad (3.4b)$$

En reportant (3.4a) et (3.4b) dans (3.3) on obtient le résultat énoncé grâce à (3.2). $\square$

3.3 Discrépance des valeurs propres de Hecke

Dans ce paragraphe, on calcule la discrépance des valeurs $\lambda_f(p)$ lorsque f parcourt certains sous-ensembles de $B(2, N)$. On a pour cela besoin de bonnes fonctions d'approximations lisses des fonctions caractéristiques d'intervalles.

LEMME 3.3.1

Pour tout $[a, b] \subset]-2, 2[$ et tout $\Delta \in [0, 2]$ il existe une fonction infiniment dérivable $F_{\Delta, a, b}$ sur $[-2, 2]$ ayant les propriétés suivantes

- 1) $F_{\Delta, a, b}$ est constamment égale à 1 sur $[a, b]$;

- 2) $F_{\Delta,a,b}$ est nulle sur $]-\infty, a - \Delta[\cup]b + \Delta, +\infty[$ et sur $\mathbb{R} \setminus [-2, 2]$;
 3) $\chi_{[a,b]} \leq F_{\Delta,a,b}$;
 4) $\left| \int_{-2}^2 F_{\Delta,a,b}(x) - \chi_{[a,b]}(x) \, dx \right| \leq 2\Delta$;
 5) il existe une suite réelle $(\hat{F}(n))_{n \geq 0}$ telle que pour tout $n \geq 1$ et tout $k \geq 0$ on a

$$\left| \hat{F}(n) \right| \ll_k \Delta^{-k} n^{-k} \quad (3.5)$$

et telle que la série

$$\sum_{n \geq 0} \hat{F}(n) X_n$$

converge normalement vers $F_{\Delta,a,b}$ sur $[-2, 2]$.

Démonstration – On introduit la fonction cloche infiniment dérivable, définie sur $\mathbb{R}$ par

$$g(t) = \begin{cases} 0 & \text{si } t \leq 0 ; \\ \exp(-\frac{1}{t^2(t-1)^2}) & \text{si } t \in [0, 1] ; \\ 0 & \text{si } t \geq 1. \end{cases}$$

On construit alors la fonction $\tilde{F}_{\Delta,a,b}$

$$\tilde{F}_{\Delta,a,b}(t) = \frac{1}{(\int_{-\infty}^{\infty} g(x) \, dx)^2} \left(\int_{-\infty}^{\frac{t-a+\Delta}{\Delta}} g(x) \, dx \right) \left(\int_{-\infty}^{\frac{b+\Delta-t}{\Delta}} g(x) \, dx \right).$$

Si $a - \Delta < -2$ on pose $F_{\Delta,a,b}(t) = \tilde{F}_{\Delta,a,b}(t)$ si $t \in [-2, 2]$ et $F_{\Delta,a,b}(t) = 0$ sinon. Si $b + \Delta > 2$ on pose $F_{\Delta,a,b}(t) = \tilde{F}_{\Delta,a,b}(t)$ si $t \in [-2, 2]$ et $F_{\Delta,a,b}(t) = 0$ sinon. Dans les autres cas, on pose $F_{\Delta,a,b} = \tilde{F}_{\Delta,a,b}$. C'est une fonction plateau qui vérifie les conditions 1) à 4). On pose alors

$$\hat{F}(n) := \int_{-2}^2 F_{\Delta,a,b} X_n \, d\mu_{\infty}.$$

On remarque que par changement de variable $x = 2 \cos \varphi$ on a

$$\begin{aligned} \hat{F}(n) &= \frac{2}{\pi} \int_0^{\pi} F_{\Delta,a,b}(2 \cos \varphi) \sin \varphi \sin(n+1) \varphi \, d\varphi \\ &= \frac{1}{\pi} \int_0^{\pi} F_{\Delta,a,b}(2 \cos \varphi) \cos n\varphi \, d\varphi - \frac{1}{\pi} \int_0^{\pi} F_{\Delta,a,b}(2 \cos \varphi) \cos(n+2)\varphi \, d\varphi. \end{aligned} \quad (3.6)$$

Pour $n \neq 0$ une intégration par parties de chacune des intégrales et la majoration absolue

$$\|F'_{\Delta,a,b}\|_{\infty} \ll \Delta^{-1}$$

donnent $|\hat{F}(n)| \ll \Delta^{-1} n^{-1}$. En réitérant ce processus k fois on obtient la majoration (3.5). Puisque $\|X_n\|_{\infty} \ll n+1$ on en déduit que la série

$$\sum_{n \geq 0} \hat{F}(n) X_n$$

converge normalement sur $[-2, 2]$ vers une fonction $\tilde{F}$ infiniment dérivable. En utilisant l'orthonormalité des polynômes X_n pour $d\mu_{\infty}$ on vérifie que

$$\frac{\pi}{2} \hat{F}(n) = \int_0^{\pi} \tilde{F}(2 \cos \varphi) \sin \varphi \sin(n+1) \varphi \, d\varphi$$

et par comparaison avec (3.6) on trouve que $F_{\Delta,a,b} \circ (2 \cos)$ et $\tilde{F} \circ (2 \cos)$ ont mêmes coefficients de Fourier. Ainsi $F_{\Delta,a,b}$ et $\tilde{F}$ coïncident sur $[-2, 2]$. Ceci prouve la dernière assertion du lemme. $\square$

Les termes d'erreur impliqués par nos formules de trace (propositions 3.2.1, 3.2.2 et 3.2.3) sont tous majorés par

$$O_\varepsilon \left(\frac{(n+1)^2 p^{-n/2+\varepsilon}}{\ln N} + (p^n N^{-1/2})^{1/2} (p^n N)^\varepsilon \right).$$

PROPOSITION 3.3.2

Soit $\Omega_N^p(f)$ un poids sur $B(2, N)$, on suppose avoir la majoration suivante pour tout nombre premier p , tout entier positif ou nul n et tout entier strictement positif N premier à p

$$\sum_{f \in B(2, N)} \Omega_N^p(f) \lambda_f(p^n) - \mu_p(X_n) \ll_\varepsilon \frac{(n+1)^2 p^{-n/2+\varepsilon}}{\ln N} + (p^n N^{-1/2})^{1/2} (p^n N)^\varepsilon. \quad (3.7)$$

Soit p un nombre premier. Pour tout ε réel strictement positif assez petit, il existe N_p dépendant de p et ε tel que pour tout $N > N_p$ premier à p , tout sous-intervalle de $[-2, 2]$ de μ_p -longueur $(\ln N)^{-1+\varepsilon} p^\varepsilon$ contient au moins une valeur propre $\lambda_f(p)$ associée à un vecteur propre $f \in B(2, N)$ vérifiant $\Omega_N^p(f) \neq 0$.

Démonstration – Soit I un intervalle ne contenant aucune valeur propre $\lambda_f(p)$. On désigne par $F_{\Delta,J}$ une fonction infiniment dérivable à support compact dans I constamment égale à 1 sur J et telle que si I_1 et I_2 sont les deux morceaux complémentaires de J dans I , ils sont tous deux de μ_p -longueurs inférieures à Δ . On suppose de plus que $\|F_{\Delta,J}^{(k)}\|_\infty \ll_k \Delta^{-k}$. On a alors

$$\mu_p(I) = \mu_p(J) + \mu_p(I_1 \cup I_2) \leq \int_{-2}^2 F_{\Delta,J} d\mu_p + 2\Delta. \quad (3.8)$$

Or I ne contient aucune valeur propre $\lambda_f(p)$ donc

$$\sum_{f \in B(2, N)} \Omega_N^p F_{\Delta,J}(\lambda_f(p)) = 0$$

et (3.8) devient

$$\mu_p(I) \leq \left| \sum_{f \in B(2, N)} \Omega_N^p(f) F_{\Delta,J}(\lambda_f(p)) - \int_{-2}^2 F_{\Delta,J} d\mu_p \right| + 2\Delta.$$

On obtient alors le résultat annoncé par utilisation du lemme 3.3.3 et le choix

$$\Delta = (\ln N)^{-1+\varepsilon} \quad \text{et} \quad k = \left\lfloor \frac{3}{\varepsilon} \right\rfloor + 1.$$

$\square$

LEMME 3.3.3

Soit p un nombre premier. Soit une suite de réels positifs $\{\Omega_N^p(f)\}$, soit $\Delta > 0$ et F une fonction infiniment dérivable à support compact dans $]-2, 2[$ vérifiant $\|F^{(k)}\|_\infty \ll_k$

Δ^{-k} pour tout entier positif ou nul k . Pour tout entier $k \geq 2$ et tout réel $\varepsilon \in]0, 1[$ il existe N_p dépendant de ε , k et p tel que pour tout $N > N_p$ premier à p l'hypothèse (3.7) implique

$$\begin{aligned} \sum_{f \in B(2, N)} \Omega_N^p(f) F(\lambda_f(p)) - \int_{-2}^2 F d\mu_p &\ll_{k, \varepsilon} (\ln p)^{k-2} (\ln N)^2 (\Delta \ln N)^{-k} \\ &+ \frac{p^\varepsilon}{\ln N} (1 + (\ln p)^{k-2} (\ln N)^2 (\Delta \ln N)^{-k}) + N^{-7/36 + \varepsilon}. \end{aligned}$$

La constante impliquée par le symbole de Vinogradov ne dépend que de k et ε .

Démonstration – La fonction F admet un développement $\sum \widehat{F}(n) X_n$ avec

$$\widehat{F}(n) = \int_{-2}^2 F X_n d\mu_\infty. \quad (3.9)$$

Soit $M \geq 2$ à choisir. On commence par remplacer F par la série partielle

$$F_M = \sum_{n=0}^M \widehat{F}(n) X_n.$$

On a alors en utilisant la positivité du poids

$$\begin{aligned} \left| \sum_{f \in B(2, N)} \Omega_N^p(f) F(\lambda_f(p)) - \int_{-2}^2 F d\mu_p \right| &\leq \sum_{f \in B(2, N)} \Omega_N^p(f) \|F - F_M\|_\infty \\ &+ \left| \sum_{f \in B(2, N)} \Omega_N^p(f) F_M(\lambda_f(p)) - \int_{-2}^2 F_M d\mu_p \right| + \int_{-2}^2 \|F - F_M\|_\infty d\mu_p. \end{aligned} \quad (3.10)$$

Comme dans la preuve du lemme 3.3.1, on montre $|\widehat{F}(n)| \ll_k n^{-k} \Delta^{-k}$. De plus $\|X_n\|_\infty \ll n$ de sorte que

$$\|F - F_M\|_\infty \ll_k \Delta^{-k} M^{-k+2}. \quad (3.11)$$

Puis, utilisant $\mu_p([-2, 2]) = 1$, (3.7) pour $n = 0$ et (3.11) on transforme (3.10) en

$$\begin{aligned} \sum_{f \in B(2, N)} \Omega_N^p(f) F(\lambda_f(p)) - \int_{-2}^2 F d\mu_p &\ll_k \Delta^{-k} M^{-k+2} \left(1 + \frac{p^\varepsilon}{\ln N}\right) + \\ &\left| \sum_{f \in B(2, N)} \Omega_N^p(f) F_M(\lambda_f(p)) - \int_{-2}^2 F_M d\mu_p \right|. \end{aligned} \quad (3.12)$$

On transforme ensuite la valeur absolue de droite

$$\begin{aligned} \left| \sum_{f \in B(2, N)} \Omega_N^p(f) F_M(\lambda_f(p)) - \int_{-2}^2 F_M d\mu_p \right| &\leq \\ &\sum_{n=0}^M |\widehat{F}(n)| \left| \sum_{f \in B(2, N)} \Omega_N^p(f) X_n(\lambda_f(p)) - \int_{-2}^2 X_n d\mu_p \right|. \end{aligned}$$

Mais $X_n(\lambda_f(p)) = \lambda_f(p^n)$ donc, grâce à (3.7) et à $|\widehat{F}(n)| \ll 1$

$$\left| \sum_{f \in B(2, N)} \Omega_N^p(f) F_M(\lambda_f(p)) - \int_{-2}^2 F_M d\mu_p \right| \ll_\varepsilon \frac{p^\varepsilon}{\ln N} + (p^M N^{-1/2})^{1/2} (p^M N)^\varepsilon. \quad (3.13)$$

Puis reportant (3.13) dans (3.12) et choisissant $M = \lfloor \frac{\ln N}{9 \ln p} \rfloor$ on obtient le résultat énoncé dans le lemme. $\square$

REMARQUE 3.1 La positivité de $L(f, \frac{1}{2})$ et $(1 + \varepsilon_f(N))L'(f, \frac{1}{2})$ permet d'écrire

$$\sum |\Omega_N^p(f)| = \sum \Omega_N^p(f).$$

Sans cela (qui n'est pas connu en poids supérieurs à 2) il faut savoir majorer $\sum \Omega_N^p(f)^2$ ce qui est plus délicat.

Le lemme suivant donne une minoration du nombre de formes primitives relativement à N n'annulant pas le poids et ayant des valeurs propres de Hecke distinctes.

LEMME 3.3.4

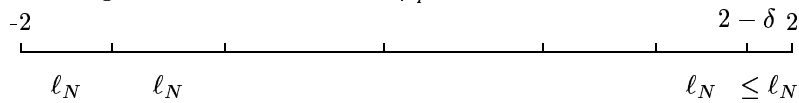
Sous les hypothèses de la proposition 3.3.2 pour tout ε , tout $N > N_p$ premier à p on a

$$\#\{\lambda_f(p) \text{ distinctes}, f \in B(2, N) \mid \Omega_N^p(f) \neq 0\} \geq (\ln N)^{1-\varepsilon} p^{-\varepsilon}.$$

Démonstration – D'après la proposition 3.3.2 tout intervalle de μ_p -longueur

$$\ell_N = (\ln N)^{-1+\varepsilon} p^\varepsilon$$

contient au moins une valeur propre $\lambda_f(p)$ avec $\Omega_N^p(f) \neq 0$. on fabrique une suite d'intervalles ouverts disjoints de μ_p -longueur ℓ_N couvrant l'intervalle $]-2, 2 - \delta[$ moins un nombre fini de points (les bords de ces intervalles) avec δ choisi assez petit pour que $0 \leq \mu_p(]2 - \delta, 2[) < \ell_N$. Ce choix est résumé sur le schéma suivant où les longueurs sont mesurées par μ_p .



Comme la $\mu(p)$ -longueur de $]-2, 2[$ est 1, il y a

$$\frac{1 - \mu_p(]2 - \delta, 2[)}{(\ln N)^{-1+\varepsilon} p^\varepsilon}$$

tels intervalles. On a vu que chacun d'eux contient au moins un $\lambda_f(p)$ d'où le résultat. $\square$

REMARQUE 3.2 Si les polynômes caractéristiques des opérateurs de Hecke étaient à racines simples³, on pourrait remplacer $(\ln N)^{1-\varepsilon}$ par $\#B(2, N)$.

³Cette « conjecture » est trop brutale. Les tables de Stein [Ste98] montrent que l'opérateur T_2 sur $S(2, 487) = S^n(2, 487)$ a un polynôme caractéristique dont 0 est racine d'ordre 4. Il faudrait en fait savoir contrôler la multiplicité des valeurs propres.

3.4 Comptage d'entiers algébriques

On note (toujours) $t_f(p) = \sqrt{p}\lambda_f(p)$. On sait que $t_f(p)$ appartient à l'ensemble $\mathcal{E}(2\sqrt{p})$ des entiers algébriques de conjugués tous réels et tous de norme inférieure à $2\sqrt{p}$. On suppose que tous les $t_f(p)$ sont de degrés inférieurs ou égaux à $d(N, p)$. Ils appartiennent alors au sous-ensemble $\mathcal{E}(2\sqrt{p}, d(N, p))$ des éléments de $\mathcal{E}(2\sqrt{p})$ de degré au plus $d(N, p)$. L'ensemble $\mathcal{E}(2\sqrt{p}, d(N, p))$ est fini : à chaque orbite galoisienne d'un élément de $\mathcal{E}(2\sqrt{p}, d(N, p))$ on peut associer un unique polynôme unitaire à coefficients dans $\mathbb{Z}$, de degré inférieur ou égal à $d(N, p)$ et dont toutes les racines sont majorées en norme par $2\sqrt{p}$. On note $\mathcal{P}(2\sqrt{p}, d(N, p))$ l'ensemble de ces polynômes. Chaque orbite contenant au plus $d(N, p)$ éléments, on a

$$\#\mathcal{E}(2\sqrt{p}, d(N, p)) \leq d(N, p) \#\mathcal{P}(2\sqrt{p}, d(N, p)). \quad (3.14)$$

LEMME 3.4.1

Pour $M \geq 1$ et $d \geq 2$, nous notons $\mathcal{P}(M, d)$ l'ensemble des polynômes unitaires à coefficients dans $\mathbb{Z}$ de degré au plus d et dont toutes les racines sont majorées en norme par M . Alors

$$\#\mathcal{P}(M, d) \leq (6M)^{d^2}.$$

Démonstration – Si $P = \sum_{i=0}^d \rho_i X^{d-i} \in \mathcal{P}(M, d)$ alors en notant $y_1, \dots, y_d$ ses racines, on a

$$\rho_i = (-1)^i \sum_{1 \leq j_1 < \dots < j_i \leq d} y_{j_1} \dots y_{j_i}, \quad (1 \leq i \leq d).$$

Chacune des racines étant majorées en norme par M on a grâce à l'expression précédente de ρ_i la majoration

$$|\rho_i| \leq C_d^i M^i.$$

Un polynôme unitaire est un choix de d valeurs de ρ_i et il y a $1 + 2C_d^i M^i$ valeurs possibles de ρ_i . On majore donc le cardinal de $\mathcal{P}(M, d)$ par

$$\#\mathcal{P}(M, d) \leq \prod_{i=1}^d \left(1 + 2 \binom{d}{i} M^i\right) \leq \prod_{i=1}^d 3 \binom{d}{i} M^i \leq (6M)^{d^2}.$$

□

REMARQUE 3.3 La majoration du lemme précédent n'est pas précise. Il apparaît néanmoins impossible d'améliorer le d^2 en d^α avec $\alpha < 2$ qui est la seule amélioration utile pour la suite.

On utilise ce lemme pour majorer $\#\mathcal{E}(2\sqrt{p}, d(N, p))$.

LEMME 3.4.2

Pour $M \geq 1$ et $d \geq 2$ on note $\mathcal{E}(M, d)$ l'ensemble des entiers algébriques totalement réels dont tous les conjugués sont majorés en norme par M et de degré inférieur à d . Alors

$$\#\mathcal{E}(M, d) \leq (8M)^{d^2}.$$

Démonstration – Grâce à la majoration (3.14) et au lemme 3.4.1 on a

$$\#\mathcal{E}(M, d) \leq d (6M)^{d^2} \leq (8M)^{d^2}.$$

□

3.5 Preuve du théorème 3.1.1

3.5.1 Noyau de la preuve On considère un poids Ω_N^p sur $B(2, N)$ satisfaisant aux conditions de la proposition 3.3.2 et dont la non-nullité est stable par action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ – c'est-à-dire que $\Omega_N^p(f) \neq 0$ reste vraie si on remplace f par f^σ où σ est n'importe quel élément de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On note $d(\Omega, N)$ le degré maximum des entiers algébriques $t_f(p)$ quand f parcourt le sous-ensemble des formes de $B(2, N)$ qui n'annulent pas Ω_N^p . Ce nombre est aussi le cardinal de la plus grande orbite sous $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ des $\lambda_f(p)$ quand $\Omega_N^p(f) \neq 0$

$$\begin{aligned} d(\Omega, N) &= \max_{\substack{f \in B(2, N) \\ \Omega_N^p(f) \neq 0}} \# \{ \sigma(\lambda_f(p)), \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \} \\ &= \max_{\substack{f \in B(2, N) \\ \Omega_N^p(f) \neq 0}} \deg(\lambda_f(p)). \end{aligned}$$

On a

$$\# \{ \lambda_f(p), f \in B(2, N), \Omega_N^p(f) \neq 0 \} \leq \# \mathcal{E}(2\sqrt{p}, d(\Omega, N)). \quad (3.15)$$

Grâce au lemme 3.4.2 on majore le membre de droite de (3.15)

$$\# \{ \lambda_f(p), f \in B(2, N), \Omega_N^p(f) \neq 0 \} \leq (16\sqrt{p})^{d(\Omega, N)^2}. \quad (3.16)$$

Mais on peut minorer le terme de gauche de (3.16) grâce au lemme 3.3.4. Ce faisant on transforme (3.16) en

$$(\ln N)^{1-\varepsilon} p^{-\varepsilon} \leq (16\sqrt{p})^{d(\Omega, N)^2}. \quad (3.17)$$

L'extraction de $d(\Omega, N)$ de (3.17) en donne la minoration

$$d(\Omega, N) \geq \sqrt{\frac{2(1-\varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

Si la non-annulation de Ω_N^p est stable par action de Galois alors en écrivant

$$\max_{f \in B(2, N)} \# \{ f^\sigma, \Omega_N^p(f^\sigma) \neq 0 \} \geq \max_{\substack{f \in B(2, N) \\ \Omega_N^p(f) \neq 0}} \# \{ \sigma(\lambda_f(p)), \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \}$$

on obtient la minoration suivante

$$\max_{f \in B(2, N)} \# \{ f^\sigma, \Omega_N^p(f^\sigma) \neq 0 \} \geq \sqrt{\frac{2(1-\varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

On résume ce qui précède dans le

LEMME 3.5.1

Soit p un nombre premier. Soit Ω_N un poids sur $B(2, N)$ qui satisfait aux conditions de la proposition 3.3.2. On suppose de plus que la non-annulation de ce poids est stable par action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On note

$$d(\Omega, N) = \max_{\substack{f \in B(2, N) \\ \Omega_N^p(f) \neq 0}} \# \{ \sigma(\lambda_f(p)), \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \}.$$

Pour tout ε strictement positif assez petit, il existe alors un entier N_p dépendant de p et ε tel que si $N \geq N_p$ est premier à p

$$d(\Omega, N) \geq \sqrt{\frac{2(1-\varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

De plus,

$$\max_{f \in B(2, N)} \# \{f^\sigma, \Omega_N^p(f^\sigma) \neq 0\} \geq \sqrt{\frac{2(1-\varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

3.5.2 Facteurs simples Si $\bar{f}$ est l'orbite d'une forme primitive f de $B(2, N)$ sous $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a vu que la dimension du facteur $\mathbb{Q}$ -simple $A_{\bar{f}}$ est le cardinal de $\bar{f}$. On considère le poids défini pour $f \in B(2, N)$ par

$$\Omega_N^p(f) = \frac{1}{\#B(2, N)}.$$

Il ne s'annule pour aucune forme f et vérifie les conditions de la proposition 3.3.2 grâce à la proposition 3.2.1. On peut donc appliquer le lemme 3.5.1 et en déduire la proposition suivante grâce à la seconde minoration du lemme.

PROPOSITION 3.5.2

Soit p un nombre premier. Pour tout réel ε strictement positif assez petit, il existe une constante $C_0 > 0$ et un entier N_0 dépendants de ε et p tels que pour tout entier $N > N_0$ premier à p il existe un facteur $\mathbb{Q}$ -simple X de la jacobienne $J_0^{\text{new}}(N)$ dont la dimension vérifie l'inégalité suivante

$$\dim X \geq \sqrt{\frac{2(1-\varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

3.5.3 Facteurs simples de rang nul On restreint notre étude aux facteurs $\mathbb{Q}$ -simples $A_{\bar{f}}$ de rang 0. On sait que ces facteurs $A_{\bar{f}}$ sont ceux associés à des formes f telles que $L(f, \frac{1}{2}) \neq 0$ – on rappelle que $L(f, \frac{1}{2}) \neq 0$ si et seulement si $L(f^\sigma, \frac{1}{2}) \neq 0$ pour tout $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On considère le poids défini pour $f \in B(2, N)$ par

$$\Omega_N^p(f) = \frac{L^p(f, \frac{1}{2})}{\sum_{f \in B(2, N)} L^p(f, \frac{1}{2})}.$$

La non-annulation de ce poids est stable par action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $B(2, N)$. Enfin on a $\Omega_N^p(f) = 0$ si et seulement si $L(f, \frac{1}{2}) = 0$ donc $\Omega_N^p(f) \neq 0$ si et seulement si $\text{rang } A_{\bar{f}} = 0$. Grâce à la proposition 3.2.2 on sait que le poids Ω_N^p vérifie les conditions de la proposition 3.3.2 et que on peut lui appliquer le lemme 3.5.1 pour en déduire la proposition suivante.

PROPOSITION 3.5.3

Soit p un nombre premier. Pour tout réel ε strictement positif assez petit, il existe une constante $C_1 > 0$ et un entier N_1 dépendants de ε et p tels que pour tout entier $N > N_1$ premier à p il existe un facteur $\mathbb{Q}$ -simple X de la jacobienne $J_0^{\text{new}}(N)$ de rang 0 et dont la dimension vérifie l'inégalité suivante

$$\dim X \geq \sqrt{\frac{2(1-\varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

3.5.4 Facteurs simples de grand rang On étudie les facteurs $\mathbb{Q}$ -simples $A_{\bar{f}}$ associé à des formes f telles que $L(f, \frac{1}{2}) = 0$ et $L'(f, \frac{1}{2}) \neq 0$ – cette condition étant stable par action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $B(2, N)$. On a vu que le rang de Mordell-Weil est donné par la formule suivante

$$\text{rang } A_{\bar{f}} = \sum_{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \text{ord}_{s=1/2} L(f^\sigma, s).$$

Ainsi, lorsque $\text{ord}_{s=1/2} L(f, s) = 1$ on sait que $\text{ord}_{s=1/2} L(f^\sigma, s) = 1$ et donc on a

$$\text{rang } A_{\overline{f}} = \sharp \overline{f} = \dim A_{\overline{f}}.$$

On considère alors le poids défini pour $f \in B(2, N)$ par

$$\Omega_N^p(f) = \frac{(1 + \varepsilon_f(N)) L'^p(f, \frac{1}{2})}{\sum_{f \in B(2, N)} (1 + \varepsilon_f(N)) L'^p(f, \frac{1}{2})}$$

Si $\Omega_N^p(f) = 0$ alors

- 1) soit $\varepsilon_f(N) = -1$. Dans ce cas
 - a) soit $L(f, \frac{1}{2}) \neq 0$ et alors $\text{ord}_{s=1/2} L(f, s) = 0$;
 - b) soit $L(f, \frac{1}{2}) = 0$, par (2.5) on a alors $L'(f, \frac{1}{2}) = 0$ et $\text{ord}_{s=1/2} L(f, s) > 1$.
- 2) soit $\varepsilon_f(N) = 1$. Dans ce cas $L'(f, \frac{1}{2}) = 0$ et on a la même conclusion.

Réciproquement, si $\text{ord}_{s=1/2} L(f, s) \neq 1$ alors

- 1) soit $\text{ord}_{s=1/2} L(f, s) > 1$ d'où $L'(f, \frac{1}{2}) = 0$ puis $\Omega_N^p(f) = 0$;
- 2) soit $\text{ord}_{s=1/2} L(f, s) = 0$ d'où $L(f, \frac{1}{2}) \neq 0$ puis $\varepsilon_f(N) = -1$ grâce à (2.13).

Finalement, $\Omega_N^p(f) = 0$ si et seulement si $\text{ord}_{s=1/2} L(f, s) > 1$ et Ω_N^p détecte les formes d'ordre 1. On déduit alors de la proposition 2.2.4 que la non-annulation de ce poids est stable par action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Grâce à la proposition 3.2.3 on sait que le poids $\Omega_N^p(f)$ vérifie les conditions de la proposition 3.3.2 et qu'on peut lui appliquer le lemme 3.5.1 pour en déduire la

PROPOSITION 3.5.4

Soit p un nombre premier. Pour tout réel ε strictement positif assez petit, il existe une constante $C_2 > 0$ et un entier N_2 dépendants de ε et p tels que pour tout entier $N > N_2$ premier à p il existe un facteur $\mathbb{Q}$ -simple X de la jacobienne $J_0^{\text{new}}(N)$ de rang 0 et dont la dimension vérifie l'inégalité suivante

$$\text{rang } X = \dim X \geq \sqrt{\frac{2(1 - \varepsilon) \ln \ln N}{\ln(4p)}} - 2\varepsilon.$$

Conclusion

La minoration calculée, en $\sqrt{\ln \ln N}$ est en deçà des résultats attendus au vu de l'expérimentation numérique. Les calculs de A. Brumer [Bru95b] laissent prévoir que les facteurs de $J_0^{\text{new}}(N)$ sont de taille comparable à la dimension de $J_0^{\text{new}}(N)$ – au moins lorsque N est premier.

Une des pertes d'information de la méthode pourrait avoir lieu lorsqu'on majore le degré du corps de rationalité en ne considérant qu'un seul des coefficients qui l'engendrent. Néanmoins Cohen m'a indiqué que ses tests numériques tendent à montrer que la perte d'information est faible.

Une autre perte a lieu lorsqu'on « oublie » que les valeurs propres des opérateurs de Hecke ne sont pas seulement des entiers algébriques mais que leurs conjugués sont tous réels. Est-ce que les polynômes de degré d à racines toutes réelles bornées par M et à coefficients entiers sont de densité non-nulle parmi les polynômes de degré d à racines bornées par M et à coefficients entiers ?

Sarnak m'a informé que (numériquement) la répartition des valeurs $\lambda_f(p)$ était de Poisson et que l'analyse de Fourier pouvait difficilement détecter les points de telles distributions, trop rapprochés (principe d'incertitude de l'analyse de Fourier). Finalement, une approche plus algébrique pourrait consister à appréhender l'ordre de multiplicité des valeurs propres des opérateurs de Hecke.

Chapitre 4

Petits zéros

Ce quatrième chapitre étudie la répartition des petits zéros des fonctions L de formes modulaires. Les résultats sont à paraître à *Acta Arithmetica* [Roy01b].

