L'équidistribution des points de Heegner des corps quadratiques imaginaires

Nicolas Templier
Avec l'aide de Philippe Michel

Octobre 2005

La théorie des nombres est un domaine qui ne se présente pas, très vaste et comprenant une foule d'objets provenant de tous les horizons mathématiques. J'ai voulu rendre compte de cette diversité tout en restant concis. Pour cela, j'ai pris un problème très précis dont l'énoncé est relativement simple. Dans le cours de sa résolution, j'introduirai quelques grands objets de la théorie des nombres, illustrés par des remarques ou exemples ou théorèmes.

1 L'énoncé du problème

Je vais tout d'abord introduire succinctement les notations et définitions pour pouvoir énoncer le théorème de [Duk88] dont je propose de donner les idées de la preuve. Je reviendrai ensuite longuement sur chaque concept un à un.

On note $\mathfrak{H}:=\{z=x+iy, y>0\}$ le demi-plan de Poincaré. On note Γ le groupe $SL_2(\mathbb{Z})=\{\gamma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, a,b,c,d\in\mathbb{Z}, ad-bc=1\}$. Il agit sur $\mathfrak{H}$ par homographies $\gamma z=\frac{az+b}{cz+d}$. On note $X=SL_2(\mathbb{Z})\backslash\mathfrak{H}$ l'espace des orbites. On peut représenter un 'domaine fondamental' pour cette action. L'espace $\mathfrak{H}$ est muni d'une forme volume $\frac{dxdy}{y^2}$ invariante par l'action de Γ. Elle engendre une mesure naturelle sur X, notée μ (on peut la voir sur un domaine fondamental comme la restriction de $\frac{dxdy}{y^2}$). X est de mesure finie : $\mu(X)=\frac{\pi}{3}=\pi-\frac{\pi}{3}-\frac{\pi}{3}-0$ (par la formule de Gauss-Bonnet).

D'un autre coté, D désignera un 'discriminant' (ie $D\in\mathbb{Z}-\{0\}$ $D\equiv 0,1[4]$), fondamental (si $D=f^2D'$, $f\in\mathbb{Z}$, D' discriminant alors $D=D'$), <u>négatif</u> ($D<0$). On définit l'ensemble des <u>points de Heegner</u> $He_D\subset X$ comme l'ensemble des racines de polynômes quadratiques à coefficients entiers de discriminant D. C'est à dire $He_D=\Gamma\backslash\{\tau\in\mathfrak{H}\text{ tq } A\tau^2+B\tau+C=0 \text{ où } B^2-4AC=D,\ A,B,C\in\mathbb{Z}\}$. Le cardinal $h(D)$ de He_D, appelé le <u>nombre de classes</u> est fini.

Théorème 1 (Duke 1988). *Les points de Heegner He_D <u>s'équidistribuent</u> dans l'espace X pour la mesure hyperbolique μ lorsque $D\to-\infty$.*

De manière plus précise, on a pour tout ouvert Ω assez régulier de X,

$$\frac{|\Omega \cap He_D|}{h(D)} = \frac{3}{\pi}\mu(\Omega) + O(|D|^{-\delta})$$

D'autres critères d'équidistributions ('sommes de Weyl') seront discutés au milieu de la partie 7.

2 La géométrie de $\Gamma\backslash\mathfrak{H}$

Le quotient $\Gamma\backslash\mathfrak{H}$ est un espace qui joue un rôle central dans de nombreux sujets en mathématiques, pour lesquels je ne vais pas tenter de donner une liste. [Shi], chapitre 1 est une bonne référence. Pour comprendre les domaines fondamentaux, on peut aussi lire [Kat92], plus expansif mais pas toujours rigoureux. Une des raison de la richesse est que le demi-plan de Poincaré est un revêtement universel à la fois pour les courbes holomorphes (ou surfaces de Riemann) et les surfaces munies d'une métrique riemannienne. Développons quelques aspects des deux géométries :

Point de vue complexe : En tant qu'ouvert de $\mathbb{C}$, $\mathfrak{H}$ est une surface de Riemann. Son groupe d'automorphisme est $PSL_2(\mathbb{R})$, les homographies. L'action de $PSL_2(\mathbb{Z}) \subset PSL_2(\mathbb{R})$ par automorphismes holomorphes est discontinue (les orbites ne s'accumulent pas), ce qui permet de munir X d'une unique structure de surface de Riemann. La théorie des courbes elliptiques sur $\mathbb{C}$ permet de construire l'invariant modulaire j qui est un isomorphisme de X sur $\mathbb{C}$.