4.1 Résultats

On a exprimé, page 31, la conjecture de Katz et Sarnak pour la statistique du j^{e} zéro. On en donne une version pour la statistique des petits zéros. Soit $F = (F(Q))$ un ensemble d'ensembles disjoints de formes modulaires indexé par un paramètre Q . À chaque forme f d'un ensemble $F(Q)$ est associé un réel c_Q appelé conducteur de f et ne dépendant que de la famille $F(Q)$ contenant f . Les zéros non triviaux de la fonction L d'une forme $f \in F(Q)$ sont notés $\frac{1}{2} + i\gamma_f$. Si on admet l'hypothèse de Riemann généralisée, on a $\gamma_f \in \mathbb{R}$. On introduit un opérateur de comptage de ces zéros

$$D(f, \phi) = \sum_{\gamma_f} \phi\left(\frac{\gamma_f}{2\pi} \ln c_Q\right)$$

où ϕ est une fonction la classe de Schwartz $\mathcal{S}(\mathbb{R})$ de transformée de Fourier à support compact. La conjecture de densité prédit, pour toute ensemble F raisonnable, l'existence d'une distribution $W(F)$ telle que

$$\lim_{Q \rightarrow \infty} \frac{1}{\#F(Q)} \sum_{f \in F(Q)} D(f, \phi) = \int_{\mathbb{R}} \phi(t) W(F)(t) dt.$$

La conjecture affirme de plus que cette fonction $W(F)$ est la fonction de densité des valeurs propres (correctement normalisées) d'un groupe de symétrie.

Un pas vers cette conjecture a été effectué par Iwaniec, Luo et Sarnak [ILS00] dans le

THÉORÈME 4.1.1

Fixons $\phi \in \mathcal{S}(\mathbb{R})$ de transformée de Fourier à support dans $] -2, 2[$. Alors, lorsque N parcourt les entiers sans facteur carré

$$\lim_{N \rightarrow \infty} \frac{1}{\#B(k, N)} \sum_{f \in B(k, N)} D(f, \phi) = \int_{-\infty}^{\infty} \phi(x) W^O(x) dx,$$

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^+(k, N)} \sum_{f \in B^+(k, N)} D(f, \phi) = \int_{-\infty}^{\infty} \phi(x) W^{SO(\text{pair})}(x) dx,$$

et

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^-(k, N)} \sum_{f \in B^-(k, N)} D(f, \phi) = \int_{-\infty}^{\infty} \phi(x) W^{SO(\text{impair})}(x) dx$$

avec

$$W^O(x) = 1 + \frac{1}{2} \delta_0(x),$$

$$W^{SO(\text{pair})}(x) = 1 + \frac{\sin(2\pi x)}{2\pi x},$$

et

$$W^{SO(\text{impair})}(x) = 1 - \frac{\sin(2\pi x)}{2\pi x} + \delta_0(x).$$

Dans ce chapitre, on fait un pas supplémentaire vers la conjecture en considérant les ensembles de formes modulaires plus petits que sont les ensembles de formes signées. On prouve le

THÉORÈME 4.1.2

Soit k et ℓ des entiers strictement positifs fixés avec k pair. Soit κ un réel vérifiant $0 < \kappa \leq 1/\ell$. L'hypothèse de Riemann est supposée vraie pour les fonctions L de Dirichlet et pour les fonctions L associées aux formes primitives de poids k . Soit $\varepsilon = (\varepsilon_1, \dots, \varepsilon_\ell)$ un vecteur de $\{-1, 1\}^\ell$. Soit ϕ une fonction paire de $\mathcal{S}(\mathbb{R})$ de transformée de Fourier à support compact dans $] -2, 2[$. On considère une suite d'entiers N sans facteur carré ayant exactement ℓ facteurs premiers $p_1, \dots, p_\ell$ tels que $N^\kappa \leq p_1 < \dots < p_\ell$. Alors on a

$$\lim_{N \rightarrow \infty} \frac{1}{\#B^\varepsilon(k, N)} \sum_{f \in B^\varepsilon(k, N)} D(f, \phi) = \int_{-\infty}^{\infty} W(x) \phi(x) dx$$

où W est définie par :

si $i^{k\varepsilon_1} \dots \varepsilon_\ell = 1$ alors

$$W(x) = W^{SO(\text{pair})}(x)$$

si $i^{k\varepsilon_1} \dots \varepsilon_\ell = -1$ alors

$$W(x) = W^{SO(\text{impair})}(x)$$

où δ_0 est la distribution de Dirac en 0.

Les fonctions de densité W sont reliées à la répartition des valeurs propres des matrices aléatoires¹ (voir [KS99b] et [KS99a]). Soit A une matrice de $U(N)$ [KS99a, AD]. Elle est équivalente à une matrice $\text{diag}(e^{i\varphi_1(A)}, \dots, e^{i\varphi_N(A)})$ avec $0 \leq \varphi_1(A) \leq \dots \leq \varphi_N(A) < 2\pi$. On définit les phases propres de A par

$$\varphi_{j+\ell N}(A) = \varphi_j(A) + 2\pi\ell, \quad 1 \leq j \leq N, \ell \in \mathbb{Z}.$$

Soit ϕ une fonction à support compact, on pose

$$D(A, \phi) = \sum_{n \in \mathbb{Z}} \phi\left(\frac{N}{2\pi} \varphi_n(A)\right).$$

On a

$$\lim_{N \rightarrow \infty} \int_{SO(2N)} D(A, \phi) d\mu_{\text{Haar}} A = \int_{\mathbb{R}} W^{SO(\text{pair})}(t) \phi(t) dt.$$

¹On appelle ainsi les matrices de $U(N)$. L'étude statistique de ces matrices remonte au physicien Wigner qui cherchait à modéliser le comportement des niveaux d'énergie de grosses molécules par le spectre de matrices de $U(N)$ quand N est grand.

Autrement dit, au regard de la répartition, les petits zéros de la fonction L d'une forme paire se comportent comme les angles propres d'une matrices de $SO(2N)$. Pour $SO(2N+1)$, on a

$$\lim_{N \rightarrow \infty} \int_{SO(2N+1)} D(A, \phi) d\mu_{\text{Haar}} A = \int_{\mathbb{R}} W^{SO(\text{impair})}(t) \phi(t) dt.$$

Autrement dit, au regard de la répartition, les petits zéros de la fonction L d'une forme impaire se comportent comme les angles propres d'une matrices de $SO(2N+1)$. Pour $O(2N)$, on a

$$\lim_{N \rightarrow \infty} \int_{O(2N)} D(A, \phi) d\mu_{\text{Haar}} A = \int_{\mathbb{R}} W^O(t) \phi(t) dt.$$

Autrement dit, au regard de la répartition, les petits zéros de la fonction L d'une forme primitive se comportent comme les angles propres d'une matrices de $O(2N)$.

Pourquoi s'intéresse-t-on aux petits zéros ? On peut avoir en tête de classifier les formes modulaires à l'aide de grandeurs statistiques qui leur sont rattachées. On a vu que, pour les petits zéros, les matrices aléatoires suggéraient une classification en formes « de types $SO(2N)$ » et formes de « de types $SO(2N+1)$ ». Dans quelle mesure les zéros des séries L de formes modulaires se comportent-ils comme les valeurs propres de matrices unitaires ? On pourrait tenter de caractériser les formes primitives par d'autres grandeurs statistiques des groupes de matrices, par exemple les fonctions de corrélation ou encore les fonctions d'espacement entre zéros. Cependant, des résultats d'existence de mesures universelles nous en empêchent². Par exemple, considérons une matrice A de $SO(2N)$. Elle est équivalente à une matrice

$$\text{diag}(e^{i\varphi_1(A)}, \dots, e^{i\varphi_N(A)}, e^{-i\varphi_1(A)}, \dots, e^{-i\varphi_N(A)})$$

avec $0 \leq \varphi_1(A) \leq \dots \leq \varphi_N(A) \leq \pi$. Considérons ensuite une matrice A de $SO(2N+1)$. Elle est équivalente à une matrice

$$\text{diag}(1, e^{i\varphi_1(A)}, \dots, e^{i\varphi_N(A)}, e^{-i\varphi_1(A)}, \dots, e^{-i\varphi_N(A)})$$

avec $0 \leq \varphi_1(A) \leq \dots \leq \varphi_N(A) \leq \pi$. Soit $I \subset [0, \pi]$, on définit la fonction

$$r_1(I) = \#\{j; 1 \leq j \leq N, \varphi_j(A) \in I\}.$$

Alors,

$$\lim_{N \rightarrow \infty} \frac{1}{N} \int_{G(N)} r_1(I)(A) d\mu_{\text{Haar}} A = \frac{\text{long}(I)}{\pi}$$

pour $G(N) = SO(2N)$ ou $G(N) = SO(2N+1)$. Des travaux de Rudnick et Sarnak[RS96] prouvent que ces obstructions demeurent sur les formes primitives (et même pour une classe plus grande de fonctions L). Au contraire, l'étude des petits zéros est un moyen de distinguer les formes paires ou impaires. Le théorème 4.1.2 prouve néanmoins qu'elle ne permet pas de faire une classification plus détaillée, à moins (peut-être) d'augmenter le support de $\hat{\phi}$. La statistique de la plus petite valeur propre permet aussi de distinguer les différents groupes.

D'autre part, un intérêt des théorèmes 4.1.1 et 4.1.2 est qu'ils sont prouvés pour un support de $\hat{\phi}$ plus grand que $[-1, 1]$. On se souvient que $\int \phi W = \int \widehat{\phi W}$. Or

$$\widehat{W^O}(\xi) = \delta_0(\xi) + \frac{1}{2},$$

²Ces résultats, s'ils ont la beauté de l'universalité sont « catastrophiques » du point de vue de la classification.

$$\widehat{W}^{SO(\text{pair})}(\xi) = \delta_0(\xi) + \frac{1}{2}C(\xi)$$

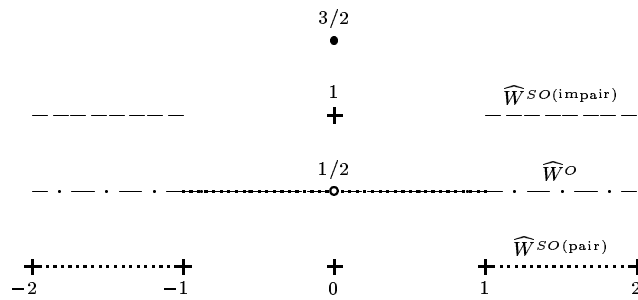
et

$$\widehat{W}^{SO(\text{impair})}(\xi) = \delta_0(\xi) - \frac{1}{2}C(\xi) + 1$$

où

$$C(\xi) = \begin{cases} 1 & \text{si } |\xi| < 1; \\ \frac{1}{2} & \text{si } |\xi| = 1; \\ 0 & \text{si } |\xi| > 1. \end{cases}$$

En particulier, rien ne permet de distinguer les différentes distributions sur $] -1, 1[$ et dans un but de classification un support de $\widehat{\phi}$ plus grand que $] -1, 1[$ est nécessaire³.



On aura besoin des sommes de Gauss sont définies, pour tout entier m et tout caractère modulo c par

$$G_\chi(m) = \sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) e\left(\frac{ma}{c}\right)$$

et si $m = 1$ on note $G_\chi(1) = G_\chi$. On a le lemme

LEMME 4.1.3

Pour tous entiers m, n, c on a

$$\sum_{\chi \pmod{c}} |G_\chi(m) G_\chi(n)| \leq \varphi(c)^2.$$

Démonstration – Grâce à l'inégalité de Cauchy-Schwarz, il est suffisant de prouver l'égalité

$$\sum_{\chi \pmod{c}} |G_\chi(q)|^2 = \varphi(c)^2$$

pour tout entier q . Or

$$\sum_{\chi \pmod{c}} |G_\chi(q)|^2 = \sum_{\substack{a \pmod{c} \\ (a,c)=1}} \sum_{\substack{b \pmod{c} \\ (b,c)=1}} e\left(\frac{q(a-b)}{c}\right) \sum_{\chi \pmod{c}} \chi(a\bar{b}).$$

On déduit de l'orthogonalité des caractères modulo c que cette somme vaut $\varphi(c)^2$.

□

³Agrandir le support est aussi un test supplémentaire de la conjecture. Et un défi.

Enfin, on utilisera la conséquence suivante de l'hypothèse de Riemann sur les séries L de Dirichlet ⁴

LEMME 4.1.4

Supposons vraie l'hypothèse de Riemann sur les séries L de Dirichlet. Soit c un entier et χ un caractère modulo c . Soit $x \geq 2$ un réel alors

$$\sum_{p \leq x} \chi(p) \frac{\ln p}{\sqrt{p}} = 2\delta_\chi \sqrt{x} + O(\ln^3(cx))$$

où δ_χ vaut 1 si $\chi = \chi_0$ est le caractère principal et 0 sinon.

4.2 Densité de répartition signée

Dans toute la suite de ce chapitre on supposera que les hypothèses de Riemann pour les fonctions L de Dirichlet et des formes primitives sont vraies. Soit k et ℓ des entiers strictement positifs fixés⁵ avec k pair. Soit $\varepsilon = (\varepsilon_1, \dots, \varepsilon_\ell)$ un vecteur de $\{-1, 1\}^\ell$. Soit ϕ une fonction paire de $S(\mathbb{R})$ de transformée de Fourier à support compact dans $] -2, 2[$. Soit $0 < \kappa \leq 1/\ell$ un réel. On considère une suite d'entiers N sans facteur carré de facteurs premiers $p_1 < \dots < p_\ell$ tel que $p_1 \geq N^\kappa$. On définit les fonctions

$$\begin{aligned} D(\phi) &: B(2, N) \rightarrow \mathbb{C} \\ f &\mapsto D(f, \phi) \end{aligned}$$

et pour tout entier $n \geq 1$

$$\begin{aligned} \lambda(n) &: B(2, N) \rightarrow \mathbb{R} \\ f &\mapsto \lambda_f(n). \end{aligned}$$

On va estimer $M^\varepsilon(D(\phi))$. Grâce à la formule de Riemann (proposition 2.2.2), on écrit cette moyenne signée sous la forme $M^\varepsilon(D(\phi)) = M_1 + M_2 + M_3 + O_k\left(\frac{\ln \ln(3N)}{\ln(N)}\right)$ où

$$\begin{aligned} M_1 &= M^\varepsilon(1) \left(\hat{\phi}(0) + \frac{1}{2} \phi(0) \right) \\ M_2 &= - \sum_{(p, N)=1} \hat{\phi}\left(\frac{2 \ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{p \ln(k^2 N)} M^\varepsilon(\lambda(p^2)) \\ M_3 &= - \sum_{(p, N)=1} \hat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} M^\varepsilon(\lambda(p)) \end{aligned}$$

Le lemme suivant permet d'estimer M_2 .

LEMME 4.2.1

Soit ℓ et k deux entiers strictement positifs, k pair. Soit N un entier sans facteur carré ayant ℓ facteurs premiers $p_1 < \dots < p_\ell$, ε un vecteur de $\{-1, 1\}^\ell$ et k un entier strictement positif. Alors, pour toute fonction ϕ de $S(\mathbb{R})$ à support compact $[-2 + \delta_0, 2 - \delta_0]$ tel que $0 < \delta_0 < 2$,

$$\sum_{(p, N)=1} \hat{\phi}\left(\frac{2 \ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{p \ln(k^2 N)} M^\varepsilon(\lambda(p^2)) \ll N^{-\frac{1}{4} - \frac{\delta_0}{5}}$$

où la constante impliquée ne dépend que de δ_0 , ℓ et k .

⁴La preuve est semblable à celle de la proposition 2.2.1.

⁵En conséquence, toutes les constantes de majoration pourront dépendre de k et ℓ même si cela n'est pas précisé.

Démonstration – Par utilisation du théorème des nombres premiers et intégration par partie on a, dès que $a > 1$ et $x \geq 2$

$$\sum_{p \leq x} \frac{\ln p \ln(ap^2)}{\sqrt{p}} \ll \ln(ax) \sqrt{x} \quad (4.1)$$

où la constante est absolue. En remarquant que $\widehat{\phi}\left(\frac{2 \ln p}{\ln(k^2 N)}\right) = 0$ pour tout premier $p > (k^2 N)^{1-\delta_0/2}$ et en utilisant (4.1) on obtient le résultat énoncé par utilisation de la proposition 1.7.9. $\square$

La proposition suivante permet d'estimer le terme M_3 .

PROPOSITION 4.2.2

L'hypothèse de Riemann sur les fonctions L de formes primitives est supposée vraie. Soit k et ℓ des entiers strictement positifs fixés. Soit κ un réel vérifiant $0 < \kappa \leq 1/\ell$. Soit $\varepsilon = (\varepsilon_1, \dots, \varepsilon_\ell)$ un vecteur de $\{-1, 1\}^\ell$. Soit ϕ une fonction paire de $\mathcal{S}(\mathbb{R})$ de transformée de Fourier à support compact dans $]-2, 2[$. On considère un entier N sans facteur carré ayant ℓ facteurs premiers $p_1, \dots, p_\ell$ tels que $N^\kappa \leq p_1 < \dots < p_\ell$. Alors

$$\begin{aligned} \sum_{(p, N)=1} \widehat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} M^\varepsilon(\lambda(p)) &= \frac{1}{2^\ell} \frac{\varphi(N)}{N} i^{k \varepsilon_1 \dots \varepsilon_\ell} \\ &\times \left(\frac{\phi(0)}{2} - \int_{-\infty}^{+\infty} \phi(x) \frac{\sin(2\pi x)}{2\pi x} dx \right) + O_{k, \kappa, \ell} \left(\frac{\ln \ln(3N)}{\ln N} \right). \end{aligned}$$

Démonstration – Grâce à (1.32) on écrit

$$2^\ell M_3 = M_3(\emptyset) + \sum_{i=1}^{\ell} (-1)^i \sum_{1 \leq j_1 < \dots < j_i \leq \ell} \varepsilon_{j_1} \dots \varepsilon_{j_i} M_3(j).$$

Pour $0 \leq i \leq \ell$ et toute suite j de i éléments tels que $1 \leq j_1 < \dots < j_i \leq \ell$ on a posé

$$M_3(j) = -\sqrt{N_j} \sum_{(p, N)=1} \widehat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} M^h(\lambda(N_j) \lambda(p))$$

avec $N_j = p_{j_1} \dots p_{j_i}$. Pour $j = \emptyset$ (c'est à dire $i = 0$) il faut prendre $N_\emptyset = 1$ dans ces formules. Le théorème 1.7.2 permet d'écrire

$$M_3(j) := M_3^p(j) + M_3^e(j) \quad (4.2)$$

avec

$$M_3^p(j) = -\sqrt{N_j} \sum_{(p, N)=1} \widehat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} \Delta_N(p, N_j)$$

et

$$\begin{aligned} M_3^e(j) &= -\frac{\sqrt{N_j}}{N} \sum_{\substack{L M = N \\ L \neq 1}} \frac{\mu(L) M}{\nu((N_j, L))} \sum_{l|L^\infty} \frac{1}{l} \\ &\times \sum_{(p, N)=1} \widehat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} \Delta_M(pl^2, N_j). \end{aligned}$$

On montre que $M_3^e(j)$ est négligeable dans le

LEMME 4.2.3

Les hypothèses de Riemann sur les fonctions L de Dirichlet et des formes primitives sont supposées vraies. Soit N un entier sans facteur carré de plus petit diviseur premier p_1 , i un entier, $0 \leq i \leq \ell$ et j une suite $1 \leq j_1 < \dots < j_i \leq \ell$. Pour tout réel ε tel que $0 < \varepsilon < \frac{\delta_0}{2}$

$$M_3^e(j) = O_{k,\varepsilon} \left(\frac{N^\varepsilon}{p_1} \right).$$

Démonstration – Grâce au lemme 1.7.3 et puisque $(l, M) = (l, p) = 1$ on a

$$\Delta_M(pl^2, N_j) = \sum_{L_1 M_1 = M} \sum_{f \in B(M_1)} \frac{\omega_{M_1}(f)}{\nu(L_1) \rho_f(L_1)} \frac{\lambda_f(l^2) \lambda_f(p) \lambda_f(N_j)}{\nu((l^2 N_j p, L_1))}.$$

Le report de cette expression dans la définition de $M_3^e(j)$ donne

$$\begin{aligned} |M_3^e(j)| &\leq \frac{\sqrt{N_j}}{N} \sum_{\substack{LL_1 M_1 = N \\ L \neq 1}} \frac{L_1 M_1}{\nu((N_j, L))} \sum_{f \in B(M_1)} \frac{\omega_{M_1}(f)}{\nu(L_1) \rho_f(L_1)} |\lambda_f(N_j)| \\ &\quad \times \sum_{l|L^\infty} \frac{|\lambda_f(l^2)|}{l} \left| \sum_{(p,N)=1} \hat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} \frac{\lambda_f(p)}{\nu((l^2 N_j p, L_1))} \right| \end{aligned}$$

La majoration de Deligne (proposition 1.2.5) donne

$$\sum_{l|L^\infty} \frac{|\lambda_f(l^2)|}{l} \leq \sum_{l|L^\infty} \frac{\tau(l^2)}{l} \leq \prod_{p|L} \frac{p(p+1)}{(p-1)^2} \leq 6^{\omega(L)}.$$

Puisque $(p, N) = 1$ et $(L, L_1) = 1$ alors $\nu((l^2 N_j p, L_1)) = \nu((N_j, L_1))$ puis

$$\nu((N_j, L_1)) \nu((N_j, L)) = \nu((N_j, LL_1)).$$

Enfin la majoration (2.20) donne

$$\frac{\omega_{M_1}(f)}{\nu(L_1) \rho_f(L_1)} \ll \frac{\ln(k M_1)}{L_1 M_1}.$$

On a alors

$$\begin{aligned} M_3^e(j) &\ll_k \frac{6^{\omega(N)}}{N} \sum_{\substack{LL_1 M_1 = N \\ L \neq 1}} \frac{\sqrt{N_j}}{\nu((N_j, LL_1))} \\ &\quad \times \sum_{f \in B(M_1)} |\lambda_f(N_j)| \left| \sum_{(p,N)=1} \hat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) \frac{\lambda_f(p) \ln p}{\sqrt{p}} \right|. \end{aligned}$$

Grâce à la proposition 2.2.1, on a

$$\begin{aligned} \sum_{(p,N)=1} \hat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) \frac{\lambda_f(p) \ln p}{\sqrt{p}} &= - \frac{1}{\ln(k^2 N)} \int_{R^{-1}}^R \sum_{\substack{p \leq t \\ (p,N)=1}} \frac{\lambda_f(p) \ln p}{\sqrt{p}} \hat{\phi}'(t) \frac{dt}{t} \\ &\ll_k \ln^3 N \end{aligned}$$

R valant $(k^2 N)^{2-\delta_0}$ et donc

$$M_3^e(j) \ll_k \frac{6^{\omega(N)} \ln^3 N}{N} \sum_{\substack{LL_1 M_1 = N \\ L \neq 1}} \frac{\sqrt{N_j}}{\nu((N_j, LL_1))} \sum_{f \in B(M_1)} |\lambda_f(N_j)|.$$

On écrit $N_j = AB$ avec $A|M_1$ et $(B, M_1) = 1$. Alors, grâce au 4) de la proposition 1.4.1, $\lambda_f(N_j) \ll \frac{\tau(B)}{\sqrt{A}}$ et $(N_j, LL_1) = (B, LL_1) = B$ donc

$$M_3^e(j) \ll_k 6^{\omega(N)} \ln^3 N \sum_{\substack{LL_1|N \\ L \neq 1}} \frac{1}{LL_1} \ll_k \frac{6^{\omega(N)} \tau(N) \ln^3 N}{p_1}$$

ce qui termine la preuve. $\square$

REMARQUE 4.1 C'est ici le *seul* endroit où l'on utilise l'hypothèse de Riemann pour les fonctions L de formes primitives. Elle est utilisée afin d'estimer « trivialement » la contribution des formes anciennes. En particulier, elle est inutile en poids $k \leq 10$, $k = 14$ ou en niveau premier.

On estime maintenant le premier membre de $M_3(j)$, (voir (4.2)). On a

$$M_3^p(j) = -\sqrt{N_j} \sum_{(p, N_j)=1} \hat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} \Delta_N(p, N_j).$$

On écrit, puisque $(p, N_j) = 1$ et grâce au lemme A.3 et à la définition (1.29)

$$M_3^p(j) = -\frac{\sqrt{N_j}}{N} \sum_{r=1}^{\infty} \frac{1}{r} \times \\ 2\pi i^k \sum_{(p, N)=1} S(pN_j, 1; rN) J_{k-1}\left(\frac{4\pi\sqrt{pN_j}}{rN}\right) \hat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)}. \quad (4.3)$$

On appelle L_j le complémentaire de N_j dans N , $N = N_j L_j$. On a $(N_j, L_j) = 1$. De même, dans le but de simplifier les sommes de Kloosterman on décompose r en partie ayant mêmes diviseurs que N_j et partie première à N_j ,

$$r = vw, \quad v|N_j^\infty, \quad (w, N_j) = 1.$$

On peut alors utiliser le lemme A.5 pour écrire

$$S(pN_j, 1; vN_j w L_j) = S(pN_j \overline{wL_j}^2, 1; vN_j) S(p\overline{v}^2 \overline{N_j}, 1; wL_j).$$

Si $(v, N_j) > 1$ alors $(pN_j \overline{wL_j}^2, v, N_j) > 1$ et, d'après le lemme A.10

$$S(pN_j \overline{wL_j}^2, 1; vN_j) = 0,$$

on peut donc supposer $(v, N_j) = 1$. Comme $v|N_j^\infty$, on peut supposer $v = 1$. On peut alors récrire (4.3)

$$M_3^p(j) = -\frac{\sqrt{N_j}}{N} \sum_{(w, N_j)=1} \frac{1}{w} \times \\ 2\pi i^k \sum_{(p, N)=1} S(pN_j, 1; wN_j L_j) J_{k-1}\left(\frac{4\pi\sqrt{pN_j}}{wN}\right) \hat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)}. \quad (4.4)$$

Le lemme A.11 donne

$$M_3^p(j) = -\frac{\sqrt{N_j}}{N} \mu(N_j) \sum_{(w, N_j)=1} \frac{1}{w} \times \\ 2\pi i^k \sum_{(p, N)=1} S(p\overline{N_j}, 1; wL_j) J_{k-1}\left(\frac{4\pi\sqrt{pN_j}}{wN}\right) \hat{\phi}\left(\frac{\ln p}{\ln(k^2 N)}\right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)}.$$

Par les majorations du lemme A.13 et (B.1) on a la majoration

$$\frac{\sqrt{N_j}}{N} \sum_{\substack{w \geq 12k\pi N_j^2 L_j \\ (w, N_j)=1}} \frac{1}{w} 2\pi i^k \sum_{(p, N)=1} S(p\overline{N_j}, 1; wL_j) \times \\ J_{k-1} \left(\frac{4\pi\sqrt{pN_j}}{wN} \right) \widehat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} \ll_k N^{-\frac{\delta_0}{2}}.$$

REMARQUE 4.2 Si $k \geq 4$, cette troncature des grandes valeurs de w n'est pas nécessaire. En (4.6) on peut en effet utiliser (B.1) au lieu de (B.2).

On transforme alors (4.4) en

$$M_3^p(j) = -\frac{\sqrt{N_j}}{N} \mu(N_j) \sum_{\substack{w \leq 12k\pi N_j^2 L_j \\ (w, N_j)=1}} \frac{1}{w} 2\pi i^k \sum_{(p, N)=1} S(p\overline{N_j}, 1; wL_j) \times \\ J_{k-1} \left(\frac{4\pi\sqrt{pN_j}}{wN} \right) \widehat{\phi} \left(\frac{\ln p}{\ln(k^2 N)} \right) \frac{2 \ln p}{\sqrt{p} \ln(k^2 N)} + O(N^{-\delta_0/2}).$$

Par intégration de Stieljes par parties et utilisation du lemme A.17 on écrit

$$M_3^p(j) = \frac{\sqrt{N_j}}{N} \mu(N_j) \sum_{\substack{w \leq 12k\pi N_j^2 L_j \\ (w, N_j)=1}} \frac{1}{w} \times \\ \frac{4\pi i^k}{\ln(k^2 N)} \int_0^\infty \left(2\mu(wL_j) \frac{\mu(wL_j)}{\varphi(wL_j)} \sqrt{x} + O(\varphi(wL_j) \ln^3 wN) \right) \\ d \left(J_{k-1} \left(\frac{4\pi\sqrt{xN_j}}{wN} \right) \widehat{\phi} \left(\frac{\ln x}{\ln(k^2 N)} \right) \right) + O(N^{-\delta_0/2}).$$

Il résulte de la condition sur le support de $\widehat{\phi}$ qu'on peut restreindre les variations de la variable d'intégration à $N^{-2+\delta_0} \ll_k x \ll_k N^{2-\delta_0}$. On a utilisé ce fait pour simplifier le terme d'erreur. On définit

$$Q^e = \frac{4\pi i^k}{\ln(k^2 N)} \int_0^\infty O(\varphi(wL_j) \ln^3(wN)) d \left(J_{k-1} \left(\frac{4\pi\sqrt{xN_j}}{wN} \right) \widehat{\phi} \left(\frac{\ln x}{\ln(k^2 N)} \right) \right).$$

Par calcul de l'élément différentiel, on obtient

$$Q^e = \frac{4\pi i^k}{\ln(k^2 N)} O(\varphi(wL_j) \ln^3(wN)) \\ \int_0^\infty \left(\frac{2\pi\sqrt{N_j}}{wN\sqrt{x}} J'_{k-1} \left(\frac{4\pi\sqrt{xN_j}}{wN} \right) \widehat{\phi} \left(\frac{\ln x}{\ln(k^2 N)} \right) \right. \\ \left. + \frac{1}{x \ln(k^2 N)} J_{k-1} \left(\frac{4\pi\sqrt{xN_j}}{wN} \right) \widehat{\phi}' \left(\frac{\ln x}{\ln(k^2 N)} \right) \right) dx.$$

Le support de $\widehat{\phi}$ étant $[-2 + \delta_0, 2 - \delta_0]$ on a la majoration

$$Q^e \ll \varphi(wL_j) \ln^3(wN) \\ \int_{R^{-1}}^R \left\{ \left| J'_{k-1} \left(\frac{4\pi\sqrt{xN_j}}{wN} \right) \right| + \frac{wN}{2\pi\sqrt{N_j}x} \left| J_{k-1} \left(\frac{4\pi\sqrt{xN_j}}{wN} \right) \right| \right\} \frac{2\pi\sqrt{N_j}}{wN\sqrt{x}} dx$$

où $R = (k^2 N)^{2-\delta_0}$. On effectue alors le changement de variable $y = \frac{4\pi\sqrt{xN_j}}{wN}$ pour obtenir

$$Q^e \ll \varphi(wL_j) \ln^3(wN) \int_z^Z |J'_{k-1}(y)| + \frac{1}{y} |J_{k-1}(y)| dy$$

où

$$Z = \frac{4\pi k^{2-\delta_0}}{w} \sqrt{N_j} N^{-\delta_0/2} \quad (4.5a)$$

et

$$z = \frac{4\pi k^{-2+\delta_0}}{wN^{2-\delta_0/2}} \sqrt{N_j}. \quad (4.5b)$$

Grâce à (B.3) et (B.4) on exprime l'intégrale en combinaison de fonctions J de Bessel

$$Q^e \ll \varphi(wL_j) \ln^3(wN) \int_z^Z |J_{k-2}(y)| + |J_{k-1}(y)| + |J_k(y)| dy. \quad (4.6)$$

Grâce à (B.2) on obtient alors

$$Q^e \ll_k \varphi(wL_j) \ln^3(wN) \sqrt{N_j} w^{-1} N^{-\delta_0/2} \ll L_j \sqrt{N_j} N^{-\delta_0/3}$$

puis

$$\frac{\sqrt{N_j}}{N} \sum_{\substack{w \leq 12k\pi N_j^2 L_j \\ (w, N_j)=1}} \frac{1}{w} Q^e \ll_k N^{-\delta_0/4}.$$

On a alors

$$M_3^p(j) = \frac{\sqrt{N_j}}{N} \mu(N_j) \sum_{\substack{w \leq 12k\pi N_j^2 L_j \\ (w, N_j)=1}} \frac{1}{w} Q^p + O(N^{-\delta_0/4})$$

avec

$$Q^p = \frac{4\pi i^k}{\ln(k^2 N)} \int_0^\infty 2\mu(wL_j) \frac{\mu(wL_j)}{\varphi(wL_j)} \sqrt{x} d\left(J_{k-1}\left(\frac{4\pi\sqrt{xN_j}}{wN}\right) \widehat{\phi}\left(\frac{\ln x}{\ln(k^2 N)}\right)\right).$$

On effectue une nouvelle intégration par parties sur l'intégrale de Q^p et le changement de variable $y = \frac{4\pi\sqrt{xN_j}}{wN}$ pour obtenir

$$Q^p = -2i^k w \frac{N}{\sqrt{N_j}} \frac{\mu(wL_j)^2}{\varphi(wL_j)} \int_0^\infty \widehat{\phi}\left(\frac{2\ln(\frac{wN}{4\pi\sqrt{N_j}}y)}{\ln(k^2 N)}\right) J_{k-1}(y) \frac{dy}{\ln(k^2 N)}.$$

Grâce à (B.2), on a

$$Q^p \ll_k w \frac{N}{\sqrt{N_j}} \frac{1}{\varphi(wL_j)} \int_z^Z |J_{k-1}(y)| dy \ll_k \frac{N\tau(L_j)}{L_j} \frac{\tau(w)}{w} N^{-\delta_0/2}$$

avec Z et z comme en (4.5). Ainsi,

$$\frac{\sqrt{N_j}}{N} \sum_{w \geq 12k\pi N_j^2 L_j} \frac{1}{w} Q^p \ll_k \frac{1}{NL_j \sqrt{N_j}}$$

et on peut réintégrer les grandes valeurs de w

$$M_3^p(j) = \frac{\sqrt{N_j}}{N} \mu(N_j) \sum_{(w, N_j)=1} \frac{1}{w} Q^p + O(N^{-\delta_0/3}).$$

On transforme ensuite l'intégrale intervenant dans l'expression de Q^p . Pour cela, on remplace $\widehat{\phi}$ par son expression en ϕ pour obtenir

$$\begin{aligned} \int_0^\infty J_{k-1}(y) \widehat{\phi}\left(\frac{2 \ln \frac{wNy}{4\pi\sqrt{N_j}}}{\ln(k^2 N)}\right) \frac{dy}{\ln(k^2 N)} \\ = \int_{t=-\infty}^\infty \phi(t) \left(\frac{wN}{4\pi\sqrt{N_j}}\right)^{-\frac{4i\pi t}{\ln(k^2 N)}} \int_{y=0}^\infty J_{k-1}(y) y^{-\frac{4i\pi t}{\ln(k^2 N)}} dy \frac{dt}{\ln(k^2 N)}. \end{aligned}$$

Enfin, grâce à (B.5) on obtient après avoir posé $x = \frac{t}{\ln(k^2 N)}$

$$\begin{aligned} \int_0^\infty J_{k-1}(y) \widehat{\phi}\left(\frac{2 \ln \frac{wNy}{4\pi\sqrt{N_j}}}{\ln(k^2 N)}\right) \frac{dy}{\ln(k^2 N)} \\ = \int_{-\infty}^\infty \phi(x \ln(k^2 N)) \left(\frac{2\pi\sqrt{N_j}}{wN}\right)^{4i\pi x} \frac{\Gamma(\frac{k}{2} - 2i\pi x)}{\Gamma(\frac{k}{2} + 2i\pi x)} dx. \end{aligned}$$

Si w et L_j ne sont pas premiers entre eux, alors $\mu(wL_j)^2 = 0$ donc on peut supposer $(w, L_j) = 1$ qui conduit à $(w, N) = 1$, $\mu(wL_j)^2 = \mu(w)^2$ et $\varphi(wL_j) = \varphi(L_j)\varphi(w)$. Ainsi, on obtient

$$\begin{aligned} M_3^p(j) = -2i^k \frac{\mu(N_j)}{\varphi(L_j)} \sum_{(w,N)=1} \frac{\mu(w)^2}{\varphi(w)} \\ \int_{-\infty}^\infty \phi(x \ln(k^2 N)) \left(\frac{2\pi}{wL_j\sqrt{N_j}}\right)^{4i\pi x} \frac{\Gamma(\frac{k}{2} - 2i\pi x)}{\Gamma(\frac{k}{2} + 2i\pi x)} dx + O(N^{-\delta_0/4}). \end{aligned}$$

On pose

$$\gamma(s) = \sum_{(r,N)=1} \frac{\mu(r)^2}{\varphi(r)} r^{-s}.$$

Cette série converge pour $\Re s > 0$. On a alors

$$\begin{aligned} M_3^p(j) = -2i^k \frac{\mu(N_j)}{\varphi(L_j)} \lim_{\varepsilon \rightarrow 0} \\ \int_{-\infty}^\infty \phi(x \ln(k^2 N)) \left(\frac{2\pi}{L_j\sqrt{N_j}}\right)^{4i\pi x} \frac{\Gamma(\frac{k}{2} - 2i\pi x)}{\Gamma(\frac{k}{2} + 2i\pi x)} \gamma(4i\pi x + \varepsilon) dx + O(N^{-\delta_0/4}). \quad (4.7) \end{aligned}$$

Or

$$\gamma(s) = \prod_{(p,N)=1} \left(1 + \frac{p^{-s}}{p-1}\right) = \beta(s)\zeta(s+1)\alpha(s)$$

avec

$$\beta(s) = \prod_{p|N} \left(1 + \frac{p^{-s}}{p-1}\right)^{-1}$$

et

$$\alpha(s) = \prod_p \left(1 + \frac{p^{-s} - p^{-2s}}{p(p-1)}\right).$$

Or,

$$\frac{\alpha'(0)}{\alpha(0)} = \sum_p \frac{\ln p}{p(p-1)} = O(1)$$

donc

$$\alpha(s) = 1 + O(s)$$

uniformément pour $|s| \leq \frac{1}{2} - \varepsilon$. De même

$$\frac{\beta'(0)}{\beta(0)} = \sum_{p|N} \frac{\ln p}{p} = O(\ln \ln(3N))$$

et $\beta(0) = \frac{\varphi(N)}{N}$ donc

$$\beta(s) = \frac{\varphi(N)}{N} (1 + O(s \ln \ln(3N)))$$

uniformément pour $|s| \leq 1$. On a alors

$$\gamma(s) = \frac{\varphi(N)}{sN} + O\left(\frac{\varphi(N) \ln \ln(3N)}{N}\right) \quad (4.8)$$

uniformément pour $|s| \leq \frac{1}{2} - \varepsilon$. D'autre part, d'après (B.6)

$$\frac{\Gamma(\frac{k}{2} - 2i\pi x)}{\Gamma(\frac{k}{2} + 2i\pi x)} = \left(\frac{k}{2}\right)^{-4i\pi x} (1 + O_k(x))$$

uniformément pour $|x| \leq \frac{1}{2\pi} - \varepsilon = A$. Après changement de x en $-x$ et par parité de ϕ on obtient enfin

$$\begin{aligned} M_3^p(j) &= -2i^k \frac{\varphi(N)}{N} \frac{\mu(N_j)}{\varphi(L_j)} \lim_{\varepsilon \rightarrow 0} \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \\ &\quad \times \left(\frac{4\pi}{kL_j \sqrt{N_j}}\right)^{-4i\pi x} \frac{dx}{\varepsilon - 4i\pi x} + O_k\left(\frac{\ln \ln(3N)}{\varphi(L_j) \ln(k^2 N)}\right). \end{aligned} \quad (4.9)$$

REMARQUE 4.3 En toute rigueur, pour appliquer (4.8) il faut couper l'intégrale de (4.7) en

$$\int_{|x| \leq (4\pi)^{-1}A} + \int_{|x| > (4\pi)^{-1}A}.$$

Mais, la seconde intégrale est inférieure à une puissance de $\ln(k^2 N)$ aussi négative que voulue puisque $\phi \in \mathcal{S}(\mathbb{R})$. On peut donc sans souci⁶ la soustraire de (4.7) pour la rajouter à (4.9). Puisque ϕ détecte les petits zéros, cela n'a rien de surprenant.

On pose

$$\Omega = \left(\frac{kN}{4\pi \sqrt{N_j}}\right)^2 = \left(\frac{k\sqrt{N_j}L_j}{4\pi}\right)^2.$$

Alors

$$\begin{aligned} \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \left(\frac{4\pi}{kL_j \sqrt{N_j}}\right)^{-4i\pi x} \frac{dx}{\varepsilon - 4i\pi x} &= \\ \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \cos(2\pi \ln \Omega) \frac{dx}{\varepsilon - 4i\pi x} &+ \\ + i \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \sin(2\pi x \ln \Omega) \frac{dx}{\varepsilon - 4i\pi x}. \end{aligned}$$

⁶En utilisant la majoration $\zeta(1+it) \ll_A \ln |t|$ pour $|t| \geq A$.

Le changement de x en $-x$ dans la première intégrale montre qu'elle est réelle (ϕ est paire) et égale à sa partie réelle. Ainsi, en posant $y = x/\varepsilon$ on a

$$\begin{aligned} \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \left(\frac{4\pi}{k L_j \sqrt{N_j}} \right)^{-4i\pi x} \frac{dx}{\varepsilon - 4i\pi x} = \\ \int_{-\infty}^{\infty} \phi(y\varepsilon \ln(k^2 N)) \cos(2\pi y\varepsilon \ln \Omega) \frac{dy}{1 + (4\pi y)^2} \\ - i \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \sin(2\pi x \ln \Omega) \frac{dx}{-\varepsilon + 4i\pi x} \end{aligned}$$

et

$$\begin{aligned} \lim_{\varepsilon \rightarrow 0} \int_{-\infty}^{\infty} \phi(x \ln(k^2 N)) \left(\frac{4\pi}{k L_j \sqrt{N_j}} \right)^{-4i\pi x} \frac{dx}{\varepsilon - 4i\pi x} = \\ \frac{\phi(0)}{4} - \frac{1}{2} \int_{-\infty}^{\infty} \phi(x) \sin\left(2\pi x \frac{\ln \Omega}{\ln(k^2 N)}\right) \frac{dx}{2\pi x}. \end{aligned}$$

Si $N \neq N_j$,

$$\left| \frac{1}{2} \int_{-\infty}^{\infty} \phi(x) \sin\left(2\pi x \frac{\ln \Omega}{\ln(k^2 N)}\right) \frac{dx}{2\pi x} \right| \leq \int_{-\infty}^{\infty} |\phi(x)| dx.$$

On déduit alors de (4.9) que si $j \neq (1, \dots, \ell)$ alors $L_j \geq p_1$ et

$$M_3^p(j) \ll \frac{1}{p_1} + \frac{\ln \ln(3N)}{\ln(k^2 N)}, \quad j \neq (1, \dots, \ell).$$

On conclut si $N = N_j$ en utilisant

$$\int_{-\infty}^{\infty} \phi(x) \sin\left(2\pi x \frac{\ln \Omega}{\ln(k^2 N)}\right) \frac{dx}{2\pi x} = \int_{-\infty}^{\infty} \phi(x) \sin(2\pi x) \frac{dx}{2\pi x} + O\left(\frac{1}{\ln(k^2 N)}\right)$$

qui se voit en calculant la différence des deux intégrales. $\square$

On déduit le théorème 4.1.2 du lemme 1.7.10 et de la proposition 4.2.2.

Chapitre 5

Statistique de $L(sym^2, 1)$

Ce cinquième chapitre étudie la statistique de $L(sym^2 f, 1)$. Les résultats sont à paraître à *Mathematische Annalen* [Roy01c].

5.1 Résultats

Soit κ un réel, $0 < \kappa \leq 1$ et $\mathcal{N}$ l'ensemble des entiers sans facteur carré N de plus petit facteur premier $p_1(N) \geq N^\kappa$. On étudie dans cet article la variable aléatoire qui associe à une forme f de l'ensemble $B(N)$ des formes primitives de niveau N la valeur en 1 de la fonction L associée au carré symétrique de f , soit

$$\begin{array}{ccc} L(sym^2, 1) & : & B(N) \rightarrow \mathbb{R} \\ & & f \mapsto L(sym^2 f, 1) \end{array}$$

lorsque N parcourt $\mathcal{N}$. On montre que ces variables aléatoires admettent une variable aléatoire limite $L(sym^2, 1)_\infty$ dont on calcule les moments dans le

THÉORÈME 5.1.1

Soit $n \geq 1$ un entier. Soit

$$M_n(N) = \frac{1}{\#B(N)} \sum_{f \in B(N)} L(sym^2 f, 1)^{n-1}.$$

Alors, lorsque N parcourt $\mathcal{N}$ il existe un réel M_n tel que

$$\lim_{N \rightarrow \infty} M_n(N) = M_n.$$

On définit pour tout $\mathbf{b} \in \mathbb{N}^n$ l'ensemble

$$\mathcal{E}_n(\mathbf{b}) = \left\{ \mathbf{d} \in \mathbb{N}^{n-1}; d_i \left| \left(\frac{b_1 \cdots b_i}{d_1 \cdots d_{i-1}}, b_{i+1} \right)^2, 1 \leq i \leq n-1 \right\}$$

puis pour tout $r \geq 1$ entier

$$m_n(r) = \sum_{\substack{\mathbf{b} \in \mathbb{N}^n \\ \det \mathbf{b} = r}} \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{b}) \\ \det \mathbf{d} = \det \mathbf{b}}} 1.$$

On a alors

$$M_n = \zeta(2)^{n-1} \sum_{r=1}^{+\infty} \frac{m_n(r)}{r}.$$

La variable aléatoire $L(sym^2, 1)$ admet lorsque N parcourt $\mathcal{N}$ une variable aléatoire limite $L(sym^2, 1)_\infty$ dont le moment d'ordre $n - 1$ est M_n . En particulier, l'espérance de $L(sym^2, 1)_\infty$ est

$$E[L(sym^2, 1)_\infty] = \zeta(2)^2$$

et sa variance

$$\text{Var}[L(sym^2, 1)_\infty] = \zeta(2)^4 \left[\frac{\zeta(2)\zeta(3)}{\zeta(6)} - 1 \right] \approx 6,908.$$

On a fait les conventions $\mathbb{N}^0 = \{1\}$, $\mathcal{E}_1(\mathbf{b}) = \{1\}$ et $d_1 \cdots d_0 = 1$.

La preuve utilise crucialement le fait, prouvé par Gelbart et Jacquet, que la fonction $L(sym^2 f, s)$ est la fonction L d'une forme automorphe de GL_3 et la théorie de la convolution de Rankin-Selberg pour ce groupe. Par des techniques dérivées du grand crible et utilisées par Luo et Kowalski-Michel on exprime $L(sym^2 f, 1)$ comme un polynôme de Dirichlet court en moyenne. Ce résultat est analogue et a été inspiré par les travaux de Luo [Luo99] dans le cas des formes de Maaß pour $SL(2, \mathbb{Z})$. En particulier, les moments sont les mêmes. On obtient un encadrement plus précis des moments que celui obtenu par Luo dans le

THÉORÈME 5.1.2

Pour tout entier $n \geq 2$ on a

$$\ln M_n = 3n \ln \ln n + O(n).$$

En fait, ces techniques permettent également le calcul (inspiré par un travail ultérieur de Luo [Luo00]) des moments négatifs.

THÉORÈME 5.1.3

Soit $n \geq 1$ un entier. On définit pour tout $r \geq 1$ entier

$$m_{-n}(r) = \sum_{\substack{\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n \\ \det \mathbf{a} \mathbf{b}^2 \mathbf{c}^3 = r}} \mu(a_1 b_1 c_1) \cdots \mu(a_n b_n c_n) \mu(b_1) \cdots \mu(b_n) \times \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{a} \mathbf{b}) \\ \det \mathbf{a} \mathbf{b} = \det \mathbf{d}}} 1.$$

Le moment négatif d'ordre $-n - 1$ de $L(sym^2, 1)_\infty$ est donné par

$$M_{-n} = \frac{1}{\zeta(2)} \sum_{r=1}^{+\infty} \frac{m_{-n}(r)}{r}.$$

REMARQUE 5.1 Avec la convention $\mathcal{E}_0(1) = \{1\}$, ce théorème reste valable pour $n = 0$. Voir la remarque 5.3.

Enfin, soit q un nombre premier, on considère $L^{(q)}(sym^2, 1)$, la variable aléatoire obtenue de $L(sym^2, 1)$ par division par le q -ième facteur eulerien (voir (2.3.1)) et on prouve le résultat d'indépendance

PROPOSITION 5.1.4

Soit q un nombre premier. Les variables aléatoires limites, lorsque N parcourt $\mathcal{N}$ en restant premier à q , des variables aléatoires

$$\begin{array}{ccc} \lambda(q) & : & B(N) \rightarrow \mathbb{R} \\ & & f \mapsto \lambda_f(q) \end{array}$$

et $L^{(q)}(sym^2, 1)$ sont indépendantes.

On rappelle que deux variables aléatoires sont indépendantes lorsque la fonction de distribution cumulative du couple qu'elles forment est le produit des fonctions de distribution cumulative de chacune d'elles.

5.2 Préliminaires probabilistes

Les notions de probabilités nécessaires à ce préliminaire sont, par exemple, données dans [Bil95]. Soit N un entier sans facteur carré. On considère la mesure définie pour toute partie A de $B(N)$ par

$$P_N(A) = \frac{\sharp A}{\sharp B(N)}.$$

On étudie la variable aléatoire

$$\begin{array}{ccc} L(sym^2, 1) & : & B(N) \rightarrow \mathbb{R} \\ & & f \mapsto L(sym^2 f, 1). \end{array}$$

La fonction de répartition cumulative associée à cette variable aléatoire est définie pour tout réel x par

$$R_N(x) = \frac{1}{\sharp B(N)} \sharp \{f \in B(N); L(sym^2 f, 1) \leq x\}.$$

Les moments de la variable $L(sym^2, 1)$ sont donnés pour tout entier n par

$$M_n(N) = \frac{1}{\sharp B(N)} \sum_{f \in B(N)} L(sym^2 f, 1)^{n-1}.$$

On a, pour tout réel $\alpha \geq 0$ et tout entier positif n l'inégalité de Markov

$$\frac{1}{\sharp B(N)} \sharp \{f \in B(N); L(sym^2 f, 1) \geq \alpha\} \leq \frac{M_{n+1}(N)}{\alpha^n}. \quad (5.1)$$

Notre but est de montrer qu'il existe une fonction de répartition cumulative R qui soit limite faible des fonctions R_N lorsque N parcourt l'ensemble $\mathcal{N}$. On dit que R_N converge faiblement vers R lorsqu'on a

$$\lim_{N \rightarrow \infty} R_N(x) = R(x)$$

en tout point de continuité x de R . On rappelle que toute fonction croissante, continue à droite de limite nulle en $-\infty$ et 1 en $+\infty$ est la fonction de répartition cumulative d'une variable aléatoire. On notera $L(sym^2, 1)_\infty$ la variable aléatoire de fonction de répartition cumulative R et de mesure de probabilité μ . Les moments de cette variable sont les réels

$$M_n = \int_{\mathbb{R}} x^{n-1} d\mu.$$

Pour prouver l'existence de R on utilisera le critère donné par le

LEMME 5.2.1

Soit $(R_N)_N$ une suite de fonctions de répartition cumulative de moments $(M_{n,N})_N$. On suppose qu'il existe une suite $(M_n)_n$ telle que $M_{n,N} \rightarrow M_n$ lorsque $N \rightarrow \infty$. On suppose que la série

$$\sum_{n=0}^{+\infty} \frac{M_{n+1}}{n!} (it)^n$$

a un rayon de convergence non nul. Alors il existe une fonction de répartition cumulative R telle qu'en tout point de continuité x de R on a

$$\lim_{N \rightarrow \infty} R_N(x) = R(x).$$

D'autre part la suite $(M_n)_n$ est la suite des moments de R .

REMARQUE 5.2 Ce lemme résulte du critère d'unique détermination des fonctions de répartition cumulative par leurs moments (voir [Bil95, théorème 30.1]), et du théorème de Helly (voir [Bil95, corollaire du théorème 25.10]).

5.3 Moments

5.3.1 Calculs On calcule les moments positifs et négatifs de la variable aléatoire $L(sym^2, 1)$. Dans toute la suite, on considère des formes primitives de poids *fixé* et de niveau variable. En particulier, les majorations peuvent dépendre du poids sans que cela soit indiqué. On donne la version du lemme 1.7.4 qu'on utilisera. Elle s'en déduit grâce au lemme 2.3.1.

PROPOSITION 5.3.1

Soit N un entier sans facteur carré et m et n des entiers tels que $(m, N) = 1$ et $(n, N^2) | N$ alors

$$\frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\lambda_f(m) \lambda_f(n)}{L(sym^2 f, 1)} = \frac{1}{\zeta(2)} \delta(m, n) + O\left(N^{-1/2} \tau^4(N) \delta(m, n) + (mn)^{1/4} (n, N)^{-1/2} \tau^2(N) \varphi(N)^{-1} \tau_3((m, n)) \ln(2mnN)\right).$$

REMARQUE 5.3 En choisissant $m = n = 1$, cette proposition donne le moment d'ordre -1 de $L(sym^2, 1)$ sans condition sur le plus petit facteur premier du niveau.

Pour tous entiers $r \geq 1$ et $n \geq 0$, on définit les entiers

$$m_n(r) = \sum_{\substack{\mathbf{a}, \mathbf{b} \in \mathbb{N}^n \\ \det \mathbf{a}^2 \mathbf{b} = r}} \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{b}) \\ \det \mathbf{d} = \det \mathbf{b}}} 1$$

et

$$m_{-n}(r) = \sum_{\substack{\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n \\ \det \mathbf{a} \mathbf{b}^2 \mathbf{c}^3 = r}} \mu(a_1 b_1 c_1) \cdots \mu(a_n b_n c_n) \mu(b_1) \cdots \mu(b_n) \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{a} \mathbf{b}) \\ \det \mathbf{a} \mathbf{b} = \det \mathbf{d}}} 1.$$

On pose ensuite

$$M_{\pm n} = \frac{1}{\zeta(2)} \sum_{r=1}^{+\infty} \frac{m_{\pm n}(r)}{r}.$$

REMARQUE 5.4 Si $n \geq 0$, on a

$$\sum_{r=1}^{+\infty} \frac{m_n(r)}{r} = \zeta(2)^n \sum_{r=1}^{+\infty} \frac{\widehat{m}_n(r)}{r}$$

avec

$$\widehat{m}_n(r) = \sum_{\substack{\mathbf{b} \in \mathbb{N}^n \\ \det \mathbf{b} = r}} \sum_{\substack{\mathbf{d} \in \mathcal{E}_n(\mathbf{b}) \\ \det \mathbf{d} = r}} 1.$$

On a alors le

THÉORÈME 5.3.2

Pour tout $n \in \mathbb{Z}$, tout entier $N \geq 2$ sans facteur carré et tout réel $0 < \varepsilon < \frac{1}{100}$ on a

$$\frac{1}{\#B(N)} \sum_{f \in B(N)} L(sym^2 f, 1)^n = M_{n+1} + O\left(N^{-\varepsilon} + \frac{N^\varepsilon}{p_1(N)}\right).$$

La constante impliquée par O dépend de ε et n .

On énonce plusieurs lemmes dont découle la preuve du théorème. Si $\eta > 0$ est un paramètre fixé suffisamment petit, on définit l'ensemble $B^+(N; \eta)$ par

$$\{f \in B(N); L(sym^2 f, s) \neq 0, \forall s = \sigma + it, \sigma > 1 - \eta, |t| \leq \ln^3 N\}$$

puis le complémentaire $B^-(N; \eta) = B(N) - B^+(N; \eta)$. On a le lemme suivant dû à Luo dans le cas des formes de Maaß de niveau 1 et à Kowalski-Michel [KM01, théorème 1] dans le cas général

LEMME 5.3.3 (LEMMA 1, [LUO99])

Il existe $b > 0$ tel que pour tous $N \geq 2$ sans facteur carré et $0 < \eta < \frac{1}{100}$ on a la majoration

$$\sharp B^-(N; \eta) \ll N^{b\eta}$$

où la constante de majoration ne dépend que de η .

Si $0 < \alpha < 1$ est un paramètre fixé et si $x = N^\alpha$ on définit

$$\omega_f^{(\pm n)}(x) = \sum_{r=1}^{+\infty} \frac{\rho_f^{(\pm n)}(r)}{r} \exp(-r/x).$$

On a alors le

LEMME 5.3.4

Pour tout entier $N \geq 2$ sans facteur carré et tout entier $n \geq 1$; pour tous réels ε et η , $0 < \varepsilon, \eta < \frac{1}{100}$ et $x = N^\alpha$ avec $0 < \alpha < 1$; pour toute forme $f \in B^+(N; \eta)$ on a

$$L(sym^2 f, 1)^{\pm n} = \omega_f^{(\pm n)}(x) + O(N^\varepsilon x^{-\eta/2}).$$

La constante impliquée par O dépend de ε , η , α et n .

Démonstration – Si γ est le chemin reliant $1 - i\infty$, $1 - i \ln^2 N$, $-\frac{\eta}{2} - i \ln^2 N$, $-\frac{\eta}{2} + i \ln^2 N$, $1 + i \ln^2 N$ et $1 + i\infty$ on a pour $s \in \gamma$ la majoration

$$L(sym^2 f, s + 1)^{\pm n} \ll N^\varepsilon$$

grâce à [Luo99, lemma 2] et [Luo00, lemma 6]. En remarquant que $\omega_f^{(\pm n)}(x)$ s'écrit

$$\omega_f^{(\pm n)}(x) = \frac{1}{2i\pi} \int_{(1)} L(sym^2 f, s + 1)^{\pm n} \Gamma(s) x^s ds$$

on conclut par le théorème des résidus le long du contour délimité par γ et la droite $\Re(s) = 1$ et la majoration de Stirling. $\square$

On déduit ensuite de la proposition 5.3.1 le

LEMME 5.3.5

Pour tout entier sans facteur carré $N \geq 1$ et tous entiers $r \geq 1$, $(r, N) = 1$ et $n \geq 0$, pour tout réel $\varepsilon > 0$ on a

$$\frac{1}{\sharp B(N)} \sum_{f \in B(N)} \frac{\rho_f^{(\pm n)}(r)}{L(sym^2 f, 1)} = \frac{1}{\zeta(2)} m_{\pm n}(r) + O(N^{-1/2+\varepsilon} r^{1/2+\varepsilon}).$$

La constante impliquée par O dépend de n et ε .

On a aussi le

LEMME 5.3.6

Pour tout entier sans facteur carré $N \geq 2$ et tout entier $n \geq 1$; pour tous réels $\varepsilon > 0$ et $0 < \alpha < 1/10$, si $x = N^\alpha$, on a

$$\frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\omega_f^{(\pm n)}(x)}{L(\text{sym}^2 f, 1)} = \frac{1}{\zeta(2)} \sum_{r=1}^{+\infty} \frac{m_{\pm n}(r)}{r} + O\left(N^\varepsilon \left(\frac{1}{p_1(N)} + x^{-1/8}\right)\right).$$

La constante impliquée par O dépend de α , ε et n .

Démonstration – On a

$$\sum_{f \in B(N)} \frac{\omega_f^{(\pm n)}(x)}{L(\text{sym}^2 f, 1)} = \sum_{r=1}^{+\infty} \frac{\exp(-r/x)}{r} \sum_{f \in B(N)} \frac{\rho_f^{(\pm n)}(r)}{L(\text{sym}^2 f, 1)}.$$

La contribution des r non premiers à N est majorée par

$$\sum_{p|N} \sum_{r=1}^{+\infty} \frac{\exp(-pr/x)}{pr} \sum_{f \in B(N)} \frac{\rho_f^{(\pm n)}(rp)}{L(\text{sym}^2 f, 1)} \ll \#B(N) \frac{N^\varepsilon}{p_1(N)}.$$

Le lemme 5.3.5 donne alors

$$\begin{aligned} \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\omega_f^{(\pm n)}(x)}{L(\text{sym}^2 f, 1)} &= \frac{1}{\zeta(2)} \sum_{(r, N)=1} \frac{\exp(-r/x)}{r} m_{\pm n}(r) \\ &\quad + O\left(N^{-1/2+\varepsilon} x^{1/2} + \frac{N^\varepsilon}{p_1(N)}\right). \end{aligned}$$

On réinsère les r non premiers à N car $m_{\pm n}(r) \ll r^\varepsilon$ et on termine grâce à

$$\sum_{r=1}^{+\infty} \frac{\exp(-r/x)}{r} m_{\pm n}(r) = \sum_{r=1}^{+\infty} \frac{m_{\pm n}(r)}{r} + O(x^{-1/8})$$

qui résulte de ce que $m_{\pm n}(r) = 0$ s'il existe un nombre premier $p|r$. $\square$

On a alors, grâce à (2.20) et au lemme 5.3.3

$$\begin{aligned} \frac{1}{\#B(N)} \sum_{f \in B(N)} L(\text{sym}^2 f, 1)^{\pm n} &= \\ &= \frac{1}{\#B(N)} \sum_{f \in B^+(N; \eta)} \frac{L(\text{sym}^2 f, 1)^{\pm n+1}}{L(\text{sym}^2 f, 1)} + O(N^{b\eta+\varepsilon-1}) \end{aligned}$$

puis, grâce au lemme 5.3.4

$$\begin{aligned} \frac{1}{\#B(N)} \sum_{f \in B(N)} L(\text{sym}^2 f, 1)^{\pm n} &= \frac{1}{\#B(N)} \sum_{f \in B^+(N; \eta)} \frac{\omega_f^{(\pm n+1)}(x)}{L(\text{sym}^2 f, 1)} \\ &\quad + O(N^\varepsilon (N^{b\eta-1} + x^{-\eta/2})). \end{aligned}$$

Grâce à la majoration $\omega_f^{(\pm n+1)}(x) \ll N^\varepsilon$ on peut de nouveau introduire les formes de $B^-(N; \eta)$. On obtient alors grâce au lemme 5.3.6

$$\begin{aligned} \frac{1}{\#B(N)} \sum_{f \in B(N)} L(\text{sym}^2 f, 1)^{\pm n} &= \frac{1}{\zeta(2)} \sum_{r=1}^{+\infty} \frac{m_{\pm n+1}(r)}{r} \\ &\quad + O(N^\varepsilon (N^{b\eta-1} + x^{-\eta/2} + \frac{1}{p_1(N)})). \end{aligned}$$

On a ainsi prouvé le théorème 5.3.2.