Point de vue riemannien : $\mathfrak{H}$ est muni d'une métrique riemannienne $\frac{dx^2+dy^2}{y^2}$. La forme volume associée est $\frac{dx\wedge dy}{y^2}$. Son groupe d'automorphismes directs est encore $PSL_2(\mathbb{R})$. L'action de Γ, bien que discontinue n'est pas libre (parce qu'il y a des points fixes comme i par $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\rho = \frac{-1+i\sqrt{3}}{2}$ par $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$), et on ne peut donc transporter la métrique riemannienne sur X qu'en laissant 2 singularités, en les images de i et ρ, de degré respectifs 2 et 3. Cela n'empêche pas de définir une mesure volume sur X notée μ. En l'∞, on a une 'pointe'.

Les deux géométries ont des comportements différents, mais aussi intimement liés. Les singularités riemanniennes ne se voient pas dans le cas complexe. La pointe qui correspond en géométrie riemannienne à un 'rétrécissement' des distances correspond à enlever un point à la courbe holomorphe compacte $P^1(\mathbb{C})$. L'opérateur de Laplace-Beltrami associé à la métrique riemannienne s'écrit $\Delta = y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$, tandis que $\frac{\partial}{\partial \bar{z}} = \frac{1}{2}(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y})$, donc l'opérateur Δ est 'proportionnel en chaque point' à l'opérateur $\partial\bar{\partial}$. On est souvent amené à calculer des intégrales le long de géodésiques, tandis que l'holomorphie d'une forme différentielle permet de déformer le chemin.

Les formes automorphes (cf plus loin) sur $\Gamma\backslash\mathfrak{H}$ se divisent en deux catégories : les formes modulaires qui sont holomorphes et les formes de Maass, fonctions propres du laplacien qui sont proches de la géométrie riemannienne. Ce n'est donc pas tout à fait un hasard si dans la résolution du théorème, où le volume joue un rôle certain, les formes de Maass soient utilisées.

3 Corps quadratiques

Il y a beaucoup de livres de théorie algébrique des nombres. Pour les corps quadratiques, on peut donner des définitions très explicites ce que je vais m'efforcer de faire dans ce paragraphe, en suivant Don Zagier (cours 2004-2005 à l'Ecole). On peut aussi consulter [Zag81] (en allemand). Le lecteur qui voit ces définitions pour la première fois peut essayer de démontrer les propriétés avant de consulter la littérature.

Un discriminant est un entier D non nul et congru à 0 ou 1 (mod 4). Le discriminant est fondamental si $D = f^2D'$ implique $D = D'$. Les ensembles suivants sont en bijetion canonique :

- Les extensions quadratiques $K/\mathbb{Q}$.
- $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.
- Les discrimants fondamentaux D.
- Les caractères de Dirichlet χ_D réels, c'est à dire à valeurs 1 ou -1.

Les liens sont $K = \mathbb{Q}(\sqrt{D})$, $D = disc(K)$, $\chi_D = \left(\begin{array}{c} D \\ \cdot \end{array}\right)$ symbole de Kronecker, χ_D primitif modulo D. (La construction du caractère χ_D est importante, liée à la loi de réciprocité quadratique).

Un ordre est un anneau qui est un $\mathbb{Z}$-module libre de type fini. Un ordre de K est un sous-anneau qui est un réseau. On a la bijection canonique entre les objets suivants :

- Les ordres O_D des corps quadratiques.
- Les discriminants D.

Le lien est $O_D = \{\frac{a+b\sqrt{D}}{2}, a \equiv bD[2]\}$. En particulier, O_K=$O_{disc(K)}$=ordre maximal de K=anneau des entiers.

Un idéal entier de K est un idéal de O_K non nul. Un idéal fractionnaire de K est un $\mathbb{Z}$-réseau de K qui est un O_K-module. Un idéal engendré par un élément est dit principal. On définit le groupe des classes d'idéaux $Cl(\mathbb{Q}(\sqrt{D}) = Cl(D)$ comme le quotient du groupe des idéaux fractionnaires par le groupe des idéaux principaux. On dit aussi que les idéaux A et λA sont équivalents. Le théorème de Dirichlet affirme que le nombre de classes $h(D) = h(\mathbb{Q}(\sqrt{D}) = |Cl(D)|$ est fini.