5.3.2 Expression combinatoire des moments positifs Soit $n \geq 1$. La fonction $r \mapsto \widehat{m}_n(r)$ est multiplicative. Le moment M_n est donc déterminé par les coefficients $\widehat{m}_n(p^i)$. On ramène l'étude de ces coefficients à un problème combinatoire grâce à la réécriture de la définition de $\widehat{m}_n(p^i)$ dans le

LEMME 5.3.7

Soit $n \in \mathbb{N}$, $n > 1$, $p \in \mathcal{P}$ et $i \in \mathbb{N}$. On a $\widehat{m}_n(p^i) =$

$$\# \left\{ \begin{array}{l} \beta \in \mathbb{N}^n, \delta \in \mathbb{N}^{n-1}; \\ \text{tr } \beta = \text{tr } \delta = i, \\ \delta_\ell \leq 2 \min(\beta_1 + \dots + \beta_\ell - \delta_1 - \dots - \delta_{\ell-1}, \beta_{\ell+1}), 1 \leq \ell \leq n-1 \end{array} \right\}.$$

De plus, $\widehat{m}_1(p^i) = \delta(i, 0)$.

En particulier, $\widehat{m}_n(p^i)$ ne dépend pas de p et on définit

$$m_{n,i} = \widehat{m}_n(p^i)$$

de sorte que

$$M_n = \zeta(2)^{n-1} \prod_{p \in \mathcal{P}} \sum_{i=0}^{+\infty} m_{n,i} p^{-i}. \quad (5.2)$$

On déduit du lemme 5.3.7 une majoration des coefficients $m_{n,i}$ donnée dans le

LEMME 5.3.8

Soit $n \geq 2$ et $i \geq 0$ des entiers. On a

$$m_{n,i} \leq \sum_{\substack{\beta \in \mathbb{N}^n \\ \text{tr } \beta = i}} (2\beta_2 + 1) \cdots (2\beta_n + 1).$$

Démonstration – Il suffit de remarquer que, pour tout $1 \leq \ell \leq n-1$ on a $0 \leq \delta_\ell \leq 2\beta_{\ell+1}$. Il y a donc $(2\beta_2 + 1) \cdots (2\beta_n + 1)$ choix possibles de vecteurs δ . $\square$

REMARQUE 5.5 Pour ne pas briser la symétrie du rôle des coordonnées de β on utilisera plutôt la majoration (impliquée par le lemme)

$$m_{n,i} \leq \sum_{\substack{\beta \in \mathbb{N}^n \\ \text{tr } \beta = i}} (2\beta_1 + 1) \cdots (2\beta_n + 1). \quad (5.3)$$

Cette majoration demeure pour $n = 1$.

On obtient aussi une minoration dans le

LEMME 5.3.9

Il existe une entier i_0 tel que pour tout entier $n \geq i_0$ et tout entier $i_0 \leq i \leq n$ on a $m_{n,i} \geq C_n^i 3^{[1+O(1/\sqrt{i})]}$.

Démonstration – Soit $0 < i \leq n$. Dans la valeur de $m_{n,i}$ donnée au lemme 5.3.7, on regroupe les vecteurs β en sous-ensembles de β ayant exactement k coordonnées nulles pour tout entier k . Grâce à la condition sur $\text{tr } \beta$, on peut se restreindre à $n-i \leq k \leq n-1$. On obtient ainsi une partition de l'ensemble des β (cet ensemble étant la projection sur $\mathbb{N}^n$ de l'ensemble définissant $m_{n,i}$) en sous-ensembles notés $\mathcal{E}(n, i; k)$. À chaque vecteur β de $\mathcal{E}(n, i; k)$ on associe l'ensemble $\mathcal{F}(\beta, i)$ des vecteurs δ associés à β ainsi que le vecteur $\bar{\beta}$ de $\mathcal{E}(n-k, i; 0)$ formé à partir de β en

supprimant toutes les coordonnées nulles. Chaque coordonnée β_ℓ nulle impose une coordonnée $\delta_{\ell-1}$ nulle (et $\beta_1 = 0$ impose $\delta_1 = 0$), ainsi, $\mathcal{F}(\beta; i)$ est en bijection avec $\mathcal{F}(\bar{\beta}; i)$. Pour tout entier r , on note $m_{r,i}^*$ le cardinal de

$$\left\{ \begin{array}{l} \beta \in (\mathbb{N} - \{0\})^r, \delta \in \mathbb{N}^{r-1}; \\ \beta_1 + \cdots + \beta_r = i, \\ \delta_\ell \leq 2 \min(\beta_1 + \cdots + \beta_\ell - \delta_1 - \cdots - \delta_{\ell-1}, \beta_{\ell+1}), 1 \leq \ell \leq r-1 \\ \delta_1 + \cdots + \delta_{r-1} = i \end{array} \right\}.$$

On a alors

$$m_{n,i} = \sum_{k=n-i}^{n-1} C_n^k m_{n-k,i}^* = \sum_{r=1}^i C_n^r m_{r,i}^*.$$

Par positivité, on a

$$m_{n,i} \geq C_n^i m_{i,i}^*. \quad (5.4)$$

On minore maintenant $m_{i,i}^*$. Le seul vecteur β intervenant dans le calcul de $m_{i,i}^*$ est le vecteur dont toutes les coordonnées sont 1. On vérifie de plus que la condition sur $\text{tr } \delta$ et la condition

$$0 \leq \delta_{i-1} \leq 2 \min(\beta_1 + \cdots + \beta_{i-1} - \delta_1 - \cdots - \delta_{i-2}, \beta_i)$$

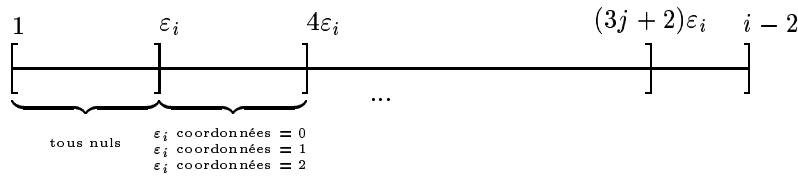
imposent $\delta_{i-1} = 2$. Pour tout vecteur δ et tout entier ℓ on note $s_\ell = \ell - \delta_1 - \cdots - \delta_{\ell-1}$. Il nous faut donc trouver $\delta_1, \dots, \delta_{i-2}$ tels que $s_{i-1} = 1$ et

$$0 \leq \delta_\ell \leq 2 \min(s_\ell, 1), \quad 1 \leq \ell \leq i-2. \quad (5.5)$$

On a toujours $\delta_\ell \in \{0, 1, 2\}$. Les coordonnées $\delta_\ell = 0$ interviennent « positivement », les coordonnées $\delta_\ell = 1$ interviennent « de façon neutre », et les coordonnées $\delta_\ell = 2$ interviennent « négativement » au sens où l'on a les implications

$$\begin{array}{lll} \delta_\ell = 0 & \Rightarrow & s_{\ell+1} = s_\ell + 1 \\ \delta_\ell = 1 & \Rightarrow & s_{\ell+1} = s_\ell \\ \delta_\ell = 2 & \Rightarrow & s_{\ell+1} = s_\ell - 1. \end{array}$$

On définit ε_i comme le plus petit entier supérieur à $\sqrt{i}$ et l'entier j tel que $(3j+2)\varepsilon_i < i-2 \leq (3j+5)\varepsilon_i$. On place les coordonnées de δ sur un axe et on résume la fin de la démonstration sur le schéma suivant.



On choisit $\delta_1 = \cdots = \delta_{\varepsilon_i} = 0$. On a alors $s_{\varepsilon_i+1} = \varepsilon_i + 1$. Puis, parmi $\delta_{\varepsilon_i+1}, \dots, \delta_{4\varepsilon_i}$ on fixe ε_i coordonnées égales à 0, ε_i coordonnées égales à 1 et ε_i coordonnées égales à 2. La condition (5.5) est ainsi satisfaite pour ces coordonnées. On a $s_{4\varepsilon_i+1} = \varepsilon_i + 1$. On fixe $\delta_{4\varepsilon_i+1}, \dots, \delta_{7\varepsilon_i}$ de la même façon puis on répète le processus jusqu'à avoir fixé $\delta_{\varepsilon_i}, \dots, \delta_{(3j+1)\varepsilon_i}$. On a alors $s_{(3j+1)\varepsilon_i+1} = \varepsilon_i + 1$. On a alors à choisir $i-2 - (3j+1)\varepsilon_i$ coordonnées dont la somme est $i-2 - 3j\varepsilon_i$. On choisit alors ε_i coordonnées égales à 2 et les $i-2 - (3j+2)\varepsilon_i$ restantes égales à 1. On a ainsi construit $(C_{3\varepsilon_i}^{\varepsilon_i} C_{2\varepsilon_i}^{\varepsilon_i})^j$ vecteurs δ satisfaisants. Or d'après la formule de Stirling on a

$$C_{3\varepsilon_i}^{\varepsilon_i} C_{2\varepsilon_i}^{\varepsilon_i} = \frac{\sqrt{3}}{2\pi} \frac{3^{3\varepsilon_i}}{\varepsilon_i} \left[1 + O\left(\frac{1}{\varepsilon_i}\right) \right]$$

d'où $m_{i,i}^* \geq 3^{i[1+O(1/\sqrt{i})]}$. Le résultat du lemme s'obtient alors grâce à la minoration (5.4). $\square$

5.3.3 Encadrement La majoration (5.3) de $m_{n,i}$ donne la majoration suivante des moments

PROPOSITION 5.3.10

Pour tout entier $n \geq 2$ on a $\ln M_n \leq 3n \ln \ln n + O(n)$.

Démonstration – On déduit de (5.3) la majoration

$$\sum_{i=2}^{+\infty} \frac{m_{n,i}}{p^i} \leq \sum_{i=2}^{+\infty} \sum_{\substack{\beta \in \mathbb{N}^n \\ \text{tr } \beta = i}} \frac{(2\beta_1 + 1) \cdots (2\beta_n + 1)}{p^{\beta_1} \cdots p^{\beta_n}}.$$

D'autre part, $m_{n,1} = 0$ d'où

$$\sum_{i=0}^{+\infty} \frac{m_{n,i}}{p^i} \leq \left(\sum_{\beta=0}^{+\infty} \frac{2\beta + 1}{p^\beta} \right)^n - \frac{3n}{p}.$$

On déduit de (5.2) la majoration

$$M_n \leq \zeta(2)^{n-1} \prod_{p \in \mathcal{P}} \left[\frac{(1 + p^{-1})^n}{(1 - p^{-1})^{2n}} - \frac{3n}{p} \right].$$

On conclut grâce à

$$\prod_{p \leq n} \frac{(1 + p^{-1})^n}{(1 - p^{-1})^{2n}} \leq (\ln n)^{3n} e^{O(n)}$$

et

$$\prod_{p > n} \left[\frac{(1 + p^{-1})^n}{(1 - p^{-1})^{2n}} - \frac{3n}{p} \right] = \prod_{p > n} \left[1 + O\left(\frac{n^2}{p^2}\right) \right] = e^{O(n)}.$$

$\square$

Le lemme 5.3.9 donne alors la minoration des moments suivante.

PROPOSITION 5.3.11

Pour tout entier $n \geq 2$ on a $M_n \geq (\ln n)^{3n} e^{O(n)}$.

Démonstration – Grâce au lemme 5.3.9 on a, pour n assez grand,

$$\begin{aligned} M_n &\geq \prod_{p \leq \sqrt{n}} \left(1 + \sum_{i=i_0}^n \frac{C_n^i}{p^i} 3^{i(1+O(1/\sqrt{i}))} \right) \\ &\geq 3^{O(n)} \prod_{p \leq \sqrt{n}} \left(1 + \sum_{i=i_0}^n C_n^i \frac{3^i}{p^i} \right) \\ &\geq 3^{O(n)} \prod_{p \leq \sqrt{n}} \left(1 - \frac{1}{p^{i_0}} \right) \left(1 + \frac{3}{p} \right)^n \end{aligned}$$

d'où $M_n \geq (\ln n)^{3n} e^{O(n)}$. $\square$

5.4 Distribution

Soit I et Z des applications de $\mathcal{N}$ dans $\mathbb{R}^+$. L'inégalité de Markov (5.1) pour la variable $L(sym^2, 1)$ donne pour tout n entier positif

$$\frac{1}{\#B(N)} \#\{f \in B(N); L(sym^2 f, 1) \geq I(N)\} \leq \frac{M_{n+1}(N)}{I(N)^n}.$$

Cette même inégalité de Markov appliquée à la variable $L(sym^2, 1)^{-1}$ donne

$$\frac{1}{\#B(N)} \#\{f \in B(N); L(sym^2 f, 1) \leq Z(N)\} \leq M_{-n+1}(N) Z(N)^n$$

soit encore

$$\frac{1}{\#B(N)} \#\{f \in B(N); L(sym^2 f, 1) > Z(N)\} \geq 1 - M_{-n+1}(N) Z(N)^n.$$

On déduit de ces considérations la

PROPOSITION 5.4.1

Soit $Z, I : \mathcal{N} \rightarrow \mathbb{R}^+$ des applications. Pour tout n entier positif, on a lorsque N parcourt $\mathcal{N}$

$$\frac{1}{\#B(N)} \#\{f \in B(N); L(sym^2 f, 1) \geq Z(N)\} = 1 + O(Z(N)^n)$$

et

$$\frac{1}{\#B(N)} \#\{f \in B(N); L(sym^2 f, 1) \geq I(N)\} = O(I(N)^{-n}).$$

La minoration des moments positifs obtenue à la proposition 5.3.11 permet de prouver la

PROPOSITION 5.4.2

L'ensemble $\{L(sym^2 f, 1); f \in B(N), N \in \mathcal{N}\}$ n'est pas borné.

Démonstration – On suppose par l'absurde qu'il existe une constante C telle que l'on ait, pour tout $N \in \mathcal{N}$ la majoration $L(sym^2 f, 1) \leq C$. On obtiendrait alors, pour tout entier $n \geq 0$ la majoration sur les moments $M_{n+1} \leq C^n$. Cette majoration contredirait la minoration $M_{n+1} \geq (\ln n)^{3n} e^{O(n)}$ de la proposition 5.3.11. $\square$

La majoration des moments positifs de la proposition 5.3.10 permet d'affirmer que la série

$$\sum_{n=1}^{+\infty} \frac{M_{n+1}}{n!} (it)^n$$

a un rayon de convergence infini. Grâce au lemme 5.2.1 on déduit alors la

PROPOSITION 5.4.3

Si N parcourt $\mathcal{N}$, il existe une fonction de répartition cumulative R telle qu'en tout point de continuité x de R on a,

$$\lim_{N \rightarrow \infty} \frac{1}{\#B(N)} \#\{f \in B(N); L(sym^2 f, 1) \leq x\} = R(x).$$

De plus, pour tout entier n , le moment d'ordre n de cette fonction de répartition cumulative est M_n .

Autrement dit, la variable aléatoire $L(sym^2, 1)$ converge en loi vers une variable aléatoire $L(sym^2, 1)_\infty$.

5.5 Espérance et variance

L'espérance de la variable aléatoire $L(sym^2, 1)_\infty$ est donnée dans la

PROPOSITION 5.5.1

L'espérance de la variable aléatoire $L(sym^2, 1)_\infty$ est

$$E[L(sym^2, 1)_\infty] = \zeta(2)^2.$$

Démonstration – L'espérance d'une variable aléatoire est son premier moment. On prouve donc $M_2 = \zeta(2)^2$. On a

$$\begin{aligned} \widehat{m}_2(r) &= \#\{(b_1, b_2) \in \mathbb{N}^2 ; b_1 b_2 = r, b_1 b_2 | (b_1, b_2)^2\} \\ &= \begin{cases} 1 & \text{si } r \text{ est un carré;} \\ 0 & \text{sinon} \end{cases} \end{aligned}$$

d'où $M_2 = \zeta(2)^2$. $\square$

L'espérance d'une variable aléatoire est la meilleure constante d'approximation quadratique. L'erreur commise est donnée par la variance.

PROPOSITION 5.5.2

La variance de la variable aléatoire $L(sym^2, 1)_\infty$ est

$$\text{Var}[L(sym^2, 1)_\infty] = \zeta(2)^4 \left[\frac{\zeta(2)\zeta(3)}{\zeta(6)} - 1 \right] \approx 6,908.$$

Démonstration – Il faut montrer

$$M_3 = \zeta(2)^2 \prod_{p \in \mathcal{P}} \frac{1 + p^{-3}}{(1 - p^{-2})^3}.$$

On commence par calculer $m_{3,i}$. Grâce au lemme 5.3.7 la valeur de $m_{3,i}$ est le cardinal de l'ensemble des $(\beta_1, \beta_2, \beta_3, \delta_1, \delta_2) \in \mathbb{N}^5$ satisfaisant aux conditions

$$\beta_1 + \beta_2 + \beta_3 = i \tag{5.6a}$$

$$\delta_1 \leq 2 \min(\beta_1, \beta_2)$$

$$\delta_2 \leq 2 \min(\beta_1 + \beta_2 - \delta_1, \beta_3) \tag{5.6b}$$

$$\delta_1 + \delta_2 = i. \tag{5.6c}$$

On a nécessairement $\delta_1 = i - 2\beta_3$: en effet si $\beta_1 + \beta_2 - \delta_1 \neq \beta_3$ alors la condition (5.6b) implique $\delta_1 + \delta_2 < \beta_1 + \beta_2 + \beta_3$ ce qui contredit les conditions (5.6a) et (5.6c) ; ainsi $\delta_1 = \beta_1 + \beta_2 - \beta_3 = i - 2\beta_3$. On déduit alors de (5.6c) que $\delta_2 = 2\beta_3$. Ainsi a-t-on

$$m_{3,i} = \left\{ \begin{array}{l} (\beta_1, \beta_2, \beta_3) \in \mathbb{N}^3 ; \\ \beta_1 + \beta_2 + \beta_3 = i \\ 0 \leq i - 2\beta_3 \leq 2 \min(\beta_1, \beta_2) \end{array} \right\}.$$

Si $m_{3,i}^\equiv$ est la contribution à $m_{3,i}$ des triplets $(\beta_1, \beta_2, \beta_3)$ tels que $\beta_1 = \beta_2$ et si $m_{3,i}^<$ est la contribution à $m_{3,i}$ des triplets $(\beta_1, \beta_2, \beta_3)$ tels que $\beta_1 < \beta_2$ on a

$$m_{3,i} = m_{3,i}^\equiv + 2m_{3,i}^<.$$

On a

$$m_{3,i}^\equiv = \#\left\{ \beta_3 \in \mathbb{N}; \beta_3 \leq \frac{i}{2}, \frac{i - \beta_3}{2} \in \mathbb{N} \right\}$$

donc

$$m_{3,i}^{\overline{}} = \# \left[\frac{i}{4}, \frac{i}{2} \right] \cap \mathbb{N}.$$

puis

$$\begin{cases} m_{3,4i}^{\overline{}} &= i+1 \\ m_{3,4i+1}^{\overline{}} &= i \\ m_{3,4i+2}^{\overline{}} &= i+1 \\ m_{3,4i+3}^{\overline{}} &= i+1 \end{cases}$$

D'autre part,

$$m_{3,i}^{<} = \# \left\{ \begin{array}{l} (\beta_1, \beta_3) \in \mathbb{N}^2; \\ \frac{i}{2} - \beta_3 \leq \beta_1 < \frac{i-\beta_3}{2} \\ \beta_3 \leq \frac{i}{2} \end{array} \right\}$$

soit

$$m_{3,i}^{<} = \sum_{\beta \leq \frac{i}{2}} \# \left[\frac{i}{2} - \beta, \frac{i-\beta}{2} \right] \cap \mathbb{N}.$$

et

$$\begin{cases} m_{3,4i}^{<} &= i(i+1) \\ m_{3,4i+1}^{<} &= i^2 \\ m_{3,4i+2}^{<} &= (i+1)^2 \\ m_{3,4i+3}^{<} &= i(i+1). \end{cases}$$

On en déduit

$$\begin{cases} m_{3,4i} &= 2i^2 + 3i + 1 \\ m_{3,4i+1} &= 2i^2 + i \\ m_{3,4i+2} &= 2i^2 + 5i + 3 \\ m_{3,4i+3} &= 2i^2 + 3i + 1. \end{cases}$$

On calcule alors

$$\sum_{i=1}^{+\infty} \frac{m_{3,i}}{p^i} = \frac{1+p^{-6}}{(1-p^{-2})^3}$$

puis

$$M_3 = \zeta(2)^2 \prod_{p \in \mathcal{P}} \frac{1+p^{-3}}{(1-p^{-2})^3} = \zeta(2)^5 \frac{\zeta(3)}{\zeta(6)}.$$

□

5.6 Dépendance avec les valeurs propres de Hecke

Si q est un nombre premier ne divisant pas N , on étudie la dépendance de $L(sym^2 f, 1)$ et $\lambda_f(q)$. Pour cela, on va montrer que cette dépendance n'est due qu'au q -ième facteur eulerien de $L(sym^2 f, s)$. À cet effet on définit

$$\begin{aligned} L^{(q)}(sym^2 f, s) &= \prod_{p \neq q} L(sym_p^2 f, s) \\ &= L(sym^2 f, s) L(sym_q^2 f, s)^{-1}. \end{aligned}$$

Soit $X : B(N) \rightarrow \mathbb{C}$ une application, on définit $M_N^h(X)$ par

$$M_N^h(X) = \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\zeta(2)}{L(sym^2 f, 1)} X(f).$$

La proposition 5.3.1 permet de voir M_N^h comme un opérateur de moyenne puisque

$$M_N^h(1) = 1 + O(N^{-1/2}\tau^4(N)).$$

On a alors la

PROPOSITION 5.6.1

Soit q un nombre premier, deux entiers $m \geq 0$ et $n > 0$. Lorsque N parcourt $\mathcal{N}$ on a

$$\lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\zeta(2)}{L(\text{sym}^2 f, 1)} L^{(q)}(\text{sym}^2 f, 1)^m \lambda_f(q^n) = 0.$$

Démonstration – On note ε_q la fonction caractéristique des entiers premiers à q . On peut voir $L^{(q)}(\text{sym}^2 f, s)$ comme la fonction L de carré symétrique de la forme parabolique $f \otimes \varepsilon_q$ de poids k et de niveau Nq^2 (qui n'est plus sans facteur carré!). Les coefficients de cette forme vérifient la majoration de Deligne et la formule de multiplicativité de Hecke. Le calcul des moments se réécrit donc ligne à ligne dans ce cas (c'est-à-dire en remplaçant $\lambda_f(n)$ par $\varepsilon_q(n)\lambda_f(n)$ et en insérant un facteur ε_q lorsque la formule de multiplicativité intervient). On obtient alors le même résultat en remplaçant $m_n(r)$ par $m_{m,n}(r)$ où

$$m_{m,n}(r) = \frac{1}{\zeta(2)} \sum_{\det \mathbf{a}^2 \mathbf{b} = r} \varepsilon_q(\det \mathbf{b}) \#\{\mathbf{d} \in \mathcal{E}_m(\mathbf{b}); q^n \det \mathbf{d}^2 = \det \mathbf{b}^2\}.$$

Or pour que la somme soit non vide, il faut que pour chaque i on ait $(q, b_i) = 1$. Mais si $n \neq 0$, cela implique que l'ensemble intervenant dans la définition de $m_{m,n}(r)$ est vide. On a alors $m_{m,n}(r) = 0$ et

$$\lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{L^{(q)}(\text{sym}^2 f, 1)^m}{L(\text{sym}^2 f, 1)} \lambda_f(q^n) = 0.$$

□

On en déduit la

PROPOSITION 5.6.2

Soit q un nombre premier, $m \geq 0$ et $n \geq 0$ deux entiers. Lorsque N parcourt $\mathcal{N}$ on a

$$\begin{aligned} \lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\zeta(2)}{L(\text{sym}^2 f, 1)} L^{(q)}(\text{sym}^2 f, 1)^m \lambda_f(q)^n = \\ \lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\zeta(2)}{L(\text{sym}^2 f, 1)} \lambda_f(q^n) \\ \times \lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} \frac{1}{\#B(N)} \sum_{f \in B(N)} \frac{\zeta(2)}{L(\text{sym}^2 f, 1)} L^{(q)}(\text{sym}^2 f, 1)^m. \end{aligned}$$

On en déduit en particulier le

COROLLAIRE 5.6.3

Soit q un nombre premier. Dans les espaces probabilisés munis de la moyenne $\frac{M_N^h}{M_N^h(1)}$, les variables aléatoires limites, lorsque N parcourt $\mathcal{N}$ en restant premier à q , des variables aléatoires

$$\begin{array}{ccc} \lambda(q) & : & B(N) \rightarrow \mathbb{R} \\ & & f \mapsto \lambda_f(q) \end{array}$$

et $L^{(q)}(\text{sym}^2, 1)$ sont indépendantes.

Démonstration – Pour tout entier $n \geq 0$ on a

$$\lambda_f(q)^n = \sum_{i=0}^n h_n(i) \lambda_f(q^i)$$

avec

$$h_n(i) = \frac{2^{n+1}}{\pi} \int_0^\pi \cos^n \theta \sin(i+1)\theta \sin \theta \, d\theta$$

(voir, par exemple, [CDF97, lemma 3]). Ainsi, grâce à la proposition 5.6.1 on obtient

$$\lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} M_N^h[L^{(q)}(\text{sym}^2, 1)^m \lambda(q)^n] = h_n(0) \lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} M_N^h[L^{(q)}(\text{sym}^2, 1)^m].$$

En prenant $m = 0$ dans cette dernière équation, on obtient

$$h_n(0) = \lim_{\substack{N \rightarrow +\infty \\ (N,q)=1}} M_N^h[\lambda(q)^n]$$

ce qui permet de conclure. $\square$

REMARQUE 5.6 Les travaux d'Iwaniec, Luo et Sarnak, et notamment une formule à la Eichler-Shimura [ILS00, proposition 2.13] permettent, en reprenant pas à pas les calculs du paragraphe 5.3.1 de remplacer la moyenne M_N^h par la moyenne naturelle et ainsi de prouver la proposition annoncée en introduction.

Chapitre 6

Détermination des formes modulaires par les valeurs de fonctions L

L'ensemble de ces résultats présentés dans ce chapitre a été obtenu avec François Martin. On donne une application de la théorie des périodes à la détermination des formes modulaires, non nécessairement primitives, par les valeurs de leurs fonctions L .

6.1 Introduction

Soit Γ un sous-groupe de congruence de $SL(2, \mathbb{Z})$ et k un entier, on note $S(2k, \Gamma)$ l'espace des formes modulaires paraboliques de poids $2k$ sur Γ (voir le §6.3.1). Si $(\mathcal{L}_1, \dots, \mathcal{L}_n)$ est un ensemble de formes linéaires sur $S(2k, \Gamma)$, on dit que cet ensemble caractérise la forme $f \in S(2k, \Gamma)$ si on a l'implication

$$\forall g \in S(2k, \Gamma), \begin{cases} \mathcal{L}_1(f) = \mathcal{L}_1(g) \\ \vdots \\ \mathcal{L}_n(f) = \mathcal{L}_n(g) \end{cases} \implies (f = g).$$

Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice de $SL(2, \mathbb{Z})$ et $f \in S(2k, \Gamma)$, on définit une fonction $f|_A$ sur le demi-plan de Poincaré $\mathcal{H}$ en posant

$$f|_A(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right).$$

À cette fonction, on peut associer une fonction L dont les valeurs intéressantes sont les valeurs aux entiers de $[1, 2k - 1]$ (voir §6.3.2). On s'intéresse dans cet article aux formes linéaires $f \mapsto L(f|_A, \ell)$ lorsque A parcourt un ensemble de représentants du quotient $\Gamma \backslash SL(2, \mathbb{Z})$. On prouve le

THÉORÈME 6.1.1

Soit Γ un sous-groupe de congruence de $SL(2, \mathbb{Z})$ contenant $-I$ et k un entier strictement positif. Soit $f \in S(2k, \Gamma)$. Il existe un sous-ensemble $\mathcal{R}$ de $SL(2, \mathbb{Z}) \times \{1, \dots, 2k - 1\}$ de cardinal

$$\frac{2k - 1}{6} [SL(2, \mathbb{Z}) : \Gamma] + \varepsilon_S(2k) \frac{\nu_2(\Gamma)}{2} + 2\varepsilon_U(2k) \frac{\nu_3(\Gamma)}{3} + \delta(k = 1)$$

tel que

$$[\forall(A, \ell) \in \mathcal{R}, \forall g \in S(2k, \Gamma), L(f|_A, \ell) = L(g|_A, \ell)] \Rightarrow (f = g).$$

Dans cet énoncé, $\delta(k = 1)$ vaut 1 si $k = 1$ et 0 sinon. Les fonctions ε_S et ε_U sont définies par

$$\varepsilon_S(2k) = \begin{cases} 1 & \text{si } 2k \equiv 0 \pmod{4}; \\ -1 & \text{si } 2k \equiv 2 \pmod{4} \end{cases}$$

et

$$\varepsilon_U(2k) = \begin{cases} 0 & \text{si } 2k \equiv 1 \pmod{3}; \\ 1 & \text{si } 2k \equiv 0 \pmod{3}; \\ -1 & \text{si } 2k \equiv -1 \pmod{3}. \end{cases}$$

Le nombre $\nu_2(\Gamma)$ (*resp.* $\nu_3(\Gamma)$) est le nombre de points elliptiques d'ordre 2 (*resp.* d'ordre 3) de Γ . À titre d'exemple, on a

$$\nu_2(\Gamma_0(m)) = \begin{cases} 0 & \text{si } 4|m; \\ \prod_{p|m} [1 + (\frac{-1}{p})] & \text{sinon} \end{cases}$$

et

$$\nu_3(\Gamma_0(m)) = \begin{cases} 0 & \text{si } 9|m; \\ \prod_{p|m} [1 + (\frac{-3}{p})] & \text{sinon.} \end{cases}$$

[Miy89, theorem 4.2.7] Ce résultat est à comparer avec la dimension de $S(2k, \Gamma)$, [Miy89, theorem 2.5.2, lemma 4.2.6, theorem 4.2.11]

$$\dim S(2, \Gamma) = 1 + \frac{\nu_0(\Gamma)}{12} - \frac{\nu_2(\Gamma)}{4} - \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}$$

et, si $2k \geq 4$,

$$\dim S(2k, \Gamma) = \frac{2k-1}{12} \nu_0(\Gamma) + \frac{\nu_2(\Gamma)}{4} + \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}$$

où $\nu_\infty(\Gamma)$ est le nombre de pointes de Γ (voir §6.3.1).

Sans restriction sur $S(2k, \Gamma)$, on a le minorant

$$\sharp \mathcal{R} \geq \dim S(2k, \Gamma).$$

D'autres grandeurs que les formes linéaires utilisées ici ont été étudiées. Si $f \in S(2k, m) = S(2, \Gamma_0(m))$, elle admet un développement de Fourier

$$f(z) = \sum_{n=1}^{+\infty} \widehat{f}(n) e^{2i\pi n z}$$

et on définit, pour tout caractère χ , la fonction

$$L(f \otimes \chi, s) = \sum_{n=1}^{+\infty} \widehat{f}(n) \chi(n) n^{-s}.$$

Luo et Ramakrishnan [LR97b] ont prouvé (entre autre) que l'ensemble des valeurs $L(f \otimes \chi, k)$ lorsque χ parcourt tous les caractères quadratiques de module premier à m détermine f . D'autre part, si $f \in S(2, m)$, on dit que f est associée à une courbe elliptique si sa fonction L coïncide avec celle d'une courbe elliptique. Stark

[Sta96] a prouvé que la valeur $L(f, 1)$ caractérise la forme f . On remarque qu'on a fait une grosse restriction sur $S(2, m)$ puisque, si on note $Ell(2, m)$ l'ensemble (fini) des formes de $S(2, m)$ associées à une courbe elliptique, on a pour tout $\varepsilon > 0$,

$$\frac{\#Ell(2, m)}{\dim S(2, m)} \leq C(\varepsilon)m^{-1/2+\varepsilon}$$

avec $C(\varepsilon)$ une constante ne dépendant que de ε [DK00].

Notre méthode consiste à tirer parti des relations de Manin. À chaque forme f on peut associer un polynôme appelé polynôme de périodes (voir §6.3.1). Ce polynôme vérifie des relations que l'on peut traduire en relations linéaires sur les valeurs $L(f|_A, \ell)$. Un morphisme injectif, dû essentiellement à Eichler et Shimura (et Skorrupa dans la version utilisée ici) permet alors de ramener notre problème au calcul du rang d'un système linéaire (voir §6.4). Ce calcul est essentiellement un travail de combinatoire, nous établirons les résultats combinatoires nécessaires au §6.2.

On déduit une autre conséquence de l'épimorphisme d'Eichler-Shimura, indépendante de la précédente. Pour p premier, on définit $X(p)$ comme l'ensemble des $p-1$ caractères modulo p et W_p l'involution de Fricke (voir §6.5). On a alors la

PROPOSITION 6.1.2

Soit k un entier et p un nombre premier. Soit f et g deux formes de $S(2k, \Gamma_0(p))$. On suppose que

$$\begin{aligned} \forall \ell \in [1, k], \forall \chi \in X(p), \quad L(W_p f \otimes \chi, \ell) &= L(W_p g \otimes \chi, \ell), \\ \forall \ell \in [1, k], \quad L(W_p f, \ell) &= L(W_p g, \ell) \end{aligned}$$

et

$$\forall \ell \in [1, k], \quad L(f, \ell) = L(g, \ell).$$

Alors, $f = g$.

On utilise les notations

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, T' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

et si E est une expression pouvant prendre uniquement la valeur vraie ou la valeur fausse, $\delta(E)$ vaut 1 si E est vraie et 0 sinon. Enfin on fait la convention $\binom{a}{b} = 0$ si $b < 0$ ou $b > a$.

6.2 Lemmes combinatoires

On établit dans ce paragraphe des lemmes combinatoires nécessaires à la suite.

LEMME 6.2.1

Soit $n \geq 0$ un entier. Soit ℓ et t des entiers tels que $0 \leq \ell \leq n$ et $0 \leq t \leq n$. Alors

$$\sum_{u=0}^{\min(t, \ell)} (-1)^u \binom{t}{u} \binom{n-u}{n-\ell} = \binom{n-t}{\ell}.$$

Démonstration – Lorsque $t \leq \ell$ le résultat est conséquence de l'égalité

$$\begin{aligned} (n-\ell)! \sum_{u=0}^t (-1)^u \binom{t}{u} \binom{n-u}{n-\ell} \\ = \sum_{v=0}^{n-\ell} \binom{n-\ell}{v} \frac{d^v}{dX^v} \Big|_{X=1} (X-1)^t \frac{d^{n-\ell-v}}{dX^{n-\ell-v}} \Big|_{X=1} X^{n-t}. \end{aligned}$$

On utilise ce cas et l'égalité

$$\sum_{u=0}^{\ell} (-1)^u \binom{t}{u} \binom{n-u}{n-\ell} = \frac{t!(n-t)!}{(n-\ell)! \ell!} \sum_{u=0}^{\ell} (-1)^u \binom{\ell}{u} \binom{n-u}{n-t}$$

pour prouver le cas $t > \ell$. $\square$

LEMME 6.2.2

Soit j, ℓ, r des entiers tels que $\ell \geq 1$ et $j - r \notin [1, \ell - 1]$. Alors

1)

$$\sum_{t=0}^r \left[\binom{\ell+t-1}{2t} \binom{j-\ell-t}{2r-2t} + \binom{\ell+t-1}{2t+1} \binom{j-\ell-t-1}{2r-2t-1} \right] = \binom{j-1}{2r}$$

2)

$$\sum_{t=0}^{r-1} \left[\binom{\ell+t-1}{2t} \binom{j-\ell-t-1}{2r-2t-1} + \binom{\ell+t}{2t+1} \binom{j-\ell-t-1}{2r-2t-2} \right] = \binom{j-1}{2r-1}$$

3)

$$\sum_{t=0}^{r-1} \left[\binom{\ell+t-1}{2t} \binom{j-\ell-t}{2r-2t-1} + \binom{\ell+t-1}{2t+1} \binom{j-\ell-t-1}{2r-2t-2} \right] = \binom{j-1}{2r-1}$$

4)

$$\sum_{t=0}^r \left[\binom{\ell+t-1}{2t} \binom{j-\ell-t-1}{2r-2t} + \binom{\ell+t}{2t+1} \binom{j-\ell-t-1}{2r-2t-1} \right] = \binom{j-1}{2r}.$$

Démonstration – Pour prouver le point 1, on note $S(\ell)$ le membre de gauche. On a $S(1) = \binom{j-1}{2r}$ et l'égalité de Pascal implique, pour $\ell \neq j - r$ l'égalité $S(\ell+1) = S(\ell)$. Les autres points se démontrent de façon identique. $\square$

Pour tous entiers $k \geq 0$ et $r \geq 1$, on définit les polynômes $P_0^k(X) = 1$,

$$P_{2r}^k(X) = \frac{1}{(2r)!} \prod_{u=0}^{2r-1} (k+r-u-X)$$

et

$$P_{2r-1}^k(X) = \frac{1}{(2r-1)!} \prod_{u=1}^{2r-1} (k+r-u-X).$$

Pour tout $j \in \mathbb{Z}$ on a les relations

$$P_{2r}^k(j) = \begin{cases} \binom{k+r-j}{2r} & \text{si } j \leq k-r; \\ \binom{j-k+r-1}{2r} & \text{si } j > k+r; \\ 0 & \text{sinon} \end{cases} \quad (6.1a)$$

et

$$P_{2r-1}^k(j) = \begin{cases} \binom{k+r-j-1}{2r-1} & \text{si } j \leq k-r; \\ -\binom{j-k+r-1}{2r-1} & \text{si } j > k+r-1; \\ 0 & \text{sinon.} \end{cases} \quad (6.1b)$$

On déduit du lemme 6.2.2 le

COROLLAIRE 6.2.3

Soit $r > 0$.

1) Si $k - r \geq 1$,

$$P_{2r}^k(j) = \binom{j-1}{2r} + \sum_{t=0}^{r-1} \left[\binom{k-r+t}{2t+1} P_{2r-2t-1}^k(j) - \binom{k-r+t}{2t+2} P_{2r-2t-2}^k(j) \right]$$

2) si $k - r \geq 2$,

$$P_{2r-1}^k(j) = -\binom{j-1}{2r-1} + (k-r)P_{2r-2}^k(j) - \sum_{t=1}^{r-1} \left[\binom{k-r+t}{2t} P_{2r-2t-1}^k(j) - \binom{k-r+t}{2t+1} P_{2r-2t-2}^k(j) \right].$$

Démonstration – On se ramène aux points 1 et 2 du lemme 6.2.2 en utilisant les égalités (6.1). En remarquant qu'il s'agit d'égalités de polynômes, on peut en effet supposer j suffisamment grand. $\square$

LEMME 6.2.4

Soit $\ell \in \mathbb{N}$,

1) si $r \in \mathbb{Z} \setminus \{0\}$,

$$\sum_{t=0}^r \left[\binom{t+\ell-r}{2t+1} \binom{\ell-1+r-t}{2r-2t-1} - \binom{t+\ell-r}{2t} \binom{\ell-1+r-t}{2r-2t} \right] = 0$$

2) si $r \in \mathbb{Z}$,

$$\sum_{t=0}^r \left[\binom{t+\ell-r}{2t+1} \binom{\ell+r-t}{2r-2t} - \binom{t+\ell-r}{2t} \binom{\ell+r-t}{2r-2t+1} \right] = 0$$

3) si $r \in \mathbb{Z}$,

$$\sum_{t=0}^r \left[\binom{t+\ell-1}{2t} \binom{\ell-t}{2r-2t+1} - \binom{t+\ell}{2t+1} \binom{\ell-1-t}{2r-2t} \right] = 0$$

4) si $r \in \mathbb{Z} \setminus \{0\}$,

$$\sum_{t=0}^r \left[\binom{t+\ell}{2t} \binom{\ell-t}{2r-2t} - \binom{t+\ell}{2t+1} \binom{\ell-t}{2r-2t-1} \right] = 0.$$

Démonstration – Le principe de démonstration est le même que pour le lemme 6.2.2.

$\square$

LEMME 6.2.5

1) Soit (b_ℓ^v) l'unique suite définie par

$$b_\ell^v = \begin{cases} 0 & \text{si } v < \ell \text{ ou } \ell < 1; \\ 2v-1 & \text{si } \ell = 1 \text{ et } v \geq 1; \\ b_\ell^{v-1} - b_{\ell-1}^{v-1} & \text{sinon.} \end{cases}$$

Soit $v \geq 1$. Alors si $(m, k) \in \mathbb{N} \times \mathbb{Z}$,

$$2 \left[\binom{m}{k} + \binom{m}{k+1-2v} \right] = \sum_{\ell=1}^v b_{\ell}^v \left[\binom{m+\ell}{k} + \binom{m+\ell}{k+1+\ell-2v} \right]$$

et

$$\sum_{\ell=1}^v b_{\ell}^v = \begin{cases} 1 & \text{si } v = 1 ; \\ 2 & \text{si } v \geq 2. \end{cases}$$

2) Soit (c_{ℓ}^v) l'unique suite définie par

$$c_{\ell}^v = \begin{cases} 0 & \text{si } v < \ell \text{ ou } \ell < 1 ; \\ 2v & \text{si } \ell = 1 ; \\ c_{\ell}^{v-1} - c_{\ell-1}^{v-1} & \text{sinon.} \end{cases}$$

Soit $v \geq 1$. Alors si $(m, k) \in \mathbb{N} \times \mathbb{Z}$,

$$2 \left[\binom{m}{k} - \binom{m}{k-2v} \right] = \sum_{\ell=1}^v c_{\ell}^v \left[\binom{m+\ell}{k} - \binom{m+\ell}{k+\ell-2v} \right].$$

Démonstration – La preuve se fait par récurrence sur v . $\square$

LEMME 6.2.6

Soit $t \geq 1$, alors

$$\sum_{r=0}^{t-1} (-1)^r \binom{t+r}{2r} \binom{2r}{r} + \sum_{r=1}^t (-1)^{r+1} \binom{t+r-1}{2r-1} \binom{2r-1}{r} = (-1)^{t+1} \binom{2t}{t}$$

et

$$\begin{aligned} \sum_{r=0}^{t-1} (-1)^r \binom{t+r-1}{2r} \binom{2r}{r} + \sum_{r=1}^{t-1} (-1)^r \binom{t+r-1}{2r-1} \binom{2r-1}{r} \\ = (-1)^{t+1} \binom{2t-1}{t}. \end{aligned}$$

Démonstration – La première égalité résulte de

$$\sum_{r=0}^t (-1)^r \binom{t+r}{2r} \binom{2r}{r} = \sum_{r=0}^t (-1)^r \binom{t+r}{2r} \binom{2r}{r} \left[1 - \frac{t}{t+r} \right] = 0$$

grâce à [BMP86, 4.2.6.13]. La seconde égalité résulte de la première et de [BMP86, 4.2.5.71]. $\square$

6.3 Les équations de Manin

6.3.1 Périodes de formes modulaires

Propriétés de Γ

On considère Γ un sous-groupe de congruence de $SL(2, \mathbb{Z})$ contenant $-I$. On note $\mathcal{R}(\Gamma)$ l'ensemble fini $\Gamma \backslash SL(2, \mathbb{Z})$ et $\nu_0(\Gamma)$ son cardinal. Un élément de $\mathcal{R}(\Gamma)$ obtenu par projection canonique d'une matrice M de $SL(2, \mathbb{Z})$ sera noté $\overline{M}$. Si $M \in SL(2, \mathbb{Z})$, on note $\mathcal{R}^M(\Gamma)$ l'ensemble des éléments de $\mathcal{R}(\Gamma)$ invariants par multiplication à droite par M :

$$\mathcal{R}^M(\Gamma) = \{\overline{A} \in \mathcal{R}(\Gamma) ; \overline{AM} = \overline{A}\}.$$

Le cardinal de $\mathcal{R}^S(\Gamma)$ est donné par $\nu_2(\Gamma)$, le nombre de points elliptiques d'ordre 2 de Γ . Le cardinal de $\mathcal{R}^U(\Gamma)$ est donné par $\nu_3(\Gamma)$, le nombre de points elliptiques d'ordre 3 de Γ . On effectue la *décomposition de $\mathcal{R}(\Gamma)$ selon S* (respectivement U) : puisque

$$\mathcal{R}(\Gamma) \setminus \mathcal{R}^S(\Gamma) = \{\overline{M} \in \mathcal{R}(\Gamma) ; \overline{MS} \neq \overline{M}\}$$

on peut construire $\mathcal{R}^2(\Gamma)$ un ensemble maximal de classes $\overline{M}$ de $\mathcal{R}(\Gamma)$ tels que $\overline{M} \neq \overline{MS}$ de sorte que si $\overline{M}$ et $\overline{N}$ sont dans $\mathcal{R}^2(\Gamma)$ alors $\overline{M} \neq \overline{NS}$. On a alors la décomposition en union disjointe

$$\mathcal{R}(\Gamma) = \mathcal{R}^2(\Gamma) \sqcup \mathcal{R}^2(\Gamma)S \sqcup \mathcal{R}^S(\Gamma).$$

On a

$$\#\mathcal{R}^2(\Gamma) = \frac{\nu_0(\Gamma) - \nu_2(\Gamma)}{2}.$$

De même, on peut construire $\mathcal{R}^3(\Gamma)$ tel que

$$\mathcal{R}(\Gamma) = \mathcal{R}^3(\Gamma) \sqcup \mathcal{R}^3(\Gamma)U \sqcup \mathcal{R}^3(\Gamma)U^2 \sqcup \mathcal{R}^U(\Gamma) \quad (6.2)$$

avec

$$\#\mathcal{R}^3(\Gamma) = \frac{\nu_0(\Gamma) - \nu_3(\Gamma)}{3}.$$

Le groupe $SL(2, \mathbb{Z})$ agit sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} ; \Im z > 0\}$ par action homographique

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}$$

et cette action s'étend en action transitive sur $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. L'ensemble $\Gamma \backslash \mathbb{Q} \cup \{\infty\}$ est fini de cardinal $\nu_\infty(\Gamma)$ et ses éléments sont appelés *pointes* de Γ .

On définit une action de $SL(2, \mathbb{Z})$ sur l'ensemble des fonctions F de $\mathbb{C} \times \mathcal{R}(\Gamma)$ telles que pour tout $\overline{M} \in \mathcal{R}(\Gamma)$, $\lim_{y \rightarrow 0} y^{k-2} F(y^{-1}, \overline{M}) < \infty$: si $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ on pose

$$\begin{aligned} h.F & : \mathbb{C} \times \mathcal{R}(\Gamma) \rightarrow \mathbb{C} \\ (X, \overline{M}) & \mapsto (-cX + a)^{k-2} F(h^{-1}X, \overline{Mh}). \end{aligned}$$

Formes modulaires

Soit $2k$ un entier pair strictement positif et Γ un sous-groupe de congruence de $SL(2, \mathbb{Z})$. Le groupe $SL(2, \mathbb{Z})$ agit sur l'espace des fonctions holomorphes sur $\mathcal{H}$ grâce à l'action

$$f|_{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right).$$

On dit que f vérifie la condition de modularité sur Γ si pour toute matrice $M \in \Gamma$ on a $f|_M = f$. Soit $M \in SL(2, \mathbb{Z})$, on définit

$$u_M = \inf\{u \in \mathbb{N}^* ; T^u \in M^{-1}\Gamma M\}.$$

Si f vérifie la condition de modularité sur Γ alors $f|_M$ est périodique de période u_M . Elle admet un développement de Fourier de la forme

$$f|_M(z) = \sum_{n \in \mathbb{Z}} \widehat{f}_M(n) \exp\left(2i\pi \frac{n}{u_M} z\right) \quad (6.3)$$

pour $\Im z$ assez grand et par modularité, le coefficient $\widehat{f}_M(n)$ ne dépend que de $\overline{M}$. On dit que f est holomorphe aux pointes si pour toute $M \in SL(2, \mathbb{Z})$ et tout $n < 0$ on a $\widehat{f}_M(n) = 0$. Dans ce cas, f étant holomorphe sur $\mathcal{H}$, (6.3) converge normalement sur tout compact de $\mathcal{H}$. Si f est une fonction holomorphe vérifiant la condition de modularité, holomorphe aux pointes et vérifiant de plus $\widehat{f}_M(0) = 0$ pour toute sur Γ . Si $M \in SL(2, \mathbb{Z})$ et si f est parabolique on déduit du développement (6.3) et du fait que $f|_M$ vérifie la condition de modularité sur $M^{-1}\Gamma M$ qu'il existe une constante c telle que pour tout n strictement positif on a [Miy89, corollary 2.1.6]

$$|\widehat{f}_M(n)| \leq cn^k. \quad (6.4)$$

On en déduit l'existence, pour toute $M \in SL(2, \mathbb{Z})$, de constantes c et y_0 telles que si $y \geq y_0$ alors

$$|f|_M(iy)| \leq ce^{-2\pi y/u_M} \quad (6.5)$$

[Miy89, lemme 4.3.3]. Lorsque $M \in \Gamma$ on écrit $\widehat{f}(n)$ au lieu de $\widehat{f}_M(n)$. On note $S(2k, \Gamma)$ l'espace des formes paraboliques de poids $2k$ sur Γ . C'est un espace de dimension finie dont la dimension a été donnée en introduction (dans le cas où $-I$ est dans Γ).

Périodes

Si f est une forme de $S(2k, \Gamma)$ et si $M \in SL(2, \mathbb{Z})$, l'équation (6.5) permet de définir le polynôme de période de f et M par

$$\rho_M(f)(X) = -\frac{1}{(2k-2)!} \int_0^{+\infty} f|_M(z)(X-z)^{2k-2} dz.$$

Ce polynôme ne dépend que de la classe de M modulo Γ . Si $\mathbb{C}[X]_{2k-2}$ est l'espace des polynômes à coefficients complexes de degré inférieur ou égal à $2k-2$, on déduit des travaux de Skoruppa [Sko90, proposition 3] que le morphisme

$$\begin{aligned} \rho & : S(2k, m) \rightarrow \mathbb{C}[X]_{2k-2}^{\nu_0(\Gamma)} \\ f & \mapsto \{\rho_M(f)\}_{\overline{M} \in \mathcal{R}(\Gamma)} \end{aligned}$$

est injectif. Pour $f \in S(2k, \Gamma)$ on définit ensuite le morphisme

$$\begin{aligned} r_f & : \mathbb{C} \times \mathcal{R}(\Gamma) \rightarrow \mathbb{C} \\ (X, \overline{M}) & \mapsto \rho_M(f)(X). \end{aligned}$$

On déduit de la relation

$$M.r_f(X, \overline{A}) = -\frac{1}{(2k-2)!} \int_{M.0}^{M.\infty} f|_A(z)(X-z)^{2k-2} dz$$

vraie pour toute matrice $M \in SL(2, \mathbb{Z})$ les relations de Manin

$$(I + S).r_f = 0 \quad (6.6)$$

$$(I + U + U^2).r_f = 0. \quad (6.7)$$

REMARQUE 6.1 Le premier auteur [Mar01, appendice] a prouvé que ces relations « engendrent » toutes celles du même type au sens où ces deux relations sont équivalentes à la propriété : pour tout

$$W = \sum_M w_M M$$

de $\mathbb{Z}[SL(2, \mathbb{Z})]$ vérifiant

$$\sum_M w_M (M.\infty - M.0) = 0$$

on a

$$\left(\sum_M w_M M \right) . r_f = 0.$$

6.3.2 Fonctions L - Liens avec les périodes Soit f une forme de $S(2k, m)$ et M une matrice de $SL(2, \mathbb{Z})$. On définit la fonction L de $f|_M$ par la série

$$L(f|_M, s) = \sum_{n=1}^{+\infty} \widehat{f_M}(n) n^{-s}.$$

Grâce à (6.4) cette série converge pour $\Re s > k + 1$. La décroissance exponentielle (6.5) et la représentation intégrale

$$\left(\frac{2\pi}{u_M} \right)^{-s} \Gamma(s) L(f|_M, s) = \int_1^{+\infty} f|_M(it) t^s \frac{dt}{t} + (-1)^k \int_1^{+\infty} f|_{MS}(it) t^{-s+2k} \frac{dt}{t} \quad (6.8)$$

donnent un prolongement holomorphe de $L(f|_M, s)$ à $\mathbb{C}$. Pour la suite, il est plus aisé d'utiliser la fonction, elle aussi entière,

$$L^*(f|_M, s) = \left(\frac{u_M}{2i\pi} \right)^s \frac{1}{\Gamma(2k-s)} L(f|_M, s).$$

On traduit les relations de Manin (6.6) et (6.7) dans la

PROPOSITION 6.3.1

Soit $f \in S(2k, \Gamma)$ et $\overline{M} \in \mathcal{R}(\Gamma)$. Pour tout entier ℓ tel que $1 \leq \ell \leq 2k-1$ on a

$$L^*(f|_M, \ell) - (-1)^\ell L^*(f|_{MS}, 2k - \ell) = 0$$

et

$$\begin{aligned} L^*(f|_M, 2k - \ell) - (-1)^\ell \sum_{j=1}^{\ell} \binom{2k-1-j}{\ell-j} L^*(f|_{MU}, j) \\ - (-1)^\ell \sum_{j=\ell}^{2k-1} \binom{j-1}{\ell-1} L^*(f|_{MU^2}, j) = 0. \end{aligned}$$

REMARQUE 6.2 La première des deux relations n'est rien d'autre qu'un cas particulier de l'équation fonctionnelle de L^* qu'on déduit de (6.8).

Démonstration – Par développement du polynôme $(X - z)^{2k-2}$, utilisation du développement de Fourier (6.3) et de

$$\int_0^{+i\infty} z^\ell e^{2i\pi n z} dz = \ell! \left(\frac{i}{2\pi n} \right)^{\ell+1}$$

[BMP86, 2.3.3.2] on montre que pour tout $\overline{M} \in \mathcal{R}(\Gamma)$

$$\rho_M(f)(X) = \sum_{\ell=0}^{2k-2} L^*(f|_M, 2k-1-\ell) X^\ell. \quad (6.9)$$

On a

$$U.r_f(X, \overline{M}) = X^{2k-2} r_f\left(\frac{X-1}{X}, \overline{MU}\right)$$

et

$$U^2.r_f(X, \overline{M}) = (X-1)^{2k-2} r_f\left(\frac{-1}{X-1}, \overline{MU^2}\right)$$

de sorte que l'équation (6.7) donne

$$\rho_M(f)(X) + X^{2k-2} \rho_{MU}(f)\left(\frac{X-1}{X}\right) + (X-1)^{2k-2} \rho_{MU^2}(f)\left(\frac{-1}{X-1}\right) = 0.$$

Grâce à (6.9) on a alors la seconde relation de la proposition. On obtient de même la première relation à partir de (6.6) (voir aussi la remarque ci-dessus). $\square$

La proposition 6.3.1 affirme que $\{L(f|_M, \ell), \overline{M} \in \mathcal{R}(\Gamma), \ell \in [1, 2k-2]\}$ est solution du système

$$\begin{cases} x(M, \ell) - (-1)^\ell x_{MS}(2k-\ell) = 0 \\ x(M, 2k-\ell) - (-1)^\ell \sum_{j=1}^{\ell} \binom{2k-1-j}{\ell-j} x_{MU}(j) - (-1)^\ell \sum_{j=\ell}^{2k-1} \binom{j-1}{\ell-1} x_{MU^2}(j) = 0 \end{cases}$$

où les équations sont répétées pour chaque $\overline{M}$ de $\mathcal{R}(\Gamma)$ et chaque ℓ de $[1, 2k-2]$. Le but des paragraphes suivants est d'estimer le rang de ce système.