Introduisons maintenant les fonctions L des corps quadratiques ainsi que la formule de Dirichlet. La fonction zêta de Dedekind du corps K est définie par $\zeta_K(s) := \sum\limits_{\mathfrak{a} \text{ entier}} N\mathfrak{a}^{-s} = \zeta(s)L(s,\chi_D)$ où $L(s,\chi_D) = \sum\limits_{n=1}^{\infty} \frac{\chi_D(n)}{n^s}$ est la série de Dirichlet attachée au caractère χ_D. La norme peut être définie par $(N\mathfrak{a}) = \mathfrak{a}\bar{\mathfrak{a}}$ ou par $N\mathfrak{a} = [\mathfrak{a} : O_K]$. Pour un idéal principal : $N(\alpha) = N_{K/\mathbb{Q}}\alpha$ ($= |\alpha|^2$ pour $D < 0$). La théorie de Hecke donne le prolongement de ζ_K en une fonction méromorphe de $\mathbb{C}$ avec un unique pôle simple en 1, une équation fonctionnelle et une formule pour le résidu. Dans le cas des corps quadratiques, on peut prolonger $L(s,\chi_D)$ et ζ par la formule de Poisson, et l'expression du résidu porte le nom de formule de Dirichlet :

$$\mathrm{Res}_{s=1}\zeta_K = L(1,\chi_D) = \begin{cases} \frac{\ln \epsilon_D}{\sqrt{D}} h(D) & \text{si } D > 0 \\ \\ \frac{2\pi}{w_D\sqrt{|D|}} h(D) & \text{si } D < 0 \end{cases}$$

où $\epsilon_D = \frac{x_D + y_D\sqrt{D}}{2} > 1$ est l'unité fondamentale définie comme la plus petite solution de l'équation de Pell $x_D^2 - Dy_D^2 = 4$ ou comme générateur du groupe cyclique des unités : $O_K^\times = \{\pm 1\} \times \epsilon_D^{\mathbb{Z}}$; w_D est le nombre de racines de l'unité : $w_{-3} = 6, w_{-4} = 4$ et $w_D = 2$ sinon. La série $L(s,\chi_D)$ est une fonction entière. Pour l'équation fonctionnelle, on note $\delta = 0,1$ la parité de χ_D : $(-1)^\delta = \chi_D(-1) = \mathrm{sgn}\, D$ et $L^*(s) = (\frac{|D|}{\pi})^{\frac{s}{2}}\Gamma(\frac{s+\delta}{2})L(s,\chi_D)$. Alors $L^*(s) = i^{-\delta}\frac{g_{\chi_D}}{\sqrt{|D|}}L^*(1-s)$ où $g_{\chi_D} = \sum\limits_{a (mod D)} \chi_D(a)e^{2i\pi\frac{a}{|D|}}$ est la somme de Gauss, $\sqrt{D}$ si $D > O$, $i\sqrt{|D|}$ si $D < 0$ (que le module soit $\sqrt{|D|}$ est évident et l'argument fut calculé par Gauss).

4 Points de Heegner

A partir de maintenant, on supposera toujours que $\underline{D < 0}$. Pour montrer l'importance des points de Heegner j'ai choisi de donner deux définitions assez différentes.

La plupart des énoncés du paragraphe précédent ont été formulé par Gauss, motivé par le point de vue des polynomes quadratiques à coefficients entiers. Les deux points de vue sont équivalents. Donnons la bijection fondamentale entre le groupe des classes $Cl(D)$ et l'ensemble des classes d'équivalences de polynomes quadratiques à coefficients entiers de discriminant D définis positifs, modulo l'action de $SL_2(\mathbb{Z})$.
$Cl(D) \cong \{Ax^2 + Bxy + Cy^2 \text{ où } A, B, C \in \mathbb{Z}, A > 0, D = B^2 - 4AC\}/SL_2(\mathbb{Z})$.
L'action de Γ sur les polynomes est par composition : $P.\gamma = P \circ \gamma$. La bijection est donnée en associant à un idéal fractionnaire $\mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta$ le polynôme $\frac{N(x\alpha + y\beta)}{N\mathfrak{a}}$. On peut noter que dans cette bijection le membre de gauche est un groupe tandis que l'autre membre est à priori seulement un ensemble. Cette loi de groupe sur les polynômes s'appelle la loi de composition de Gauss. (Très récemment des exemples de bijections de ce type ont été découverts en dimension supérieure.).

En prenant la racine du polynôme qui se trouve dans le demi-plan de Poincaré, on trouve une bijection avec l'ensemble des points de Heegner $He_D = \Gamma\backslash\{\tau \in \mathfrak{H} \text{ tq } A\tau^2 + B\tau + C = 0 \text{ où } B^2 - 4AC = D,\ A, B, C \in \mathbb{Z}\}$ définis dans le préambule. Le nombre de points de Heegner est donc bien aussi le nombre de classes.