6.3.3 Base du système de Manin

Équations provenant de S

D'après la proposition 6.3.1, l'équation $(1+S).r_f = 0$ est équivalente au système d'équations

$$\{\{\ell M\} : L^*(f|_M, \ell) - (-1)^\ell L^*(f|_{MS}, 2k-\ell) = 0\} \overline{M \in \mathcal{R}(\Gamma)}_{1 \leq \ell \leq 2k-1}.$$

On appelle alors *équations provenant de S* les équations $\{\ell M\}$ données par

$$x_M(\ell) - (-1)^\ell x_{MS}(2k-\ell) = 0 \quad \{\ell M\}$$

Puisque $S^2 = -I \in \Gamma$, on a l'égalité $\{\ell M\} = (-1)^{\ell+1} \{(2k-\ell)MS\}$. Le système précédent est donc équivalent au système des $\nu_0(\Gamma)k$ équations $\{\ell M\}$ lorsque $\overline{M}$ parcourt $\mathcal{R}(\Gamma)$ et ℓ parcourt $[1, k]$. En fait, les seules relations de dépendance entre équations de ce nouveau système proviennent des équations $\{kM\}$. Le système des équations $\{kM\}$ lorsque $\overline{M}$ parcourt $\mathcal{R}(\Gamma)$ est engendré par

$$\frac{\nu_0(\Gamma) - (-1)^k \nu_2(\Gamma)}{2}$$

équations indépendantes : en effet, si $\overline{M} \neq \overline{MS}$ alors $\{kM\} = (-1)^{k+1} \{kMS\}$ et si $\overline{M} = \overline{MS}$, alors l'équation $\{kM\}$ est non triviale si et seulement si $(-1)^k = -1$. On en déduit le

LEMME 6.3.2

Le système d'équations

$$\{\{\ell M\} ; \overline{M} \in \mathcal{R}(\Gamma), \ell \in [1, 2k-1]\}$$

est de rang

$$\frac{2k-1}{2} \nu_0(\Gamma) - (-1)^k \frac{\nu_2(\Gamma)}{2}.$$

Il est équivalent au système d'équations indépendantes formé par la réunion des deux systèmes

$$\{\{\ell M\} ; \overline{M} \in \mathcal{R}(\Gamma), \ell \in [1, k-1]\}$$

et

$$\{\{kM\} ; \overline{M} \in \mathcal{R}^2(\Gamma) \cup \mathcal{R}^S(\Gamma)\} \text{ si } k \text{ est impair,}$$

$$\{\{kM\} ; \overline{M} \in \mathcal{R}^2(\Gamma)\} \text{ si } k \text{ est pair.}$$

Équations provenant de U

D'après la proposition 6.3.1, l'équation $(1 + U + U^2).r_f = 0$ est équivalente au système d'équations

$$\begin{aligned} L^*(f|_M, 2k-\ell) - (-1)^\ell \sum_{j=1}^{\ell} \binom{2k-1-j}{\ell-j} L^*(f|_{MU}, j) \\ - (-1)^\ell \sum_{j=\ell}^{2k-1} \binom{j-1}{\ell-1} L^*(f|_{MU^2}, j) = 0 \end{aligned}$$

où les équations sont répétées pour chaque $\overline{M}$ de $\mathcal{R}(\Gamma)$ et chaque ℓ de $[1, 2k-1]$. On appelle donc *équations provenant de U* les équations $[\ell M]$ données par

$$\begin{aligned} x_{MU}(2k-\ell) - (-1)^\ell \sum_{j=1}^{\ell} \binom{2k-1-j}{\ell-j} x_{MU^2}(j) \\ - (-1)^\ell \sum_{j=\ell}^{2k-1} \binom{j-1}{\ell-1} x_M(j) = 0. \quad [\ell M] \end{aligned}$$

On considère le système

$$(*) = \{[\ell M] ; \overline{M} \in \mathcal{R}(\Gamma), \ell \in [1, 2k-1]\}.$$

Il existe des relations de dépendance entre les équations de $(*)$. On le montre dans le

LEMME 6.3.3

Pour tout $1 \leq \ell \leq 2k-1$ et tout $\overline{M} \in \mathcal{R}(\Gamma)$ on a

$$[(2k-\ell)MU] = (-1)^{\ell+1} \sum_{j=2k-\ell}^{2k-1} \binom{j-1}{2k-\ell-1} [(2k-j)M]$$

et

$$[(2k-\ell)MU^2] = (-1)^{\ell+1} \sum_{j=1}^{2k-\ell} \binom{2k-1-j}{\ell-1} [(2k-j)M].$$

Démonstration – On calcule, par interversion de sommes

$$\begin{aligned} \sum_{j=2k-\ell}^{2k-1} \binom{j-1}{2k-\ell-1} [(2k-j)M] &= \sum_{t=2k-\ell}^{2k-1} \binom{t-1}{2k-\ell-1} x_{MU}(t) \\ &\quad - \sum_{t=1}^{\ell} x_{MU^2}(t) \sum_{j=2k-\ell}^{2k-t} (-1)^j \binom{2k-t-1}{j-1} \binom{j-1}{2k-\ell-1} \\ &\quad - \sum_{t=1}^{2k-1} x_M(t) \sum_{j=\max(2k-\ell, 2k-t)}^{2k-1} (-1)^j \binom{j-1}{2k-\ell-1} \binom{t-1}{2k-j-1}. \end{aligned}$$

On conclut grâce à l'égalité

$$\sum_{j=2k-\ell}^{2k-t} (-1)^j \binom{2k-t-1}{j-1} \binom{j-1}{2k-\ell-1} = (-1)^\ell \delta(t=\ell)$$

et au lemme 6.2.1 qui donne

$$\sum_{j=\max(2k-\ell, 2k-t)}^{2k-1} (-1)^j \binom{j-1}{2k-\ell-1} \binom{t-1}{2k-j-1} = -\binom{2k-1-t}{\ell-1}.$$

La seconde égalité se prouve de même. $\square$

Afin de réduire le système, on définit par récurrence les équations $[\ell M]'$, pour $0 \leq 2\ell + 1 \leq 2k$ par les formules

$$\begin{aligned} [2\ell M]' &= [2\ell M] + (k-\ell)[(2\ell-1)M]' - \sum_{t=1}^{\ell-1} \left[\binom{k-\ell+t}{2t} [(2\ell-2t)M]' \right. \\ &\quad \left. - \binom{k-\ell+t}{2t+1} [(2\ell-2t-1)M]' \right] \end{aligned}$$

et

$$\begin{aligned} [(2\ell+1)M]' &= [(2\ell+1)M] + \sum_{t=0}^{\ell-1} \left[\binom{k-\ell+t}{2t+1} [(2\ell-2t)M]' \right. \\ &\quad \left. - \binom{k-\ell+t}{2t+2} [(2\ell-2t-1)M]' \right]. \end{aligned}$$

On développe ces équations dans le

LEMME 6.3.4

On suppose $k \geq 3$. Soit $\overline{M} \in \mathcal{R}(\Gamma)$. Les équations $[\]'$ sont données par

$$\begin{aligned} - \sum_{t=1}^{2\ell} \binom{k-1+\ell-t}{2\ell-t} x_{MU^2}(t) + \sum_{t=1}^{2\ell} \binom{k-1+\ell-t}{2\ell-t} x_{MU}(2k-t) \\ + \sum_{t=1}^{2k-1} P_{2\ell-1}^k(t) x_M(t) = 0 \quad [2\ell M]' \end{aligned}$$

pour $2\ell \leq k$ et

$$\sum_{t=1}^{2\ell+1} \binom{k-1+\ell-t}{2\ell+1-t} x_{MU^2}(t) + \sum_{t=1}^{2\ell+1} \binom{k+\ell-t}{2\ell+1-t} x_{MU}(2k-t) \\ + \sum_{t=1}^{2k-1} P_{2\ell}^k(t) x_M(t) = 0 \quad [(2\ell+1)M]'$$

pour $2\ell+1 \leq k$.

Démonstration – Pour $\ell = 0$ et $\ell = 1$, on vérifie immédiatement que $[1M]'$ et $[2M]'$ sont données par les formules du lemme. On suppose que $[tM]'$ est donnée par le lemme pour tout $t < 2\ell$ et on montre que $[2\ell M]'$ et $[(2\ell+1)M]'$ sont données par le lemme. On calcule

$$\begin{aligned} & [2\ell M] + (k-\ell) \left[\sum_{t=1}^{2\ell-1} \binom{k-2+\ell-t}{2\ell-1-t} x_{MU^2}(t) + \sum_{t=1}^{2\ell-1} \binom{k-1+\ell-t}{2\ell-1-t} x_{MU}(2k-t) \right. \\ & \left. + \sum_{t=1}^{2k-1} P_{2\ell-2}^k(t) x_M(t) \right] - \sum_{j=1}^{\ell-1} \binom{k-\ell+j}{2j} \left[- \sum_{t=1}^{2\ell-2j} \binom{k-1+\ell-j-t}{2\ell-2j-t} x_{MU^2}(t) \right. \\ & \left. + \sum_{t=1}^{2\ell-2j} \binom{k-1+\ell-j-t}{2\ell-2j-t} x_{MU}(2k-t) + \sum_{t=1}^{2k-1} P_{2\ell-2j-1}^k(t) x_M(t) \right] + \sum_{j=1}^{\ell-1} \binom{k-\ell+j}{2j+1} \\ & \times \left[\sum_{t=1}^{2\ell-2j-1} \binom{k-2+\ell-j-t}{2\ell-1-2j-t} x_{MU^2}(t) + \sum_{t=1}^{2\ell-2j-1} \binom{k-1+\ell-j-t}{2\ell-1-2j-t} x_{MU}(2k-t) \right. \\ & \left. + \sum_{t=1}^{2k-1} P_{2\ell-2j-2}^k(t) x_M(t) \right] \end{aligned}$$

et on doit montrer que cette expression est la même que celle donnée pour $[2\ell M]'$ dans le lemme. Pour $2t \leq 2\ell - 4$, le coefficient de $x_{MU^2}(2t)$ est

$$\begin{aligned} & - \binom{k+\ell-2t-1}{2\ell-2t} - \binom{2k-2t-1}{2\ell-2t} + \sum_{j=0}^{\ell-t} \left[\binom{k-\ell+j}{2j} \binom{k-1+\ell-j-2t}{2\ell-2j-2t} \right. \\ & \left. + \binom{k-\ell+j}{2j+1} \binom{k-2+\ell-j-2t}{2\ell-2j-2t-1} \right] \end{aligned}$$

et vaut bien $-\binom{k+\ell-2t-1}{2\ell-2t}$ grâce au point 1 lemme 6.2.2. Pour $2t-1 \leq 2\ell-3$, le coefficient de $x_{MU^2}(2t-1)$ est

$$\begin{aligned} & - \binom{k+\ell-2t}{2\ell-2t+1} - \binom{2k-2t}{2\ell-2t+1} + \sum_{j=0}^{\ell-t} \left[\binom{k-\ell+j}{2j} \binom{k+\ell-j-2t}{2\ell-2j-2t+1} \right. \\ & \left. + \binom{k-\ell+j}{2j+1} \binom{k+\ell-j-2t-1}{2\ell-2j-2t} \right] \end{aligned}$$

et vaut bien $-\binom{k+\ell-2t}{2\ell-2t+1}$ grâce au point 3 du lemme 6.2.2.

Si $2t \leq 2\ell - 4$, le terme $x_{MU}(2k-2t)$ est

$$\begin{aligned} & \binom{k+\ell-2t-1}{2\ell-2t} + \sum_{j=0}^{\ell-t} \left[\binom{k-\ell+j}{2j+1} \binom{k-1+\ell-2t-j}{2\ell-2t-2j-1} \right. \\ & \left. - \binom{k-\ell+j}{2j} \binom{k-1+\ell-2t-j}{2\ell-2t-2j} \right] \end{aligned}$$

et vaut bien $\binom{k+\ell-2t-1}{2\ell-2t}$ grâce au point 1 du lemme 6.2.4. Si $2t-1 \leq 2\ell-3$, le terme $x_{MU}(2k-2t+1)$ est

$$\binom{k+\ell-2t}{2\ell-2t+1} + \sum_{j=0}^{\ell-t} \left[\binom{k-\ell+j}{2j+1} \binom{k+\ell-2t-j}{2\ell-2t-2j} - \binom{k-\ell+j}{2j} \binom{k+\ell-2t-j}{2\ell-2t-2j+1} \right]$$

et vaut bien $\binom{k+\ell-2t}{2\ell-2t+1}$ grâce au point 2 du lemme 6.2.4. Enfin, le coefficient de $x_M(t)$ est

$$- \binom{t-1}{2\ell-1} + (k-\ell)P_{2\ell-2}^k(t) - \sum_{j=1}^{\ell-1} \binom{k-\ell+j}{2j} P_{2\ell-2j-1}^k(t) + \sum_{j=1}^{\ell-1} \binom{k-\ell+j}{2j+1} P_{2\ell-2j-2}^k(t) = P_{2\ell-1}^k(t)$$

grâce au corollaire 6.2.3. Tous les cas exclus sont immédiats. Le résultat pour $[(2\ell+1)M]'$ se montre de même façon. $\square$

On définit les équations supplémentaires

$$(E)_M = [(2q+1)M]' + [2qMU]', \quad \text{lorsque } k = 3q+1, q \in \mathbb{N}.$$

Le pendant, pour U du lemme 6.3.2 obtenu pour S est le

LEMME 6.3.5

Soit $k \geq 3$. Le système d'équations

$$\{[\ell M]; \overline{M} \in \mathcal{R}(\Gamma), \ell \in [1, 2k-1]\}$$

est de rang

$$\frac{2k-1}{3}\nu_0(\Gamma) + \begin{cases} 0 & \text{si } k \equiv 2 \pmod{3}; \\ \frac{2}{3}\nu_3(\Gamma) & \text{si } k \equiv 1 \pmod{3}; \\ -\frac{2}{3}\nu_3(\Gamma) & \text{si } k \equiv 0 \pmod{3}. \end{cases}$$

Il est équivalent au système d'équations indépendantes

$$\left\{ [\ell M]', \overline{M} \in \mathcal{R}(\Gamma), 1 \leq \ell \leq \frac{2k-1}{3} \right\}$$

lorsque $k \equiv 2 \pmod{3}$,

$$\left\{ [\ell M]', \overline{M} \in \mathcal{R}(\Gamma), 1 \leq \ell \leq \frac{2k-2}{3} \right\} \cup \{(E)_M, \overline{M} \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^U(\Gamma)\}$$

lorsque $k \equiv 1 \pmod{3}$ puis

$$\left\{ [\ell M]', \overline{M} \in \mathcal{R}(\Gamma), 1 \leq \ell \leq \frac{2k}{3} - 1 \right\} \cup \left\{ \left[\frac{2k}{3} M \right]', \overline{M} \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^3(\Gamma)U \right\}$$

lorsque $k \equiv 0 \pmod{3}$.

REMARQUE 6.3 La preuve se lit plus facilement si on se contente de prouver que le nombre d'équations indépendantes de (*) est *au moins* donné par le lemme.

Démonstration – Fixons $\overline{M} \in \mathcal{R}(\Gamma)$. On note $(*)_M$ le système

$$(*)_M = \{[\ell M], [\ell MU], [\ell MU^2]; \ell \in [1, 2k-1]\}.$$

Grâce au lemme 6.3.3, le nombre d'équations indépendantes de ce système est inférieur ou égal à $2k-1$. Par construction, quelque soit $r \in [1, k]$, le système engendré par les équations $[\ell M]', \overline{M}$ fixé, ℓ parcourant $[1, r]$ est équivalent au système engendré par les équations $[\ell M], \overline{M}$ fixé, ℓ parcourant $[1, r]$. Soit $n \geq 0$ tel que $2n+1 \leq k$ et $\overline{M} \neq \overline{MU}$. Dans les équations du lemme 6.3.4, la variable $x_M(k+n)$ apparaît (avec un coefficient non nul) dans $[1M]', [2M]', \dots, [2nM]'$ et dans aucune des équations $[\ell M]'$ avec $\ell > 2n$. Si d'autre part $n \in [0, k/3[$, la variable $x_M(k+n)$ n'apparaît ni dans les équations $[1MU]', \dots, [2nMU]'$ ni dans les équations $[1MU^2]', \dots, [2nMU^2]'$. De même, la variable $x_M(k-n)$ apparaît dans $[1M]', \dots, [(2n+1)M]'$ et, si d'autre part $n \in [0, (k-1)/3[$, elle n'apparaît ni dans les équations $[1MU]', \dots, [(2n+1)MU]'$ ni dans les équations $[1MU^2]', \dots, [(2n+1)MU^2]'$. On en déduit que si $L = \lfloor (2k-1)/3 \rfloor$ alors les équations $[\ell M]', [\ell MU]', [\ell MU^2]'$ lorsque ℓ parcourt $[1, L]$ sont indépendantes. Finalement, si $\overline{M} \neq \overline{MU}$, le nombre d'équations indépendantes de $(*)_M$ appartient à $[3\lfloor (2k-1)/3 \rfloor, 2k-1]$. Si $\overline{M} = \overline{MU}$, le même raisonnement montre que les équations $[\ell M]', 1 \leq \ell \leq \lfloor (2k-1)/3 \rfloor$ sont linéairement indépendantes. Notons S_M l'ensemble des équations linéairement indépendantes

$$S_M = \{[\ell M]', [\ell MU]', [\ell MU^2]', 1 \leq \ell \leq \lfloor \frac{2k-1}{3} \rfloor\}.$$

1) Soit $k \equiv 2 \pmod{3}$. Si $\overline{M} \neq \overline{MU}$, le système $(*)_M$ est de rang $2k-1$ et S_M est un système ét de $2k-1$ équations indépendantes. Si $\overline{M} = \overline{MU}$, le système $(*)_M$ est le même que pour un représentant $\overline{M} \neq \overline{MU}$ mais $x_M = x_{MU} = x_{MU^2}$. Ainsi, les calculs formels précédents impliquent que toute équation $[\ell M]'$ avec $\ell > \lfloor (2k-1)/3 \rfloor$ est combinaison linéaire des équations $[tM]', [tMU]', [tMU^2]'$ avec $t \leq \lfloor (2k-1)/3 \rfloor$, mais $[tM]' = [tMU]' = [tMU^2]'$. La décomposition (6.2) implique alors que le nombre d'équations indépendantes du système $(*)_M$ est

$$\nu_3(\Gamma) \frac{2k-1}{3} + \frac{2k-1}{3} [\nu_0(\Gamma) - \nu_3(\Gamma)] = \frac{2k-1}{3} \nu_0(\Gamma)$$

et une base de ce système est $[\ell M]', \overline{M} \in \mathcal{R}(\Gamma), 1 \leq \ell \leq \frac{2k-1}{3}$.

2) Si $k \equiv 1 \pmod{3}$, on a $3\lfloor \frac{2k-1}{3} \rfloor = 2k-2$. Posons $k = 3q+1$. Si $\overline{M} \neq \overline{MU}$, le système $(*)_M$ est engendré par les $[\ell M]', [\ell MU]', [\ell MU^2]', 1 \leq \ell \leq \lfloor \frac{2k-1}{3} \rfloor$ et éventuellement une autre équation. D'après le lemme 6.3.4, et les équations (6.1a) et (6.1b), $(E)_M$ se récrit

$$\begin{aligned} \sum_{j=1}^{2q+1} \binom{4q-j}{2q-1} [x_M(j) + x_{MU}(j) + x_{MU^2}(j)] \\ + \sum_{j=4q+2}^{6q+1} \binom{j-2q-2}{2q} [x_M(j) + x_{MU}(j) + x_{MU^2}(j)] = 0. \quad (E)_M \end{aligned}$$

Cette équation ne comportant aucune valeur $x_M(j)$ aux points $j, 2q+2 \leq j \leq 4q+1$, elle n'est pas combinaison linéaire des équations de S_M , ce qui montre que $S_M \cup (E)_M$ est une base d'équations engendrant $(*)_M$ qui est de rang $2k-1$.

Pour $\overline{M} = \overline{MU}$, l'équation $(E)_M$ est non triviale, donc les équations $[\ell M]', 1 \leq \ell \leq 2q$, $(E)_M$ sont linéairement indépendantes et engendrent $(*)_M$.

D'après la décomposition (6.2) le nombre d'équations indépendantes du système est

$$(2q+1)\nu_3(\Gamma) + (6q+1) \frac{\nu_0(\Gamma) - \nu_3(\Gamma)}{3} = \frac{2k-1}{3} \nu_0(\Gamma) + \frac{2\nu_3(\Gamma)}{3}$$

et une base d'équations de $(*)$ est $\{[\ell M]', \overline{M} \in \mathcal{R}(\Gamma)m, 1 \leq \ell \leq \frac{2k-2}{3}\} \cup \{(E)_M, \overline{M} \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^U(\Gamma)\}$.

3) Si $k \equiv 0 \pmod{3}$, posons $k = 3q$. On a $3 \lfloor (2k-1)/3 \rfloor = 2k-3$. Supposons que $\overline{M} \neq \overline{MU}$, le système $(*)_M$ est engendré par les équations $[\ell M]', [\ell MU]', [\ell MU^2]'$ lorsque $1 \leq \ell \leq 2q-1$ et éventuellement deux autres équations. Considérons l'équation $[2qM]'$, grâce aux valeurs des polynômes P_t^k , cette équation s'écrit :

$$\sum_{j=1}^{2q} \binom{4q-1-j}{2q-1} [x_M(j) - x_{MU^2}(j)] + \sum_{j=4q}^{6q-1} \binom{j-2q-1}{2q-1} [x_{MU}(j) - x_M(j)] = 0. \quad [2qM]'$$

Les équations $[2qM]'$ et $[2qMU]'$ ne comportent aucune variable $x_M(j)$ avec $2q+1 \leq j \leq 4q-1$, et ne sont pas multiples l'une de l'autre, donc l'ensemble $S_M \cup \{[2qM]', [2qMU]'\}$ est formé de $2k-1$ équations linéairement indépendantes, elles forment donc une base de $(*)_M$. Si $\overline{M} \neq \overline{MU}$, l'équation $[2qM]'$ est triviale, on en déduit que l'ensemble des équations $[\ell M]', 1 \leq \ell \leq 2q-1$ est une base d'équations de $(*)_M$. Finalement, d'après la décomposition (6.2) le nombre d'équations indépendantes du système est

$$(2q-1)\nu_3(\Gamma) + (6q-1)\frac{\nu_0(\Gamma) - \nu_3(\Gamma)}{3} = \frac{2k-1}{3}\nu_0(\Gamma) - \frac{2\nu_3(\Gamma)}{3},$$

une base de $(*)$ est donnée par $\{[\ell M]', \overline{M} \in \mathcal{R}(\Gamma), 1 \leq \ell \leq 2q-1\} \cup \{[2qM]', \overline{M} \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^3(\Gamma)U\}$.

□

6.4 Caractérisation par les valeurs de fonctions L

Au paragraphe précédent, on a déterminé le nombre d'équations indépendantes, ainsi qu'une base de ces équations, provenant d'une part de S , et d'autre part de U . On va montrer maintenant que toutes ces équations sont linéairement indépendantes.

On a vu qu'un ensemble générateur des équations provenant de S est donné par les $\{\ell M\}$, lorsque ℓ parcourt $[1, k]$ et $\overline{M}$ parcourt $\mathcal{R}(\Gamma)$. Posons dans la suite $r_k = \lfloor \frac{2k-1}{3} \rfloor$. On a vu qu'un ensemble générateur des équations provenant de U est donné par les équations $[\ell M]'$ pour ℓ parcourant $[1, r_k]$ et $\overline{M}$ parcourt $\mathcal{R}(\Gamma)$, auxquelles on ajoute les équations $(E)_M$, $\overline{M} \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^U(\Gamma)$ si $3|k-1$ et les équations $[(r_k+1)M]', \overline{M} \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^3(\Gamma)U$ si $3|k$.

Par l'absurde, on suppose avoir une relation de dépendance

$$\begin{aligned} \sum_{M \in \mathcal{R}(\Gamma)} \sum_{t=1}^k s_M(t) [x_M(t) + (-1)^{t-1} x_{MS}(2k-t)] &= \sum_{M \in \mathcal{R}(\Gamma)} \sum_{t=1}^{r_k} u_M(t) [tM]' \\ &+ \delta(3|k-1) \sum_{M \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^U(\Gamma)} v_M(r_k+1) (E)_M \\ &+ \delta(3|k) \sum_{M \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^3(\Gamma)U} w_M(r_k+1) [(r_k+1)M]'. \end{aligned} \quad (6.10)$$

D'après le lemme 6.3.2, on suppose que

$$\text{si } k \text{ est pair, } s_M(k) = 0 \text{ si } M \in \mathcal{R}^2(\Gamma)S \sqcup \mathcal{R}^S(\Gamma) \quad (6.11a)$$

et

$$\text{si } k \text{ est impair, } s_M(k) = 0 \text{ si } M \in \mathcal{R}^2(\Gamma)S. \quad (6.11b)$$

On définit (cela sera justifié par la preuve du lemme 6.4.1) si $3|k-1$,

$$u_M(r_k + 1) = \begin{cases} v_M(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^3(\Gamma); \\ v_{MU}(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^3(\Gamma)U^2; \\ v_{MU^2}(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^3(\Gamma)U; \\ 3v_M(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^U(\Gamma). \end{cases}$$

On a alors

$$u_M(r_k + 1) = u_{MU}(r_k + 1) = u_{MU^2}(r_k + 1) \text{ si } k \equiv 1 \pmod{3}. \quad (6.12a)$$

On définit ensuite, si 3 divise k ,

$$u_M(r_k + 1) = \frac{1}{3} \begin{cases} 2w_M(r_k + 1) - w_{MU}(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^3(\Gamma); \\ 2w_M(r_k + 1) - w_{MU^2}(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^3(\Gamma)U; \\ -w_{MU}(r_k + 1) - w_{MU^2}(r_k + 1) & \text{si } \overline{M} \in \mathcal{R}^3(\Gamma)U^2; \\ 0 & \text{si } \overline{M} \in \mathcal{R}^U(\Gamma). \end{cases}$$

On a alors, pour tout $\overline{M} \in \mathcal{R}(\Gamma)$,

$$u_M(r_k + 1) + u_{MU}(r_k + 1) + u_{MU^2}(r_k + 1) = 0 \text{ si } k \equiv 0 \pmod{3}. \quad (6.12b)$$

6.4.1 Mise en équation du système

LEMME 6.4.1

On définit, pour tout $j \in [1, 2k-1]$,

$$\begin{aligned} \alpha_M(j) = & \sum_{t=1}^{r_k/2} \left[u_M(2t)P_{2t-1}^k(j) + u_{MU^2}(2t) \binom{t+j-k-1}{2t+j-2k} \right. \\ & \left. - u_{MU}(2t) \binom{t-j+k-1}{2t-j} \right] \\ & + \sum_{t=0}^{(r_k-1)/2} \left[u_M(2t+1)P_{2t}^k(j) + u_{MU^2}(2t+1) \binom{t+j-k}{2t+j-2k+1} \right. \\ & \left. + u_{MU}(2t+1) \binom{t-j+k-1}{2t-j+1} \right] \\ & + \delta(3|k-1)u_M(r_k+1) \left[\binom{2r_k-j}{r_k-1} + \binom{j-r_k-2}{r_k} \right] \\ & + \delta(3|k) \left\{ \binom{2r_k+1-j}{r_k} [u_M(r_k+1) - u_{MU}(r_k+1)] \right. \\ & \left. + \binom{j-r_k-2}{r_k} [u_{MU^2}(r_k+1) - u_M(r_k+1)] \right\} \end{aligned}$$

et

$$\beta_M(j) = \delta(j \leq k)s_M(j) - (-1)^j \delta(j \geq k)s_{MS}(2k-j).$$

Alors, l'équation (6.10) conduit à $\alpha_M(j) = \beta_M(j)$.

Démonstration –

On a

$$\begin{aligned} \sum_{t=1}^{r_k/2} u_M(2t)[2tM]' &= - \sum_{j=1}^{2k-1} x_{MU^2}(j) \sum_{t=1}^{r_k/2} \binom{k-1+t-j}{2t-j} u_M(2t) \\ &\quad + \sum_{j=1}^{2k-1} x_{MU}(j) \sum_{t=1}^{r_k/2} \binom{-k-1+t+j}{-2k+2t+j} u_M(2t) \\ &\quad + \sum_{j=1}^{2k-1} x_M(j) \sum_{t=1}^{r_k/2} P_{2t-1}^k(j) u_M(2t). \end{aligned}$$

Ainsi

$$\begin{aligned} \sum_{M \in \mathcal{R}(\Gamma)} \sum_{t=1}^{r_k/2} u_M(2t)[2tM]' &= \\ \sum_{M \in \mathcal{R}(\Gamma)} \sum_{j=1}^{2k-1} x_M(j) \sum_{t=1}^{r_k/2} &\left[- \binom{k-1+t-j}{2t-j} u_{MU}(2t) \right. \\ &\quad \left. + \binom{-k-1+t+j}{-2k+2t+j} u_{MU^2}(2t) + P_{2t-1}^k(j) u_M(2t) \right]. \quad (6.13) \end{aligned}$$

Puis

$$\begin{aligned} \sum_{t=0}^{(r_k-1)/2} u_M(2t+1)[(2t+1)M]' &= \\ \sum_{j=1}^{2k-1} x_{MU^2}(j) \sum_{t=0}^{(r_k-1)/2} &\binom{k-1+t-j}{2t+1-j} u_M(2t+1) \\ + \sum_{j=1}^{2k-1} x_{MU}(j) \sum_{t=0}^{(r_k-1)/2} &\binom{-k+t+j}{-2k+1+2t+j} u_M(2t+1) \\ &+ \sum_{j=1}^{2k-1} x_M(j) \sum_{t=0}^{(r_k-1)/2} P_{2t}^k(j) u_M(2t+1). \end{aligned}$$

Ainsi

$$\begin{aligned} \sum_{M \in \mathcal{R}(\Gamma)} \sum_{t=0}^{(r_k-1)/2} u_M(2t+1)[(2t+1)M]' &= \\ \sum_{M \in \mathcal{R}(\Gamma)} \sum_{j=1}^{2k-1} x_M(j) \sum_{t=0}^{(r_k-1)/2} &\left[\binom{k-1+t-j}{2t+1-j} u_{MU}(2t+1) \right. \\ &\quad \left. + \binom{-k+t+j}{-2k+1+2t+j} u_{MU^2}(2t+1) + P_{2t}^k(j) u_M(2t+1) \right]. \quad (6.14) \end{aligned}$$

Si $k \equiv 1 \pmod{3}$, on a également

$$\begin{aligned} \sum_{M \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^U(\Gamma)} v_M(r_k+1)(E)_M &= \\ \sum_{M \in \mathcal{R}(\Gamma)} \sum_{j=1}^{2k-1} x_M(j) u_M(r_k+1) &\left[\binom{2r_k-j}{r_k-1} + \binom{j-r_k-2}{r_k} \right] \quad (6.15) \end{aligned}$$

et si $k \equiv 0 \pmod{3}$, on a

$$\begin{aligned} \sum_{M \in \mathcal{R}^3(\Gamma) \cup \mathcal{R}^3(\Gamma)U} w_M(r_k + 1)[(r_k + 1)M]' = \\ \sum_{M \in \mathcal{R}(\Gamma)} \sum_{j=1}^{2k-1} x_M(j) \left[\binom{2r_k + 1 - j}{r_k} [u_M(r_k + 1) - u_{MU}(r_k + 1)] \right. \\ \left. + \delta(2k - j \leq r_k + 1) \binom{j - r_k - 2}{r_k} [u_{MU^2}(r_k + 1) - u_M(r_k + 1)] \right] \quad (6.16) \end{aligned}$$

Finalement, les équations (6.13) à (6.16) montrent que le terme de droite de l'équation (6.10) est égal à

$$\sum_{M \in \mathcal{R}(\Gamma)} \sum_{j=1}^{2k-1} \alpha_M(j) x_M(j). \quad (6.17)$$

Enfin

$$\begin{aligned} \sum_{M \in \mathcal{R}(\Gamma)} \sum_{t=1}^k s_M(t) [x_M(t) + (-1)^{t-1} x_{MS}(2k - t)] = \\ \sum_{M \in \mathcal{R}(\Gamma)} \sum_{j=1}^{2k-1} x_M(j) [\delta(j \leq k) s_M(j) - (-1)^j \delta(j \geq k) s_{MS}(2k - j)]. \quad (6.18) \end{aligned}$$

L'égalisation de (6.17) et (6.18) donne le résultat. $\square$

LEMME 6.4.2

Soit $j < k$, on a

$$\begin{aligned} s_M(j) \mp (-1)^j s_{MUS}(j) = \\ \sum_{t=1}^{r_k/2} \left[\binom{k+t-j-1}{2t-1} \pm \binom{k+t-j-1}{2t-j} \right] u_M(2t) \\ + \sum_{t=0}^{(r_k-1)/2} \left[\binom{k+t-j}{2t} \pm \binom{k+t-j}{2t+1-j} \right] u_M(2t+1) \\ - \sum_{t=1}^{r_k/2} \left[\pm \binom{k+t-j-1}{2t-1} + \binom{k+t-j-1}{2t-j} \right] u_{MU}(2t) \\ + \sum_{t=0}^{(r_k-1)/2} \left[\pm \binom{k+t-j-1}{2t} + \binom{k+t-j-1}{2t+1-j} \right] u_{MU}(2t+1) \\ + \delta(3|k-1) \left[\binom{2r_k-j}{r_k-1} u_M(r_k+1) \pm \binom{2r_k-j}{r_k-j} u_{MU}(r_k+1) \right] \\ + 2\delta(3|k)\delta(\mp = -) \binom{2r_k+1-j}{r_k} [u_M(r_k+1) - u_{MU}(r_k+1)]. \end{aligned}$$

Démonstration – Puisque $j < k$, le lemme 6.4.1 conduit à

$$\begin{aligned} s_M(j) &= \sum_{t=1}^{r_k/2} \left[u_M(2t) P_{2t-1}^k(j) - u_{MU}(2t) \binom{t-j+k-1}{2t-j} \right] \\ &\quad + \sum_{t=0}^{(r_k-1)/2} \left[u_M(2t+1) P_{2t}^k(j) + u_{MU}(2t+1) \binom{t-j+k-1}{2t+1-j} \right] \\ &\quad + \delta(3|k-1) u_M(r_k+1) \binom{2r_k-j}{r_k-1} + \delta(3|k) \binom{2r_k+1-j}{r_k} [u_M(r_k+1) - u_{MU}(r_k+1)]. \end{aligned}$$

On a aussi $\beta_{MU}(2k-j) = \alpha_{MU}(2k-j)$ et puisque $2k-j > k$ on en déduit

$$\begin{aligned} -(-1)^j s_{MUS}(j) &= \sum_{t=1}^{r_k/2} \left[u_M(2t) \binom{t+k-j-1}{2t-j} + u_{MU}(2t) P_{2t-1}^k(2k-j) \right] \\ &\quad + \sum_{t=0}^{(r_k-1)/2} \left[u_M(2t+1) \binom{k+t-j}{2t+1-j} + u_{MU}(2t+1) P_{2t}^k(2k-j) \right] \\ &\quad + \delta(3|k-1) u_{MU}(r_k+1) \binom{2k-j-r_k-2}{r_k} \\ &\quad + \delta(3|k) \binom{2k-j-r_k-2}{r_k} [u_M(r_k+1) - u_{MU}(r_k+1)]. \end{aligned}$$

On conclut grâce aux égalités (6.1). $\square$

LEMME 6.4.3

Soit $2v < k$, (b_ℓ^v) et (c_ℓ^v) les suites définies dans le lemme 6.2.5. On a

$$\sum_{j=v}^{2v-1} \frac{b_{2v-j}^v}{2} [s_M(j) - (-1)^j s_{MUS}(j)] = s_M(2v) - s_{MUS}(2v)$$

et

$$\sum_{j=v+1}^{2v} \frac{c_{2v+1-j}^v}{2} [s_M(j) + (-1)^j s_{MUS}(j)] = s_M(2v+1) - s_{MUS}(2v+1).$$

Démonstration – Cela résulte du lemme 6.4.2, d'une interversion des sommes et du lemme 6.2.5. On utilise aussi (6.12a). $\square$

6.4.2 Résolution

LEMME 6.4.4

Soit $(a_M)_{M \in \mathcal{R}(\Gamma)}$ et $(b_M)_{M \in \mathcal{R}(\Gamma)}$ des suites à valeurs complexes. Si pour tout $\overline{M} \in \mathcal{R}(\Gamma)$, on a :

- 1) $a_{MUS} = a_M$;
- 2) $a_M = b_{MUS} - b_M$

alors $a_M = 0$ pour tout $\overline{M} \in \mathcal{R}(\Gamma)$.

Démonstration – Puisque Γ est d'indice fini dans $SL(2, \mathbb{Z})$ on peut poser $v_M = \inf\{\ell \in \mathbb{N}^* ; \overline{M}(US)^\ell = \overline{M}\}$. On a

$$0 = b_{M(US)^{v_M}} - b_M = \sum_{i=0}^{v_M-1} [b_{M(US)^{i+1}} - b_{M(US)^i}] = v_M a_M$$

d'où $a_M = 0$. $\square$

De ce lemme, on déduit le

LEMME 6.4.5

Pour tout $\overline{M} \in \mathcal{R}(\Gamma)$ et tout $j \in [1, k-2]$ on a $s_M(j) = 0$ et $s_{MUS}(k-1) = s_M(k-1)$.

Démonstration – On raisonne par récurrence. Pour $j = 1$, le lemme 6.4.2 montre que pour tout $\overline{M} \in \mathcal{R}(\Gamma)$, $s_M(1) - s_{MUS}(1) = 0$, et le lemme 6.4.3 montre que $s_M(2) - s_{MUS}(2) = [s_M(1) + s_{MUS}(1)]/2$, donc $s_M(1) = s_M(2) - s_{MUS}(2)$. D'après le lemme 6.4.4, on a $s_M(1) = 0$ et donc $s_M(2) = s_{MUS}(2)$ pour tout $\overline{M} \in \mathcal{R}(\Gamma)$. Soit $j < k-2$, et supposons que pour tout $\overline{M} \in \mathcal{R}(\Gamma)$, on a $s_M(\ell) = 0$ pour tout $1 \leq \ell \leq j-1$ et $s_M(j) = s_{MUS}(j)$. Le lemme 6.4.3 et l'hypothèse de récurrence donnent

$$s_M(j+1) - s_{MUS}(j+1) = d_j[s_M(j) + s_{MUS}(j)] = 2d_js_M(j)$$

où d_j est une constante non nulle dépendant de j . Le lemme 6.4.4 montre alors que $s_M(j) = 0$ pour tout $\overline{M} \in \mathcal{R}(\Gamma)$, et que $s_M(j+1) = s_{MUS}(j+1)$, ce qui démontre le lemme. $\square$

LEMME 6.4.6

Si k est pair,

$$u_M(1) - u_{MUS}(1) = u_M(1) + u_{MU}(1) = \sum_{j=k/2}^{k-1} \frac{b^{k/2}}{2} [s_M(j) - (-1)^j s_{MUS}(j)].$$

Si k est impair,

$$\begin{aligned} u_M(1) - u_{MUS}(1) &= u_M(1) - u_{MU}(1) \\ &= \sum_{j=(k+1)/2}^{k-1} \frac{c^{(k-1)/2}}{2} [s_M(j) + (-1)^j s_{MUS}(j)]. \end{aligned}$$

Démonstration – Grâce au lemme 6.4.1 pour $j = k$ on a

$$u_M(1) = s_M(k) - (-1)^k s_{MS}(k).$$

Cette égalité conduit à $u_M(1) = (-1)^{k-1} u_{MS}(1)$ et on obtient les égalités de gauche du lemme 6.4.6. Les deux égalités de droite se démontrent en partant des termes de somme, en utilisant le lemme 6.4.2, en intervertissant les sommes et en utilisant le lemme 6.2.5. $\square$

D'après les lemmes 6.4.5 et 6.4.4, on en déduit que

$$s_M(k-1) = 0, \quad \forall \overline{M} \in \mathcal{R}(\Gamma) \quad (6.19)$$

puis que

$$u_M(1) = u_{MUS}(1). \quad (6.20)$$

De plus, le lemme 6.4.1 pour $j = k$ donne

$$s_M(k) - (-1)^k s_{MS}(k) = u_M(1). \quad (6.21)$$

Si k est pair, on déduit de (6.21) que, pour tout $\overline{M} \in \mathcal{R}(\Gamma)$ on a $u_M(1) = -u_{MS}(1)$, ce qui équivaut à

$$u_{MU}(1) = -u_{MUS}(1), \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.22)$$

Par comparaison de (6.20) et (6.22) on obtient

$$u_M(1) = -u_{MU}(1), \quad \forall \overline{M} \in \mathcal{R}(\Gamma).$$

Cette équation conduit à

$$u_M(1) = -u_{MU^3}(1), \quad \forall \overline{M} \in \mathcal{R}(\Gamma)$$

soit, puisque $U^3 = I$, à

$$u_M(1) = 0, \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.23)$$

Compte-tenu de (6.23), l'équation (6.21) devient

$$s_M(k) = s_{MS}(k), \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.24)$$

On déduit de l'équations (6.24) reportée dans l'équation (6.11) que

$$s_M(k) = 0, \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.25)$$

Ainsi, grâce au lemme 6.4.5, à (6.19) et (6.25) on a $s_M(\ell) = 0$ pour tout $\overline{M} \in \mathcal{R}(\Gamma)$ et $\ell \in [1, 3q + 2]$. On en déduit qu'il n'y a pas de relation de dépendance linéaire faisant intervenir à la fois des équations provenant de S et de U . Cela achève la preuve du théorème lorsque k est pair.

Si k est impair, on déduit de (6.21) l'équation

$$u_M(1) = u_{MS}(1) \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.26)$$

Puisque S et US engendrent $SL(2, \mathbb{Z})$, on déduit de (6.26) et de (6.20) qu'il existe une constante $u(1)$ telle que

$$u_M(1) = u(1) \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.27)$$

Avec les notations du lemme 6.4.1, on déduit du lemme 6.4.5 et de (6.19) que $\alpha_M(j) = 0$ pour tout $j \in [1, k - 1]$. Par définition, on en déduit que pour tout $j \in [r_k + 1, 2k - r_k - 1] \setminus \{k\}$ et pour tout $\overline{M} \in \mathcal{R}(\Gamma)$, on a

$$\begin{aligned} \sum_{\ell=1}^{r_k} u_M(\ell) P_{\ell-1}^k(j) + \delta(3|k-1)\delta(j=r_k+1)u_M(r_k+1) \\ + \delta(3|k)\delta(j=r_k+1)[u_M(r_k+1) - u_{MU}(r_k+1)] \\ + \delta(3|k)\delta(j=2k-r_k-1)[u_{MU^2}(2k-r_k-1) - u_M(2k-r_k-1)] = 0. \quad (A_j) \end{aligned}$$

On suppose, en plus de k impair, que 3 ne divise pas k (ce dernier cas, légèrement différent, est traité ensuite). Pour $t \in [1, k - r_k - 1]$, l'équivalence $P_{\ell-1}^k(k+t) = 0 \Leftrightarrow \ell \geq 2t+1$ (*resp.* $P_{\ell-1}^k(k-t) = 0 \Leftrightarrow \ell \geq 2t+2$) permet de transformer l'équation (A_{k+t}) (*resp.* (A_{k-t})) en les relations de récurrence

$$\begin{cases} u_M(2t) &= \sum_{r=0}^{t-1} u_M(2r+1) \binom{t+r-1}{2r} - \sum_{r=1}^{t-1} u_M(2r) \binom{t+r-1}{2r-1} \\ -u_M(2t+1) &= \sum_{r=0}^{t-1} u_M(2r+1) \binom{t+r}{2r} + \sum_{r=1}^t u_M(2r) \binom{t+r-1}{2r-1} \end{cases} \quad (6.28)$$

Par récurrence, on déduit alors de (6.27) qu'il existe pour tout $\ell \in [1, 2k - 2r_k - 1]$ une constante $u(\ell)$ telle que

$$u_M(\ell) = u(\ell), \quad \forall \overline{M} \in \mathcal{R}(\Gamma). \quad (6.29)$$

Grâce au lemme 6.2.6 on vérifie par récurrence que

$$\begin{cases} u(2t) &= (-1)^{t+1} \binom{2t-1}{t} u(1) \\ u(2t+1) &= (-1)^t \binom{2t}{t} u(1) \end{cases} \quad (6.30)$$

Toujours avec les notations du lemme 6.4.1, l'égalité $\alpha_M(2k - r_k) = 0$ s'écrit alors

$$\begin{aligned} & \left[(-1)^k \binom{r_k - 1}{k - r_k - 1} + \sum_{r=1}^{k-r_k-1} (-1)^r \binom{2r-1}{r} \binom{k-r_k-1+r}{2r-1} \right. \\ & \quad \left. + \sum_{r=0}^{k-r_k-1} (-1)^r \binom{k-r_k-1+r}{2r} \binom{2r}{r} \right] u(1) = 0. \end{aligned}$$

Grâce au lemme 6.2.6, cette équation se réécrit

$$\begin{cases} \left[(-1)^q \binom{2q}{q} + (-1)^q \binom{2q+1}{q} \right] u(1) = 0 & \text{si } k = 3q + 2; \\ \left[(-1)^q \binom{2q+1}{q} - (-1)^q \binom{2q-1}{q} \right] u(1) = 0 & \text{si } k = 3q + 1. \end{cases}$$

On a donc $u(1) = 0$ puis, grâce à (6.30) et (6.29)

$$u_M(\ell) = 0, \quad \forall \overline{M} \in \mathcal{R}(\Gamma), \forall \ell \in [1, r_k]. \quad (6.31)$$

Lorsque 3 divise k , les équations (6.28) restent vraies pour $t \in [1, k - r_k - 2]$. On en déduit que (6.30) reste vraie pour $t \in [1, k - r_k - 2]$. Ainsi (A_{k-r_k-2}) donne l'existence d'une constante C telle que

$$u_M(r_k + 1) - u_{MU}(r_k + 1) = C, \quad \forall \overline{M} \in \mathcal{R}(\Gamma).$$

Le choix particulier de $M \in \mathcal{R}^U(\Gamma)$ montre que $C = 0$. Grâce à (6.12b),

$$u_M(r_k + 1) = 0.$$

L'égalité $\alpha_M(2k - r_k - 1) = 0$ donne ensuite $u(1) = 0$ puis (6.31).

Finalement, si k est impair, le membre de droite de (6.10) est nul et, puisque les équations $\{tM\}$ sont linéairement indépendantes lorsque $\overline{M}$ parcourt $\mathcal{R}(\Gamma)$ et t parcourt $[1, k]$, on déduit que $s_M(t) = 0$. On en déduit qu'il n'y a pas de relation de dépendance linéaire faisant intervenir à la fois les équations provenant de S et de U .

On déduit le théorème 6.1.1 de ce qui précède.

6.5 Une autre application des périodes

Cet courte section propose une application du morphisme d'Eichler-Shimura indépendante de la précédente. On suppose désormais $\Gamma = \Gamma_0(p)$ avec p un nombre premier et on note $S(2k, p)$ de préférence à $S(2k, \Gamma_0(p))$.

Si p est un nombre premier, à une forme f de $S(2k, p)$ de développement de Fourier

$$f(z) = \sum_{n=1}^{+\infty} \widehat{f}(n) e(nz)$$

et un caractère χ modulo p , on associe

$$f \otimes \chi(z) = \sum_{n=1}^{+\infty} \widehat{f}(n) \chi(n) e(nz).$$

On note W_p l'involution de Fricke définie par

$$W_p f(z) = f|_{\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}}(z) = p^{-k} z^{-2k} f\left(\frac{-1}{pz}\right).$$

On note alors

$$W_p f \otimes \chi = (W_p f) \otimes \chi.$$

Le but de cette section est de montrer comment on peut caractériser une forme modulaire à partir des fonctions L de $W_p f$.

Dans [Mar01], le premier auteur prouve le

LEMME 6.5.1

Soit $k \geq 1$ un entier, p un nombre premier, χ un caractère modulo p et $f \in S(2k, p)$.

On a pour tout s complexe

$$\frac{p^{k-s}}{\tau(\overline{\chi})} \sum_{h=1}^p \overline{\chi}(h) \Lambda(f|_{\begin{pmatrix} 0 & -1 \\ 1 & h \end{pmatrix}}, s) = \begin{cases} \Lambda(W_p f \otimes \chi, s) & \text{si } \chi \neq \chi_0 ; \\ p \Lambda(W_p f \otimes \chi_0, s) - (p-1) \Lambda(W_p f, s) & \text{si } \chi = \chi_0. \end{cases}$$

Par orthogonalité, on déduit le

COROLLAIRE 6.5.2

Soit $k \geq 1$ un entier, p un nombre premier et $h \in \{1, \dots, p-1\}$. Soit $f \in S(2k, p)$ et $s \in \mathbb{C}$. Alors

$$\Lambda(f|_{\begin{pmatrix} 0 & -1 \\ 1 & h \end{pmatrix}}, s) = \frac{p^{s-k}}{p-1} \sum_{\chi \pmod{p}} \chi(h) \tau(\overline{\chi}) \Lambda(W_p f \otimes \chi, s) - p^{s-k} \Lambda(W_p f \otimes \chi_0, s) + p^{s-k} \Lambda(W_p f, s).$$

On définit $X(p)$ comme l'ensemble des $p-1$ caractères modulo p . On déduit du corollaire 6.5.2 la proposition 6.1.2 : on note $m(h)$ la matrice $\begin{pmatrix} 0 & -1 \\ 1 & h \end{pmatrix}$. D'après le corollaire 6.5.2, l'hypothèse de la proposition à prouver implique que $L(f|_{m(h)}, \ell) = L(g|_{m(h)}, \ell)$ pour tout h de $[1, p-1]$ et ℓ de $[1, k]$. D'autre part, on déduit de l'égalité

$$L(f|_S, \ell) = -\frac{(2\pi)^\ell}{\Gamma(\ell)} \Lambda(W_p f, \ell)$$

que $L(f|_S, \ell) = L(g|_S, \ell)$ pour tout ℓ de $[1, k]$. Puisque I , S et les matrices $m(h)$ lorsque h parcourt $[1, p-1]$ constituent un ensemble de représentants du quotient $\Gamma_0(p) \backslash SL(2, \mathbb{Z})$, on déduit de la proposition 6.3.1 que $L(f|_M, \ell) = L(g|_M, \ell)$ pour tout $M \in \mathcal{R}(\Gamma)$ et $\ell \in [1, 2k-1]$. Finalement, on a $\rho_M(f) = \rho_M(g)$ et, grâce à l'épimorphisme de d'Eichler-Shimura on a $f = g$, ce qui termine la preuve.

Annexe A

Sommes de Kloosterman

Soit m, n des entiers positifs ou nuls et c un entier strictement positif, on définit la somme de Kloosterman $S(m, n; c)$ par

$$S(m, n; c) = \sum_{\substack{x \pmod{c} \\ (x, c) = 1}} e\left(\frac{mx + n\bar{x}}{c}\right)$$

avec $x\bar{x} \equiv 1 \pmod{c}$. Cette somme ne dépend que des classes modulo c de m et n . Pour faciliter la lecture des preuves, on fera la

CONVENTION 1

Lorsqu'un symbole surligné apparaît dans une somme de Kloosterman, il désigne l'inverse du même symbole non surligné modulo le dernier terme de la somme. Ainsi dans $S(a\bar{r}, b; c)$ a-t-on $r\bar{r} \equiv 1 \pmod{c}$.

On donne quelques propriétés individuelles des sommes de Kloosterman. On a d'abord le lemme de commutation

LEMME A.1

Soit m, n des entiers positifs ou nuls et c un entier strictement positif alors

$$S(m, n; c) = S(n, m; c).$$

Démonstration – Cela résulte du changement de variable $x \mapsto \bar{x}$ dans la définition.
 $\square$

Si $m = 0$ on obtient les sommes de Ramanujan,

LEMME A.2

(Sommes de Ramanujan) Soit m, n des entiers positifs ou nuls et c un entier strictement positif tel que c divise m alors

$$S(m, n; c) = \sum_{d|(n, c)} \mu\left(\frac{c}{d}\right) d = \varphi(c) \frac{\mu\left(\frac{c}{(n, c)}\right)}{\varphi\left(\frac{c}{(n, c)}\right)}.$$

Démonstration – On a

$$S(m, n; c) = \sum_{\substack{x \pmod{c} \\ (x, c) = 1}} e\left(\frac{nx}{c}\right) = R(n; c).$$

Soit d un entier premier à c . Un système de représentants modulo cd des éléments inversibles modulo cd est

$$\{\delta c + \gamma d, 1 \leq \delta \leq d, 1 \leq \gamma \leq c, (\delta, d) = 1, (\gamma, c) = 1\}$$

comme le montre la non-équivalence de chacun des termes de cet ensemble et le calcul de son cardinal. On a donc

$$R(n; cd) = \sum_{\substack{\gamma \pmod{c} \\ (\gamma, c) = 1}} \sum_{\substack{\delta \pmod{d} \\ (\delta, d) = 1}} e\left(\frac{n(\delta c + \gamma d)}{cd}\right) = R(n; c)R(n; d).$$

Ainsi, $c \mapsto R(n; c)$ est multiplicative.

On obtient la première égalité du lemme en utilisant le fait que la fonction de Möbius est l'inverse de convolution de la fonction constante égale à 1

$$R(n; c) = \sum_{1 \leq x \leq c} e\left(\frac{nx}{c}\right) \sum_{\ell \mid (x, c)} \mu(\ell) = \sum_{\ell \mid c} \mu(\ell) \sum_{1 \leq y \leq \frac{c}{\ell}} e\left(\frac{n\ell y}{c}\right)$$

ce qui, après évaluation de la somme intérieure se récrit

$$R(n; c) = \sum_{\substack{\ell \mid c \\ \frac{c}{\ell} \mid n}} \mu(\ell) \frac{c}{\ell} = \sum_{d \mid (n, c)} \mu\left(\frac{c}{d}\right) d$$

après avoir posé $d = \frac{c}{\ell}$.

Enfin la deuxième égalité est obtenue en comparant les membres de droite et gauche lorsque c est puissance d'un nombre premier et en concluant par multiplicativité. $\square$

LEMME A.3

(Relation de Selberg) Si m, n, c sont des entiers strictement positifs tels que $(m, n, c) = 1$ alors

$$S(m, n; c) = S(mn, 1; c).$$

LEMME A.4

Si m, n, a, c sont des entiers strictement positifs tels que $(a, c) = 1$ alors

$$S(m, na; c) = S(ma, n; c).$$

Démonstration – Il suffit d'effectuer le changement de variable $x \mapsto ax$ dans la définition. $\square$

LEMME A.5

(Multiplicativité croisée) Si m, n, q, r sont des entiers strictement positifs tels que $(q, r) = 1$ alors

$$S(m, n; qr) = S(m\bar{q}, n\bar{q}; r)S(m\bar{r}, n\bar{r}; q) = S(m\bar{q}^2, n; r)S(m\bar{r}^2, n; q).$$

LEMME A.6

(Multiplicativité croisée) Soit $q = \prod_{p \mid q} p^{v_p(q)}$ un entier strictement positif. Pour tout nombre premier $p \mid q$ on note $q_p = \frac{q}{p^{v_p(q)}}$. Alors si m et n sont deux entiers strictement positifs

$$S(m, n; q) = \prod_{p \mid q} S(m\bar{q}_p, n\bar{q}_p; p^{v_p(q)}) = \prod_{p \mid q} S(m\bar{q}_p^2, n; p^{v_p(q)}).$$

Démonstration – On considère trois entiers strictement positifs s, t, u premiers entre eux deux à deux. Alors grâce au lemme A.5

$$S(m, n; stu) = S(m\tilde{s}, n\tilde{s}; tu)S(m\overline{tu}, n\overline{tu}; s)$$

où $s\tilde{s} \equiv 1 \pmod{tu}$. Or

$$S(m\tilde{s}, n\tilde{s}; tu) = S(m\tilde{s}\tilde{t}, n\tilde{s}\tilde{t}; u)S(m\tilde{s}\tilde{u}, n\tilde{s}\tilde{u}; t).$$

D'autre part, puisque $s\tilde{s} \equiv 1 \pmod{tu}$ alors $s\tilde{s} \equiv 1 \pmod{t}$ et $s\tilde{s} \equiv 1 \pmod{u}$ donc on peut remplacer dans les équations précédentes $\tilde{s}$ par $\overline{s}$ pour obtenir

$$S(m, n; stu) = S(m\overline{st}, n\overline{st}; u)S(m\overline{su}, n\overline{su}; t)S(m\overline{tu}, n\overline{tu}; s).$$

Cette remarque permet d'obtenir la première égalité du lemme par itération. La seconde égalité découle du lemme A.4. $\square$

On note que si $(m, n, qr) = 1$ l'application des lemmes A.5 et A.3 donne le

LEMME A.7

Si m, n, q, r sont des entiers strictement positifs tels que $(q, r) = 1$ et $(m, n, qr) = 1$ alors

$$S(m, n; qr) = S(mn\overline{q}^2, 1; r)S(mn\overline{r}^2, 1; q)$$

D'autre part, lorsque c est une puissance d'un nombre premier on a le

LEMME A.8

Si p est un nombre premier, si m est un entier strictement positif divisible par p et si a est un entier positif ou nul alors

$$S(m, 1; p^a) = \mu(p^a)$$

On en déduit les lemmes A.9 et A.10.

LEMME A.9

Soit q un entier supérieur ou égal à 1 et m un entier strictement positif divisible par le noyau de q , $N(q) = \prod_{p|q} p$. Alors

$$S(m, 1; q) = \mu(q).$$

Démonstration – On écrit $q = \prod_{p|q} p^{v_p(q)}$. Alors, d'après le lemme de multiplicativité croisée (lemme A.6) on a

$$S(m, 1; q) = \prod_{p|q} S(m\overline{q_p}^2, 1; p^{v_p(q)})$$

avec $q_p = \frac{q}{p^{v_p(q)}}$. Le lemme A.8 donne alors

$$S(m\overline{q_p}^2, 1; p^{v_p(q)}) = \mu(p^{v_p(q)})$$

et la multiplicativité de μ permet de conclure. $\square$

LEMME A.10

Si m, q, r sont des entiers strictement positifs tels que $(m, q, r) > 1$ alors

$$S(m, 1; qr) = 0.$$

Démonstration – Soit p un diviseur premier de (m, q, r) . On écrit $m = m'p^a$, $q = q'p^b$ et $r = r'p^c$ avec $(m', p) = (q', p) = (r', p) = 1$ et $a \geq 1, b \geq 1, c \geq 1$. Alors, grâce à la relation de multiplicativité croisée (lemme A.5), $S(m, 1; qr)$ est divisible par $S(m'q'r'^2 p^a, 1; p^{b+c})$. Mais, puisque $b + c \geq 2$ et $a \geq 1$, cette dernière somme est nulle d'après le lemme A.8. $\square$

On déduit aussi des lemmes A.5 et A.8 le

LEMME A.11

Pour tous entiers strictement positifs m, n, q et r avec $n|q$

$$S(mn, 1; rq) = \begin{cases} \mu(q)S(m\overline{n}, 1; r\frac{q}{n}) & \text{si } (r, n) = 1 \text{ et } n \parallel q; \\ 0 & \text{sinon.} \end{cases}$$

Démonstration – Si $(r, n) = 1$ et $(n, \frac{q}{n}) = 1$, la relation de multiplicativité croisée (lemme A.5) permet d'écrire la factorisation

$$S(mn, 1; rq) = S(m\overline{n}, 1; r\frac{q}{n})S(mnr\frac{\overline{q}^2}{n}, 1; n).$$

Le lemme A.9 permet alors de conclure. Si $(r, n) \neq 1$ on a $(mn, q, r) \neq 1$. Si $(n, \frac{q}{n}) \neq 1$ on écrit $rq = rn\frac{q}{n}$ et $(mn, rn, \frac{q}{n}) \neq 1$. Dans les deux cas le lemme A.10 implique la nullité de $S(mn, 1; rq)$. $\square$

LEMME A.12

Soit m, n, c trois entiers strictement positifs. Soit p un nombre premier. On suppose que p^2 divise c et que p divise m . La somme $S(m, n; c)$ est nulle dès que l'une des conditions suivantes est vérifiée

- 1) p ne divise pas n ;
- 2) $v_p(m) \geq v_p(c) \geq v_p(n) + 2$;
- 3) $v_p(c) \geq v_p(m) + 1 \geq v_p(n) + 2$.

Démonstration – 1. Dans le premier cas, les lemmes A.4 et A.5 permettent de factoriser $S(m, n; c)$ par $S(mh, 1; p^{v_p(c)})$ avec $h = n\overline{c'}^2, c = p^{v_p(c)}c', c'\overline{c'} \equiv 1 \pmod{p^{v_p(c)}}$. Cette dernière somme est alors nulle d'après le lemme A.8.

Dans les deuxième et troisième cas, on peut supposer que p divise n (sinon on se ramène au cas 1.) et on écrit

$$\begin{aligned} c &= p^{\gamma+2}c', (p, c') = 1, \gamma \geq 0; \\ m &= p^{\nu+2}m', (p, m') = 1, \nu \geq 0; \\ n &= p^{\eta+1}c', (p, n') = 1, \eta \geq 0. \end{aligned}$$

Grâce aux lemmes A.4 et A.5, on factorise $S(m, n; c)$ par $S(hp^{\nu+2}, p^{\eta+1}; p^{\gamma+2})$ avec $h = m'n'\overline{c'}^2, c'\overline{c'} \equiv 1 \pmod{p^{\gamma+2}}$.

2. Dans le deuxième cas, on a $\nu + 2 \geq \gamma + 2$, la somme $S(hp^{\nu+2}, p^{\eta+1}; p^{\gamma+2})$ est une somme de Ramanujan. Puisque p^2 divise $\frac{p^{\gamma+2}}{(p^{\eta+1}, p^{\gamma+2})}$, cette somme de Ramanujan est nulle.

3. Dans le troisième cas, on a $\gamma \geq \nu + 1$ et $\nu \geq \eta$. On écrit alors

$$\begin{aligned} S(hp^{\nu+2}, p^{\eta+1}; p^{\gamma+2}) &= \sum_{\substack{x \pmod{p^{\gamma+2}} \\ (x, p^{\gamma+2})=1}} e\left(\frac{hp^{\nu+1}x + p^{\eta}\overline{x}}{p^{\gamma+1}}\right) \\ &= \sum_{\substack{x=0 \\ (x, p)=1}}^{p^{\gamma+2}-1} e\left(\frac{hp^{\nu+1}x + p^{\eta}\overline{x}}{p^{\gamma+1}}\right). \end{aligned}$$

Par division euclidienne de x par $p^{\gamma+1}$ on écrit de façon unique $x = y + p^{\gamma+1}k$ avec $0 \leq y \leq p^{\gamma+2} - 1$ et $0 \leq k \leq p - 1$. Les assertions $(x, p) = 1$ et $(y, p) = 1$ sont alors équivalentes. On a alors $\bar{x} = \bar{y}(1 - \bar{y}kp^{\gamma+1})$ avec $y\bar{y} \equiv 1 \pmod{p^{\gamma+2}}$. Pour le prouver, il suffit de vérifier que $x\bar{x} \equiv 1 \pmod{p^{\gamma+2}}$. Et si $y\bar{y} \equiv 1 \pmod{p^{\gamma+2}}$ alors $y\bar{y} \equiv 1 \pmod{p^{\gamma+1}}$. On a alors

$$\begin{aligned} S(hp^{\nu+2}, p^{\eta+1}; p^{\gamma+2}) &= \sum_{k=0}^{p-1} \sum_{\substack{y=0 \\ (y,p)=1}}^{p^{\gamma+1}-1} e\left(\frac{hp^{\nu+1}y + p^{\eta}\bar{y}}{p^{\gamma+1}}\right) \\ &= pS(hp^{\nu+1}, p^{\eta}; p^{\gamma+1}). \end{aligned}$$

Si $\eta = 0$ alors $\nu + 1 \geq 1$ et $\gamma + 1 \geq 2$ donc le lemme A.8 permet de conclure. Si $\eta \neq 0$, on réitère le processus pour obtenir

$$S(hp^{\nu+2}, p^{\eta+1}; p^{\gamma+2}) = p^{\eta+1}S(hp^{\nu+1-\eta}, 1; p^{\gamma+1-\eta}).$$

Puisque $\nu + 1 - \eta \geq 1$ et $\gamma + 1 - \eta \geq 2$, on conclut à l'aide du lemme A.8 $\square$

Enfin, on a la majoration due à Weil et Estermann [Est61],

LEMME A.13 (MAJORATION DE WEIL-ESTERMANN)

Si m, n, c sont trois entiers strictement positifs,

$$|S(m, n; c)| \leq \sqrt{(m, n, c)\tau(c)}\sqrt{c}.$$

On donne ensuite quelques propriétés de sommes de Kloosterman.