Donnons une autre construction plus conceptuelle : X est aussi une variété algébrique qui peut être définie comme espace de modules pour les courbes elliptiques. Les points $\tau \in X$ sont en bijection avec les courbes elliptiques sur $\mathbb{C}$, $(\mathbb{Z}\tau + \mathbb{Z})\backslash\mathbb{C}$. Les points de Heegner correspondent alors aux courbes elliptiques à multiplication complexe par O_D. (En effet avoir multiplication complexe par O_D revient à dire que $\mathbb{Z}\tau + \mathbb{Z}$ est stable par O_D, donc un idéal fractionnaire. De plus l'équivalence des idéaux est identique à une homothétie de réseaux qui donne la même courbe elliptique).

5 Le problème de Gauss

Pour que des points s'équidistribuent, il faut tout d'abord qu'il y en ait beaucoup ! Cette question a été explicitement posée par Gauss dans le language des formes quadratiques :

Conjecture (Problème de Gauss). *Le nombre de classes $h(D)$ tend vers l'infini avec $|D|$.*

Pour $D > 0$, la conjecture n'est pas résolue, et on n'est toujours pas certain qu'il n'y ait qu'un nombre fini de corps quadratiques réels d'anneau d'entiers principal. Cela est dû au terme $\ln \epsilon_D$. Pour $D < 0$, les preuves de ce résultat constituent une avancée majeure dans l'arithmétique du XXieme siècle. J'aurai pu prendre cette histoire comme sujet de ce mémoire, mais je pense qu'elle est déjà parfaitement résumée dans [Oes88]. Citons seulement deux théorèmes majeurs (nous n'utiliserons que le premier pour notre problème) :

Théorème 2 (Siegel, 1935). *Lorsque D tend vers $-\infty$, $\ln h(D) \sim \frac{1}{2}\ln|D|$. De manière équivalente, $h(D) \gg_\epsilon |D|^{\frac{1}{2}-\epsilon}$, pour tout $\epsilon > 0$ (la minoration de h est classique).*

Rappelons que la notation de Vinogradov $\gg$ signifie O. Ainsi, pour tout $\epsilon > 0$, il existe une constante C_ϵ telle que $h(D) > C_\epsilon |D|^{\frac{1}{2}-\epsilon}$. La preuve de ce théorème est très courte et je conseille vivement au lecteur de lire l'article original de Siegel dans [Sie] (bien qu'il soit en allemand).

Pourtant, ce théorème ne résout pas parfaitement le problème de Gauss. Pourquoi ? La constane C_ϵ est 'ineffective' ! En français, cela veut dire que la preuve de Siegel ne donne aucun moyen de trouver C_ϵ, même pour un ϵ fixé (disons 0.4). Il faut lire Siegel pour comprendre pourquoi. Ceci explique l'existence du théorème suivant (la borne est bien plus faible), dont la preuve est un très grand achèvement des mathématiques modernes :

Théorème 3 (Goldfeld et Gross-Zagier, 1985). *Pour tout $\epsilon > 0$, on <u>sait</u> calculer une constante C_ϵ telle que $h(D) > C_\epsilon(\ln|D|)^{1-\epsilon}$ pour tout $D < 0$.*

6 Formes automorphes, références

La théorie des formes automorphes est essentielle dans l'arithmétique moderne et est au coeur de la plupart des travaux du XXième siècle. Dans ce paragraphe, je donne quelques repères bibliographiques. En effet, depuis les fameux travaux de Langlands, la littérature est très abondante mais difficile à lire pour un non spécialiste. D'ailleurs si vous demandez à des gens ce qu'est une forme automorphe, vous aurez autant de définitions que de personnes interrogées. J'espère ainsi éviter au lecteur les difficultés bibliographiques que j'ai rencontrées au début.

Les formes automorphes les plus connues sont les 'formes modulaires'. Les 'formes automorphes sur GL_2' sont formées des 'formes modulaires' et des 'formes de Maass'. Il y a deux formalismes pour traiter des formes automorphes en général.

Le premier, classique, consiste à considérer des fonctions sur le demi-plan de Poincaré invariantes par une action d'un groupe d'automorphie (par exemple $SL_2(\mathbb{Z})$). Pour étudier les formes modulaires, la référence est [Shi]. Pour une étude des formes de Maass, lire [Iwa02].

Le second formalisme se fond dans la 'théorie des représentations'. Il permet de considérer des 'formes automorphes sur G', où G est un groupe algébrique assez général. La question clé est de décomposer l'action régulière par translations à droites d'un groupe G sur sur un espace de fonctions sur G invariantes à gauche par un sous-groupe discret. Les deux livres historiques [GGPS] et [JL70] sont excellents, très longs, mais je pense assez difficiles à lire lorsqu'on ne sait pas où on va, en particulier lorsqu'on connait uniquement le premier formalisme. De plus ils ne traitent que le cas de GL_2. Le livre récent [CKM04] donne en quelques pages les définitions rigoureuses et l'articulation des théorèmes principaux dans le language actuel. Il y a aussi les références précises pour comprendre les preuves ensuite.

Il reste le lien entre les deux formalismes qui est assez négligé dans la littérature, considéré acquis pour la conscience collective. Je trouve pourtant que c'est le point crucial et qu'il mérite d'être clarifié au maximum. Le seul livre que je connais à ce sujet est [Gel75], que je conseille vivement.

7 Formes de Maass, théorème spectral

Les formes de Maass sur $\Gamma\backslash\mathfrak{H} = X$ seront les seuls exemples de formes automorphes considérées dans cet exposé. Ce sont des objets intimement liées à la structure riemannienne de X. On peut voir le théorème spectral comme un théorème d'analyse pure, appartenant au domaine des EDP. Bien que son énoncé soit naturel, sa démonstration est subtile, et s'il s'avère si puissant en pratique c'est sans doute parce que les étapes de sa preuve contiennent déjà des estimées non triviales, surtout en ce qui concerne les séries d'Eisenstein. (Voir [Iwa02] pour un exposé impeccable). Le contenu <u>arithmétique</u> qu'on pense (programme de Langlands) être aussi riche que pour les formes modulaires est encore très méconnu. Ainsi, le théorème spectral assure l'existence de beaucoup de formes de Maass, mais on est incapable d'en construire explicitement (à quelques exceptions qui se comptent sur les doigts de la main).

Une forme de Maass parabolique est une fonction u sur X fonction propre du laplacien qui décroit très vite en l'∞. C'est à dire que $u : \mathfrak{H} \to \mathbb{C}$ vérifie :

1. $u(\gamma z) = u(z)\ \forall z \in \mathfrak{H}, \forall \gamma \in \Gamma$.
2. $-\Delta u = s(1-s)u$ où $s \in \frac{1}{2} + i\mathbb{R}$.
3. une condition de croissance à l'∞ (unique pointe de X).

Une forme de Maass est lisse. On a une notion de développement de Fourier en x. Le spectre de Δ est discret et on note (s_j) l'ensemble des 'paramètres spectraux' comptés avec multiplicités. Les espaces propres sont deux à deux orthogonaux.

D'un autre coté, on va définir les séries d'Eisenstein $E(z,s)$, pour $s \in \mathbb{C}$. Les deux premières conditions, prises indépendament sont très facilement satisfaites. Pour 1., il suffit de prendre une fonction $X \to \mathbb{C}$. Pour 2. on peut prendre y^s, mais qui n'est invariant que par les translations $\gamma \in \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} =: \Gamma_\infty$. Pour concilier les deux, l'idée naturelle est alors de former la série d'Eisenstein :

$$E(s,z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \mathrm{Im}(\gamma z)^s = y^s \sum_{c \wedge d = 1} |cz+d|^{-2s}$$

La série converge absolument pour Re $s > 1$, et à s fixé, la somme vérifie l'automorphie 1. et l'équation 2. Cependant elle a une croissance polynomiale à l'∞ et ne satisfait pas le point 3, ce qui est normal car il n'y a pas de formes de Maass paraboliques de paramètre spectral $s \notin \frac{1}{2} + i\mathbb{R}$.

La théorie des séries d'Eisenstein affirme qu'elles ont un prolongement méromorphe en s à tout le plan complexe, avec une équation fonctionnelle et un unique pôle en 1. Les points 1. et 2. restent satisfaits par un argument de prolongement analytique. On a $\mathrm{Res}_{s=1} E(s,z) = \frac{3}{\pi} = \mu(\Gamma \backslash \mathfrak{H})$ (indépendant de z). Il faut faire attention que $E(s,.)$ n'est jamais dans L^2, même pour Re $s = \frac{1}{2}$ (elle est seulement dans L^1). Les séries d'Eisenstein sont orthogonales aux formes de Maass paraboliques pour tout s.

Théorème 4 (théorème spectral). *L'espace $L^2(\Gamma \backslash \mathfrak{H})$ se décompose en somme directe et intégrale directe orthogonales :*

$$L^2(\Gamma \backslash \mathfrak{H}) = \mathbb{C}\mathbf{1} \oplus \bigoplus_j \mathbb{C}u_j \oplus \int_{\mathbb{R}} \mathbb{C}E(\frac{1}{2} + it, .)dt$$

où u_j est une famille orthonormée de formes de Maass paraboliques.