LEMME A.14

Si m, n, c sont des entiers strictement positifs alors

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} S(m, na; c) = \frac{\mu\left(\frac{c}{(m,c)}\right)}{\varphi\left(\frac{c}{(m,c)}\right)} \frac{\mu\left(\frac{c}{(n,c)}\right)}{\varphi\left(\frac{c}{(n,c)}\right)} \varphi(c)^2.$$

Démonstration – On ouvre la somme de Kloosterman et, après interversion des sommes finies on obtient

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} S(m, na; c) = \sum_{\substack{x \pmod{c} \\ (x,c)=1}} e\left(\frac{m\bar{x}}{c}\right) \sum_{\substack{a \pmod{c} \\ (a,c)=1}} e\left(\frac{nax}{c}\right).$$

Dans la seconde somme, on effectue le changement de variable $b = ax$, qui est justifié puisque $(x, c) = 1$ puis, dans la première on effectue le changement $x \mapsto \bar{x}$. On obtient alors

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} S(m, na; c) = \sum_{\substack{x \pmod{c} \\ (x,c)=1}} e\left(\frac{mx}{c}\right) \sum_{\substack{b \pmod{c} \\ (b,c)=1}} e\left(\frac{nb}{c}\right).$$

Le résultat s'obtient par évaluation des sommes de Ramanujan. $\square$

On peut légèrement généraliser ce résultat en tordant les sommes par des caractères de Dirichlet. On obtient alors le

LEMME A.15

Si m, n, c sont des entiers strictement positifs et si χ est un caractère modulo c , alors

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a)S(m, na; c) = G_{\chi}(m)G_{\chi}(n)$$

où $G_\chi(m)$ est la somme de Gauss associée à m

$$G_\chi(m) = \sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) e\left(\frac{ma}{c}\right).$$

En particulier, si $(n, c) = 1$ on a

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) S(m, na; c) = \bar{\chi}(n) G_\chi(m) G_\chi$$

où $G_\chi = G_\chi(1)$ est la somme de Gauss associée à 1

Démonstration – On ouvre les sommes de Kloosterman, on intervertit les sommes puis, après le changement de variable $b = ax$ on obtient

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) S(m, na; c) = \sum_{\substack{x \pmod{c} \\ (x,c)=1}} e\left(\frac{m\bar{x}}{c}\right) \sum_{\substack{b \pmod{c} \\ (b,c)=1}} \chi(\bar{x}b) e\left(\frac{nb}{c}\right).$$

la multiplicativité des caractères de Dirichlet puis le changement de variables $x \mapsto \bar{x}$ permettent de conclure. Dans le cas particulier où n et c sont premiers entre eux, on fait le changement de variables supplémentaires $d = nb$ pour obtenir le résultat énoncé. $\square$

On donne un résultat semblable lorsque χ est un caractère modulo un diviseur de c .

LEMME A.16

Soit c un entier et χ un caractère modulo c . Soit n un entier alors

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) S(an, 1; cn) = \chi(n) \mu(n) G_\chi^2$$

Démonstration – Si $(c, n) \neq 1$ alors $S(an, 1; cn) = 0$ d'après le lemme A.10 et $\chi(n) = 0$ donc le résultat est vrai. On suppose maintenant $(c, n) = 1$. Par les lemmes A.5 et A.2 on a

$$\sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) S(an, 1; cn) = \mu(n) \sum_{\substack{a \pmod{c} \\ (a,c)=1}} \chi(a) S(a\bar{n}, 1; c)$$

et on obtient le résultat énoncé par utilisation du lemme A.15. $\square$

LEMME A.17

On suppose vraie l'hypothèse de Riemann des séries L associées aux caractères de Dirichlet. Soit ℓ, t, N des entiers strictement positifs et x un réel strictement positif

$$\sum_{\substack{p \leq x \\ (p, N)=1}} S(p\ell, 1; t) \frac{\ln p}{\sqrt{p}} = 2\mu(t) \frac{\mu\left(\frac{t}{(\ell, t)}\right)}{\varphi\left(\frac{t}{(\ell, t)}\right)} \sqrt{x} + O(\varphi(t) \ln^3(tx) + \sqrt{t} \tau(t) \ln(N))$$

Démonstration – On note $\Sigma_N(x; \ell; t)$ la somme de gauche du lemme. La contribution à cette somme des p divisant t est négligeable. On pose $t = pt'$. Grâce aux lemmes A.11 et A.13 on a

$$|S(p\ell, 1; pt')| \leq |S(\overline{p}\ell, 1; t')| \ll \frac{1}{\sqrt{p}} \sqrt{t}\tau(t)$$

d'où

$$\left| \sum_{\substack{p \leq x \\ (p, N)=1, p|t}} S(p\ell, 1; t) \frac{\ln p}{\sqrt{p}} \right| \ll \sqrt{t}\tau(t) \ln \ln(3t).$$

Ainsi

$$\Sigma_N(x; \ell; t) = \sum_{\substack{p \leq x \\ (p, N)=(p, t)=1}} S(p\ell, 1; t) \frac{\ln p}{\sqrt{p}} + O(\sqrt{t}\tau(t) \ln \ln(3t)).$$

On efface la condition $(p, N) = 1$ grâce à la majoration

$$\sum_{p|N} S(p\ell, 1; t) \frac{\ln p}{\sqrt{p}} \ll \sqrt{t}\tau(t) \sum_{p|N} \frac{\ln p}{\sqrt{p}} \leq \sqrt{t}\tau(t) \ln N.$$

Soit a tel que $p \equiv a \pmod{t}$ alors $(a, t)|p$ et puisque $(p, t) = 1$ alors $(a, t) = 1$. Ainsi

$$\begin{aligned} \Sigma_N(x; \ell; t) &= \sum_{\substack{a \pmod{t} \\ (a, t)=1}} S(a\ell, 1; t) \sum_{\substack{p \leq x \\ p \equiv a \pmod{t}}} \frac{\ln p}{\sqrt{p}} \\ &\quad + O(\sqrt{t}\tau(t) \ln \ln(3t) + \sqrt{t}\tau(t) \ln N). \end{aligned}$$

Par utilisation de l'orthogonalité des caractères modulo t on a ensuite

$$\Sigma_N(x; \ell; t) = \frac{1}{\varphi(t)} \sum_{\chi \pmod{t}} \sum_{a \pmod{t}} \chi(a) S(a\ell, 1; t) \sum_{p \leq x} \overline{\chi}(p) \frac{\ln p}{\sqrt{p}}.$$

Grâce au lemme A.15 et à l'hypothèse de Riemann des séries L de Dirichlet on en déduit

$$\begin{aligned} \Sigma_N(x; \ell; t) &= \frac{1}{\varphi(t)} \sum_{\chi \pmod{t}} G_\chi G_\chi(\ell) (2\delta_\chi \sqrt{x} + O(\ln^3 tx)) \\ &\quad + O(\sqrt{t}\tau(t) \ln \ln(3t) + \sqrt{t}\tau(t) \ln N). \end{aligned}$$

On peut alors conclure

$$\Sigma_N(x; \ell; t) = 2\mu(t) \frac{\mu\left(\frac{t}{(\ell, t)}\right)}{\varphi\left(\frac{t}{(\ell, t)}\right)} \sqrt{x} + O(\varphi(t) \ln^3(tx) + \sqrt{t}\tau(t) \ln N).$$

□

On obtient un terme d'erreur plus précis dans le

LEMME A.18

On suppose vraie l'hypothèse de Riemann des séries L associées aux caractères de Dirichlet. Soit N un entier, n un diviseur de N et c un multiple de N . Alors pour tout $x \geq 2$

$$\sum_{\substack{p \leq x \\ (p, N)=1}} S(pn, 1; c) \frac{\ln p}{\sqrt{p}} = 2\delta(n|c) \mu(n) \frac{\mu\left(\frac{c}{n}\right)^2}{\varphi\left(\frac{c}{n}\right)} \sqrt{x} + O\left(\frac{c}{n} \ln^3(cx)\right)$$

où $\delta(n|c) = 1$ si $(n, \frac{c}{n}) = 1$ et 0 sinon.

Démonstration – On pose $c' = \frac{c}{n}$. On commence par évaluer la somme

$$\sum_{\substack{p \leq x \\ (p, c')=1}} S(pn, 1; c) \ln p.$$

Après avoir regroupé les p par classes de congruences et détecté ces congruences par insertion de caractères, on trouve

$$\sum_{\substack{p \leq x \\ (p, c')=1}} S(pn, 1; c) \ln p = \frac{1}{\varphi(c')} \sum_{\chi \pmod{c'}} \sum_{\substack{a \pmod{c'} \\ (a, c')=1}} \bar{\chi}(a) S(an, 1; c) \sum_{p \leq x} \chi(p) \ln p. \quad (\text{A.1})$$

En effet, si $p \equiv a \pmod{c'}$ alors $pn \equiv an \pmod{c}$ et $S(pn, 1; c) = S(an, 1; c)$. L'hypothèse de Riemann des séries L de Dirichlet donne, pour un caractère χ quelconque modulo c'

$$\sum_{p \leq x} \chi(p) \ln p = \delta_\chi x + O(\sqrt{x}(\ln c' x)^2)$$

δ_χ valant 1 si χ est le caractère principal et 0 pour tout autre caractère. Le lemme A.16 permet d'écrire

$$\sum_{\substack{a \pmod{c'} \\ (a, c')=1}} \bar{\chi}(a) S(an, 1; c) = \bar{\chi}(n) \mu(n) G_\chi^2.$$

Ainsi (A.1) devient

$$\sum_{\substack{p \leq x \\ (p, c')=1}} S(pn, 1; c) \ln p = \delta(n \| c) \mu(n) \frac{\mu(c')^2}{\varphi(c')} x + O\left(\frac{1}{\varphi(c')} \sum_{\chi \pmod{c'}} |G_\chi|^2 \sqrt{x}(\ln c' x)^2\right)$$

Or, par développement du carré et utilisation de la relation d'orthogonalité des caractères on obtient

$$\sum_{\chi \pmod{c'}} |G_\chi|^2 = \varphi(c')^2.$$

Ainsi

$$\sum_{\substack{p \leq x \\ (p, c')=1}} S(pn, 1; c) \ln p = \delta(n \| c) \mu(n) \frac{\mu(c')^2}{\varphi(c')} x + O(\varphi(c') \sqrt{x}(\ln c' x)^2) \quad (\text{A.2})$$

On efface la condition $(p, c') = 1$ en utilisant, si $(n, c') = 1$

$$\left| \sum_{\substack{p \leq x \\ p|c'}} S(pn, 1; c) \ln p \right| \leq \sum_{\substack{p \leq x \\ p|c'}} |S(\bar{n}p, 1; c')| \ln p \ll \tau(c') \sqrt{c'} \ln(c') \ll \varphi(c') \ln(c')$$

la première inégalité résultant du lemme A.11 et la deuxième du A.13. Ce résultat reste valable lorsque $(n, c') \neq 1$ car dans ce cas la somme est nulle par le lemme A.11. Enfin, on efface la contribution des p divisant N en utilisant, si $(n, c') = 1$

$$\left| \sum_{\substack{p \leq x \\ p|N}} S(pn, 1; c) \ln p \right| \leq \sum_{\substack{p \leq x \\ p|N}} |S(p\bar{n}, 1; c')| \ln p \ll \tau(c') \sqrt{c'} \ln(N) \ll \varphi(c') \sqrt{c'} \ln(c').$$

Ainsi, l'expression (A.2) est vraie en remplaçant la condition $(p, c') = 1$ par la condition $(p, N) = 1$. Ce résultat reste valable lorsque $(n, c') \neq 1$ car dans ce cas la somme est nulle par le lemme A.11. Enfin, on obtient le résultat du lemme par intégration par parties. $\square$

Annexe B

Fonctions de Bessel

On récapitule dans cette partie les propriétés des fonctions J de Bessel dont on aura besoin. Si k est un entier positif ou nul, la fonction de Bessel d'ordre k est définie par

$$J_k(z) = \sum_{r=0}^{\infty} \frac{(-1)^r}{r!(k+r)!} \left(\frac{z}{2}\right)^{k+2r}$$

pour tout $z \in \mathbb{C}$. Pour $k \geq 1$ on a

$$J_k(z) \ll_k z. \quad (\text{B.1})$$

D'autre part, pour tout $k \geq 0$ on a

$$J_k(z) = \frac{1}{\pi} \int_0^\pi \cos(n\theta - z \sin \theta) d\theta$$

d'où on déduit, pour tout $k \geq 0$ et tout $z \in \mathbb{C}$

$$|J_k(z)| \leq 1. \quad (\text{B.2})$$

D'autre part, on a les relations de récurrence suivantes

$$2\frac{k}{x}J_k(x) = J_{k-1}(x) + J_{k+1}(x) \quad (x \neq 0, k \geq 1) \quad (\text{B.3})$$

et

$$2J'_{k-1}(x) = J_{k-2}(x) - J_k(x) \quad (k \geq 2) \quad (\text{B.4})$$

Enfin, la transformée de Mellin de J_{k-1} est donnée par

$$\int_0^\infty J_{k-1}(x)x^s dx = 2^s \frac{\Gamma(\frac{k+s}{2})}{\Gamma(\frac{k-s}{2})} \quad (\text{B.5})$$

cette égalité étant valable pour $\Re(s) < \frac{1}{2}$ et $\Re(s+k) > 0$. On obtient un développement asymptotique de cette transformée de Mellin en considérant le développement en produit de Gauss de la fonction Γ

$$\Gamma(z) = \lim_{n \rightarrow \infty} \frac{n^z}{z} \prod_{k=1}^n \frac{k}{z+k}$$

valable pour $\Re(z) > 0$. On en déduit, pour tout $0 < \varepsilon < 1$ la majoration

$$\frac{\Gamma(a+s)}{\Gamma(a-s)} = a^{2s} \left(1 + O_\varepsilon \left(\frac{s}{a} \right) \right) \quad (\text{B.6})$$

uniforme en $a > 1$ et $|s| \leq 1 - \varepsilon$.

Bibliographie

- [AL70] A.O.L. ATKIN et Joseph LEHNER. « Hecke Operators on $\Gamma_0(m)$ ». *Mathematische Annalen*, 185 : 134–160, 1970.
- [BD85] Theodor BRÖCKER et Tammo tom DIECK. *Representations of Compact Lie Group*, volume 98 de *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1985.
- [Bil95] Patrick BILLINGSLEY. *Probability and Measure*. John Wiley & Sons, New York, Chichester, Brisbane, Toronto, Singapore, 3^e édition, 1995.
- [BM90] Armand BRUMER et Oisín MCGUINNESS. « The Behavior of the Mordell-Weil Group of Elliptic Curves ». *Bulletin of the American Mathematical Society*, 23(2) : 375–382, october 1990.
- [BMP86] Yuriĭ Aleksandrovich BRYCHOV, Oleg Igorevich MARICHEV et Anatoliĭ Platonovich PRUDNIKOV. *Elementary Functions*, volume 1 de *Integrals and Series*. Gordon and Beach Science Publishers, New York, Londres, Paris, Montreux, Tokyo, Melbourne, 1986. 3^e impression corrigée, 1992.
- [Brü95a] Jörg BRÜDERN. *Einführung in die analytische Zahlentheorie*. Springer-Lehrbuch. Springer-Verlag, Berlin, Heidelberg, New York, 1995.
- [Bru95b] Armand BRUMER. « The Rank of $J_0(N)$ ». *Astérisque*, 228 : 41–68, 1995.
- [BS96] Armand BRUMER et Joseph H. SILVERMAN. « The Number of Elliptic Curves over $\mathbb{Q}$ with Conductor N ». *Manuscripta Mathematica*, 91 : 95–102, 1996.
- [Bum98] Daniel BUMP. *Automorphic Forms and Representations*, volume 55 de *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, New York, Melbourne, 1998.
- [CDF97] John Brian CONREY, William DUKE et David W. FARMER. « The distribution of the eigenvalues of Hecke operators ». *Acta Arithmetica*, LXXVIII(4) : 405–409, 1997.
- [CS97] Gary CORNELL et Joseph H. SILVERMAN, éditeurs. *Modular Forms and Fermat's Last Theorem*. Springer-Verlag, Berlin, Heidelberg, New York, 1997.
- [Del74] Pierre DELIGNE. « La conjecture de Weil. I ». *Publications mathématiques de l'institut des hautes études scientifiques*, 43 : 273–307, 1974.
- [DJ] Aise Johan DE JONG. « A Theorem of Serre ». Manuscrit transmis par Peter Sarnak.
- [DK00] William DUKE et Emmanuel KOWALSKI. « A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations ». *Inventiones Mathematicae*, 139(1) : 1–39, 2000.
- [Ef81] Nikolai EFIMOV. *Géométrie Supérieure*. Mir, Moscou, 1981.

-
- [Eic54] Martin EICHLER. « Quaternäre quadratische Formen und die Riemannsche Vermutung ». *Archiv der Mathematik*, V : 355–366, 1954.
 - [Est61] Theodor ESTERMANN. « On Kloosterman's sum ». *Mathematika*, 8 : 83–86, 1961.
 - [Fer96] Stéphane FERMIGIER. « Étude expérimentale du rang de familles de courbes elliptiques sur $\mathbb{Q}$ ». *Experimental Mathematics*, 5(2) : 119–130, 1996.
 - [Fla79] Daniel E. FLATH. « Decomposition of representations into tensor products ». Dans Armand BOREL et William A. CASSELMAN, éditeurs, *Automorphic forms, representations and L-functions*, volume XXXIII, pages 179–183, Rhode Island, 1979. Proceedings of the symposium in pure mathematics of the American Mathematical Society, Corvallis, 1977, American Mathematical Society.
 - [Gan66] Felix Ruvimovič GANTMACHER. *Théorie des matrices, tome 1 : théorie générale*, volume XVIII de *Collection universitaire de mathématiques*. Dunod, Paris, 1966.
 - [Gel97] Stephen GELBART. « Three Lectures on the Modularity of $\bar{\rho}_{E,3}$ and the Langlands Reciprocity Conjecture », chapitre VI, pages 155–207. Dans Cornell et Silverman [CS97], 1997.
 - [GHL94] Dorian GOLDFELD, Jeffrey HOFFSTEIN et Daniel LIEMAN. « An effective zero-free region ». *Annals of Mathematics*, 140 : 177–181, 1994. 2^e sÈrie. Appendice de [HL94].
 - [GR80] Izrail Solomonovich GRADSHTEYN et Iosif Moiseevich RYZHIK. *Table of Integrals, Series and Products*. Academic Press, New York, Londres, Toronto, Sydney, San Fransisco, 1980.
 - [Guo96] Jiandong GUO. « On the positivity of the central critical values of automorphic L -functions for $GL(2)$ ». *Duke Mathematical Journal*, 83 : 157–190, avril 1996.
 - [GZ86] Benedict H. GROSS et Don B. ZAGIER. « Heegner points and derivatives L -series ». *Inventiones Mathematicae*, 84 : 225–320, 1986.
 - [Hec37] Erich HECKE. « Über Modulfunktionen und die Dirichletschen Reihen mit Eulerschen Produktentwicklung II ». *Mathematische Annalen*, 114 : 316–351, 1937.
 - [HL94] Jeffrey HOFFSTEIN et Paul LOCKHART. « Coefficients of Maass forms and the Siegel zero ». *Annals of Mathematics*, 140 : 161–181, 1994. 2^e sÈrie.
 - [Hua82] Loo-Keng HUA. *Introduction to number theory*. Springer-Verlag, Berlin, Heidelberg, New York, 1982.
 - [Hum80] James E. HUMPHREYS. *Arithmetic Groups*, volume 789 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1980.
 - [Igu59] Jun-ichi IGUSA. « Kroneckerian Model of Fields of Elliptic Modular Functions ». *American Journal of Mathematics*, LXXXI : 561–577, 1959.
 - [ILS00] Henryk IWANIEC, Wenzhi LUO et Peter SARNAK. « Low Lying Zeros of Families of L -Functions ». *Publications mathématiques de l'Institut des hautes études scientifiques*, 91 : 55–131, 2001.
 - [IS00] Henryk IWANIEC et Peter SARNAK. « Perspectives on the Analytic Theory of L -Functions ». Dans Noga ALON, Jean BOURGAIN, Alain CONNES, Mickael GROMOV et Vitali MILMAN, éditeurs, *Visions in Mathematics – Toward 2000*, volume II, pages 705–741, Birkhäuser, Basel, 2000. GAFA 2000. Special Volume, conference held at Tel Aviv in 1999.

-
- [Iwa97] Henryk IWANIEC. *Topics in Classical Automorphic Forms*, volume 17 de *Graduate Studies in Mathematics*. American Mathematical Society, Providence, Rhode Island, 1997.
 - [JL70] Hervé JACQUET et Robert P. LANGLANDS. *Automorphic Forms on $GL(2)$* , volume 114 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1970. Disponible sur [http : // www. ubc. ca / DigitalMathArchive / Langlands](http://www.ubc.ca/DigitalMathArchive/Langlands).
 - [KM99] Emmanuel KOWALSKI et Philippe MICHEL. « The analytic rank of $J_0(q)$ and zeros of automorphic L -functions ». *Duke Mathematical journal*, 100(3) : 503–542, décembre 1999.
 - [KM01] Emmanuel KOWALSKI et Philippe MICHEL. « Zeros of families of automorphic L -functions close to 1 and applications ». En préparation, ≥ 2001 .
 - [KMV00a] Emmanuel KOWALSKI, Philippe MICHEL et Jeffrey M. VANDERKAM. « Mollification of the fourth moment of automorphic L -functions and arithmetic applications ». *Inventiones Mathematicae*, 142(1) : 95–151, 2000.
 - [KMV00b] Emmanuel KOWALSKI, Philippe MICHEL et Jeffrey M. VANDERKAM. « Non-vanishing of high derivatives of automorphic L -functions at the center of the critical strip ». *Journal für die reine und angewandte Mathematik*, 526 : 1–34, 2000.
 - [Kna92] Anthony W. KNAPP. *Elliptic Curves*, volume 40 de *Mathematical Notes*. Princeton University Press, Princeton, 1992.
 - [KS99a] Nicholas M. KATZ et Peter SARNAK. *Random Matrices, Frobenius Eigenvalues, and Monodromy*, volume 45 de *Colloquium Publications*. American Mathematical Society, Providence, Rhode Island, 1999.
 - [KS99b] Nicholas M. KATZ et Peter SARNAK. « Zeroes of zeta functions and symmetry ». *Bulletin of the American Mathematical Society*, 36(1) : 1–26, Janvier 1999. Nouvelle série.
 - [Li75] Wen-Ch'ing Winnie LI. « Newforms and Functional Equations ». *Mathematische Annalen*, 212 : 285–315, 1975.
 - [LR97a] Wenzhi LUO et Dinar RAMAKRISHNAN. « Determination of modular elliptic curves by Heegner points ». *Pacific Journal of Mathematics*, 181(3) : 251–258, 1997.
 - [LR97b] Wenzhi LUO et Dinar RAMAKRISHNAN. « Determination of modular forms by twists of critical L -values ». *Inventiones mathematicae*, 130 : 371–398, 1997.
 - [Luo99] Wenzhi LUO. « Values of symmetric L -functions at 1 ». *Journal für die reine und angewandte Mathematik*, 506 : 215–235, 1999.
 - [Luo00] Wenzhi LUO. « Nonvanishing of L -values and the strong Weyl law ». Préimprimé, 2000.
 - [Mar01] François MARTIN. « Périodes de formes modulaires de poids 1 ». Préimprimé, 2001.
 - [Miy89] Toshitsune MIYAKE. *Modular Forms*. Springer-Verlag, Berlin, Heidelberg, New York, 1989.
 - [MR97] François MARTIN et Emmanuel ROYER. « Formes modulaires ». Rapport de stage d'option scientifique, promotion X94, École polytechnique, Palaiseau, 1997.
 - [MR01] François MARTIN et Emmanuel ROYER. « Caractérisation des formes modulaires par les valeurs de leurs fonctions L ». Préimprimé, 2001.

-
- [Rib80] Ken RIBET. « Twists of Modular Forms and Endomorphisms of Abelian Varieties ». *Mathematische Annalen*, 253 : 43–62, 1980.
 - [Rie59] Bernhard RIEMANN. « Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse », pages 177–185. Dans [Rie90], 1859. Monatsberichte der Berliner Akademie, novembre 1859.
 - [Rie90] Bernhard RIEMANN. *Collected papers*. Springer-Verlag, Teubner, Berlin Heidelberg New York Leipzig, 1990.
 - [Roh97] David E. ROHRlich. « *Modular Curves, Hecke Correspondences, and L-Functions* », chapitre III, pages 41–100. Dans Cornell et Silverman [CS97], 1997.
 - [Roy00] Emmanuel ROYER. « Facteurs $\mathbb{Q}$ -simples de $J_0(N)$ de grande dimension et de grand rang ». *Bulletin de la Société mathématique de France*, 128 : 219–248, 2000.
 - [Roy01a] Emmanuel ROYER. « Formes modulaires et matrices aléatoires ». Exposé au séminaire des doctorants de l’université d’Orsay. Disponible sur [http : //royer.emmanuel.free.fr](http://royer.emmanuel.free.fr) , 2001.
 - [Roy01b] Emmanuel ROYER. « Petits zéros de fonctions L de formes modulaires ». *Acta Arithmetica*, 101 : 147–172, 2001.
 - [Roy01c] Emmanuel ROYER. « Statistique de la variable aléatoire $L(\text{sym}^2 f, 1)$ ». *Mathematische Annalen*, $\geq$ 2001. À paraître.
 - [RS96] Zéev RUDNICK et Peter SARNAK. « Zeros of principal L -functions and random matrix theory ». *Duke Mathematical Journal*, 81(2) : 269–322, 1996.
 - [Rud95] Walter RUDIN. *Analyse fonctionnelle*. Éditions internationales, Paris, 1995. Traduction de la 2^e édition américaine de *Functional Analysis*, McGraw-Hill, 1991.
 - [Sel92] Atle SELBERG. « Old and New Conjectures and Results About a Class of Dirichlet Series ». Dans Enrico BOMBIERI, éditeur, *Analytic Number Theory*, pages 367–385. Proceedings of the Amalfi Conference, Università di Salerno, 1992.
 - [Ser95] Jean-Pierre SERRE. *Cours d’arithmétique*. Le mathématicien. Presses Universitaires de France, Paris, 4^e édition, 1995.
 - [Ser97] Jean-Pierre SERRE. « Répartition asymptotique des valeurs propres de l’opérateur de Hecke T_p ». *Journal of the American Mathematical Society*, 10(1) : 75–102, 1997.
 - [Shi58] Gorô SHIMURA. « Correspondances modulaires et les fonctions ζ de courbes algébriques ». *Journal of the Mathematical Society of Japan*, 10(1) : 1–28, janvier 1958.
 - [Shi71] Gorô SHIMURA. *Introduction to the arithmetic theory of automorphic functions*, volume 11. Iwanami Shoten and Princeton University Press, Princeton, 1971. Kanô Memorial lectures 1.
 - [Shi72] Gorô SHIMURA. « Class fields over real quadratic fields and Hecke operators ». *Annals of Mathematics*, 95(1) : 130–190, janvier 1972. 2^e série.
 - [Shi75] Gorô SHIMURA. « On the holomorphy of certain Dirichlet series ». *Proceedings of the London Mathematical Society*, 31 : 79–98, 1975.
 - [Sko90] Nils-Peter SKORUPPA. « Binary quadratic forms and the Fourier coefficients of elliptic and Jacobi Forms ». *Journal für die reine und angewandte Mathematik*, 411 : 66–95, 1990.

-
- [ST99] Tetsuji SHIODA et Tomohide TERASOMA. « Existence of simple jacobian varieties of genus g with rank at least $4g + 5$ ». *American Journal of Mathematics*, 121 : 65–72, 1999.
- [Sta96] H.M. STARK. « On the determination of an L-function from one value ». Dans Bruce C. BERNDT, Harold G. DIAMOND et Adolf J. HILDEBRAND, éditeurs, *Analytic Number Theory*, volume 139 de *Progress in Mathematics*, pages 737–743, Basel, 1996. Proceedings of a Conference in Honor of Heini Halberstam, Allerton Park, 1995, Birkhäuser.
- [Ste98] William STEIN. « Hecke operators acting on the space $S_2(\Gamma_0(N))$ of weight 2 cusp forms for $\Gamma_0(N)$ ». [http : // modular . fas . harvard . edu / Tables / charpoly_s2 . html](http://modular.fas.harvard.edu/Tables/charpoly_s2.html), 1998.
- [Tch62] P.L. TCHEBYCHEF. *Œuvres de P.L. Tchebychef*, volume II. Chelsea, New York, 1962.
- [Ten95] Gérard TENENBAUM. *Introduction à la théorie analytique et probabiliste des nombres*, volume 1 de *Cours spécialisés*. Société mathématique de France, Paris, 1995.
- [ZK87] Don ZAGIER et Gerhard KRAMARZ. « Numerical investigations related to the L -series of certain elliptic curves ». *Journal of the Indian Mathematical Society*, 52 : 51–69, 1987.

Résumé

On propose quatre contributions à l'étude des fonctions L de formes modulaires. La première montre que le Jacobien d'une courbe modulaire possède un facteur simple sur le corps des rationnels de grande dimension et de rang nul, et un facteur simple de grande dimension et de grand rang. La seconde établit la conjecture de densité de niveau 1 des petits zéros pour de nouvelles familles de fonctions L de formes modulaires. La troisième étudie la distribution de la valeur en 1 de la fonction L de carré symétrique d'une forme modulaire. La dernière établit, en collaboration avec F. Martin, un critère de détermination des formes modulaires par les valeurs spéciales de leurs fonctions L .