(La notion d'intégrale directe est délicate et on peut y penser par analogie à la transformée de Fourier qui serait une version continue des séries de Fourier, en écrivant $L^2(\mathbb{R}) = \int_{\mathbb{R}} \mathbb{C}e^{2i\pi tx} dt$).

Voyons maintenant comment appliquer ce théorème à notre problème d'équidistribution initial. Cela demande des principes 'classiques' d'analyse. Ils sont systématiquement négligés dans la littérature car 'techniques'. Voici un moyen propre de les traiter rigoureusement et avec peu de calculs.

Rappelons tout d'abord des faits du cours de probabilités, valables pour X assez régulier (variété par exemple).

Proposition. *Les 8 assertions suivantes sont équivalentes :*

Les points He_D s'équidistribuent dans X pour la mesure μ.

La suite de mesures $\frac{3}{\pi}\mu_D := \frac{1}{h(D)} \sum_{e \in He_D} \delta_e$ converge étroitement vers $\frac{3}{\pi}\mu$.

Pour toute fonction f continue bornée, $\int f d\mu_D$ tend vers $\int f d\mu$.

Pour tout ouvert U de X, liminf $\mu_D(U) \geq \mu(U)$.

Pour tout fermé F de X, limsup $\mu_D(F) \leq \mu(F)$.

Pour tout borélien B dont la frontière est de mesure nulle ($\mu(\partial B) = 0$), $\mu_D(B)$ tend vers $\mu(B)$.

Pour toute fonction f continue bornée, $\int f d\mu_D$ tend vers $\int f d\mu$.

Pour toute fonction f continue à support compact, $\int f d\mu_D$ tend vers $\int f d\mu$.

Dans le cas où $X = \mathbb{R}^d$, on peut aller plus loin et montrer l'équivalence avec la convergence simple de la transformée de Fourier des mesures (thèorème de Levy). Dans le cas où $X = \mathbb{R}$, on peut montrer l'équivalence avec la convergence simple vers la fonction de répartition aux points de continuité. Dans le contexte de l'équidistribution sur $\mathbb{R}/\mathbb{Z}$ le théorème de Lévy correspond aux sommes de Weyl $\sum\limits_n e^{2i\pi k u_n}$. Par extension, on appelle aussi 'sommes de Weyl' ces sommes dans d'autres contextes, c'est à dire pour d'autres espaces X.

Ainsi, pour obtenir nos sommes de Weyl pour $\Gamma\backslash\mathfrak{H}$, on décompose notre fonction f continue à support compact à l'aide du théorème spectral. Le terme principal provient de la fonction constante $\mathbf{1}$ qui donne bien $\frac{3}{\pi}\int_X f$ et il s'agit de majorer les restes. Pour la convergence, on sait ([Iwa02]) que la décomposition spectrale de f converge très vite car f est à support compact. On peut alors appliquer Fubini à condition de contrôler uniformément les coefficients par rapport au paramètre spectral. (ainsi dans le théorème suivant, $\ll_t$ et $\ll_u$ correspondent en fait à $\ll |t|^A$, mais je ne l'ai pas écrit pour ne pas alourdir les notations pour la suite). Il s'agit donc de prouver :

Théorème 5. *Pour $t \in \mathbb{R}$, on a, lorsque $D \to -\infty$:*

$$\frac{1}{h(D)} \sum_{e \in He_D} E(\frac{1}{2} + it, e) \ll_{\epsilon,t} |D|^{-\frac{1}{16}+\epsilon} \to 0$$

Si u est une forme de Maass parabolique, on a :

$$\frac{1}{h(D)} \sum_{e \in He_D} u(e) \ll_{\epsilon,u} |D|^{-\frac{1}{28}+\epsilon} \to 0$$

Les parties 8. et 9. sont consacrées à la preuve du théorème pour les séries d'Eisenstein. Dans la partie 10. on explique la deuxième majoration où les outils sont beaucoup plus élaborés bien que suivant un chemin analogue.

8 Une formule de Hecke

Une difficulté dans la première somme est que les valeurs $E(\frac{1}{2} + it, e)$ ont été obtenues de manière indirecte par prolongement analytique de s. Pourtant, la série E étant très explicite, on va pouvoir 'calculer' chaque valeur. Rappelons (paragraphe 3) que les points de Heegner sont en biection avec le groupe des classes d'idéaux, Cl_K. On note $e_{\mathcal{A}}$ le point associé à la classe $\mathcal{A} \in Cl_K$. On introduit aussi la fonction zêta partielle : $\zeta_K(s) = \sum_{\mathcal{A}\in Cl_K} \zeta_K(s,\mathcal{A})$ avec $\zeta_K(s,\mathcal{A}) = \sum_{\mathfrak{a}\text{entier } \in\mathcal{A}} N\mathfrak{a}^{-s}$. On a la formule classique due à Hecke :

$$E(s, e_{\mathcal{A}}) = \frac{w|D|^{\frac{s}{2}}}{2^{s+1}}\zeta(2s)^{-1}\zeta_K(s,\mathcal{A})$$

La démonstration utilise les formules mentionnées aux paragraphes 3 et 4, et je laisse au lecteur le plaisir de démontrer cette jolie formule. (C'est un parfait exercice pour vérifier qu'on a assimilé les concepts). En sommant sur les classes d'idéaux, on obtient donc :

$$\sum_{e\in He_D} E(s,e) = \frac{w|D|^{\frac{s}{2}}}{2^{s+1}}\zeta(2s)^{-1}\zeta_K(s)$$

Remarque: En prenant le résidu en $s = 1$, on retrouve la formule de Dirichlet.

9 Bornes de sous-convexité, borne de Burgess

Grâce à la formule du paragraphe précédent, on voit qu'il s'agit de majorer la valeur centrale $L(\frac{1}{2} + it, \chi_D)$ en fonction de D ('centrale' car au centre de l'équation fonctionnelle de la fonction L). Soulignons le fait que les valeurs centrales sont les valeurs les 'moins accessibles' d'une fonction L. En effet, le domaine de convergence absolue se situe pour Re $s > 1$ et l'équation fonctionnelle permet d'avoir une expression pour Re $s < 0$. Ce sont aussi les valeurs les plus intéressantes!

Première idée : Par sommation d'Abel, on peut voir que le problème est à peu près équivalent à majorer 'une somme de caractère' $\sum_n \chi(n)$. C'est un problème crucial en théorie analytique des nombres. Citons le très célèbre :

Théorème 6 (Polya-Vinogradov). *Soit χ un caractère de Dirichlet (mod q), non trivial. Alors :*

$$|\sum_{n\in intervalle} \chi(n)| \leq 6\sqrt{q}\ln q$$

Ce qui est très beau dans ce théorème est que la majoration est indépendante de la longueur de l'intervalle de sommation. En calculant, on voit que cela permet de trouver la borne $L(\frac{1}{2}+it,\chi) \ll |t|q^{\frac{1}{2}}$. Avec la formule de Hecke et le théorème de Siegel, on obtient donc (rappelons que χ_D est un caractère primitif modulo $|D| = q$) $\frac{1}{h(D)}\sum_{e\in He_D} E(\frac{1}{2}+it,e) \ll |D|^{\frac{1}{2}+\epsilon}$. On est donc très loin d'avoir montré que l'expression tendait vers 0. Cela est dû au fait que le théorème de Polya-Vinogradov ne donne plus une borne satisfaisante losque la longueur de l'intervalle de sommation est petite.

Deuxième idée : On utilise ce qu'on connait des propriétés analytiques de $L(s,\chi)$. Rappelons le fait suivant d'analyse complexe (application du principe du maximum) :

Théorème 7 (Principe de Phragmèn-Lindelöf). *Soit $L(s)$ une fonction holomorphe dans une bande verticale $\sigma_1 \leq Re\ s \leq \sigma_2$, à croissance modérée $L(s) \ll e^{|s|^A}$.*

Alors les majorations $L(s) \leq (C(1+|t|))^{a_2}$ pour $s = \sigma_2 + it$ et $L(s) \leq (C(1+|t|))^{a_1}$ pour $s = \sigma_1 + it$ impliquent la majoration dans toute la bande $L(s) \leq (C(1+|t|))^{a(\sigma)}$, où a est la fonction affine valant a_1 en σ_1 et a_2 en σ_2.

Ce principe est aussi appelé 'principe de convexité', car en pratique, lorsqu'on a un exposant $a(\sigma)$ pour certaines valeurs de σ, on sait alors qu'on peut étendre a en prenant son enveloppe convexe. Dans la suite, on fera un très léger abus en remplacant le $1+|t|$ par $|t|$, bien que ce ne soit pas parfaitement rigoureux lorsque t s'annule.

Pour notre fonction $L(s,\chi)$, on sait qu'elle converge absolument pour $\sigma > 1$ et on peut prendre $a(\sigma) = 0, C fixe$ pour $\sigma > 1+\epsilon$. En utilisant l'équation fonctionnelle et la formule de Stirling, on voit qu'on peut prendre $a(\sigma) = \frac{1}{2} - \sigma, C = |q|$ pour $\sigma < -\epsilon$. On trouve donc $L(\frac{1}{2}+it,\chi) \ll (|t|q)^{\frac{1}{4}+\epsilon}$, la constante étant uniforme en χ et t. On l'appelle 'borne de convexité'. Cela permet de trouver l'estimation $\frac{1}{h(D)} \sum_{e \in He_D} E(\frac{1}{2}+it, e) \leq |D|^{\epsilon}$. Malheureusement, cette expression ne tend pas vers 0 à cause du $+\epsilon$.

Remarque: On peut améliorer l'argument précédent avec des majorations un peu moins brutales, et montrer que l'on a $\boxed{L(\frac{1}{2}+it,\chi) \ll (|t|q)^{\frac{1}{4}}}$ comme borne de convexité. Cela suffit pas car il reste un ϵ dans le théorème de Siegel.

On a échoué à un ϵ près, et ce phénomène est très courant en théorie des nombres : La borne de convexité est aussi la meilleure borne qui ne résout pas le problème arithmétique !

Lorsqu'on trace la fonction a, on aurait envie de prolonger les deux droites. C'est la conjecture de Lindelöf généralisée.

Conjecture (Lindelöf). *On a $L(\frac{1}{2}+it,\chi) \ll_{\epsilon} (|t|q)^{\epsilon}$.*

Il va sans dire qu'elle est largement suffisante pour résoudre notre problème. Elle est une conséquence de l'hypothèse de Riemann pour les fonction $L(s,\chi)$, bien que les calculs soient assez fastidieux.

troisième idée : On a vu que la borne de convexité s'obtient assez facilement à partir des propriétés analytiques standardes de la fonction L. C'est cela qui est gênant : on n'a pas utilisé la structure arithmétique du caractère χ. Burgess a démontré, dans le cadre des courtes sommes de caractère (première idée), la borne célèbre suivante :

Théorème 8 (Burgess, 1962). *On a la borne suivante, valable uniformément pour tout caratère primitif modulo q et tout $t \in \mathbb{R}$:*

$$L(\frac{1}{2}+it,\chi) \ll_{\epsilon} |t|q^{\frac{3}{16}+\epsilon}$$

On peut remarquer que la borne est légèrement moins bonne en $|t|$, mais notre problème avait justement besoin de la majoration en fonction du niveau $q = |D|$. On appelle ce type de bornes qui améliorent l'exposant de la borne de convexité, 'une borne de sous-convexité'. La démonstration est difficile et utilise les conjectures de Weil pour les courbes algébriques. Elle achève la démonstration de la première partie du théorème.

Donnons quelques remarques générales sur les bornes de sous-convexité. Tout d'abord terminologique : par analogie, les majorations de quantités qu'on obtient avec des moyens 'rudimentaires' sont aussi appelées bornes de convexité, même si le principe de Phragmèn-Lindelöf n'intervient plus. Nous verrons dans le paragraphe suivant l'exemple des coefficients de Fourier d'une forme de Maass. (ici, le 'moyen rudimentaire' est tout de même la borne de Weil pour les sommes de Kloosterman !). Depuis relativement peu de temps, on s'est rendu compte que non seulement les bornes de sous-convexité résolvent beaucoup de problèmes arithmétiques, mais on est aussi parvenu à en démontrer dans une foule de cas. La démonstration est toujours délicate et intéressante. On peut certes dire que ces bornes sont conséquences de la conjonction de l'hypothèse de Riemann généralisée, la conjecture de Ramanujan-Peterson généralisée et des correspondances de Langlands. Seulement, on est loin à ce jour de comprendre ces grandes conjectures, et les démonstrations de conséquences non triviales donnent une idée de leurs difficultés ; on peut aussi espérer que les techniques développées dans les preuves soient des clés de leur résolution.

10 Le cas parabolique

La majoration pour les formes de Maass paraboliques est beaucoup plus délicate. Elle suit tout de même un shéma analogue.

La formule de Dirichlet est remplacée par un 'Maass' lift' pris dans un cas très particulier. L'article original de Maass, [Maa59] a été oublié pendant longtemps, sans doute à cause de la difficulté des calculs. Toutes ces formules sont des exemples de 'périodes de formes automorphes', dont la théorie est encore en développement (voir les cours de Don Zagier au collège de France). Sans donner de détails sur les travaux de Maass, repris ensuite par d'autres mathématiciens, on peut néanmoins écrire la formule qui ressemblera à un don du ciel :

Théorème 9 (Maass 1959). *Soit u une forme de Maass parabolique sur $SL_2(\mathbb{Z})$. Alors la fonction*

$$\begin{aligned} v(z) &= \sum_{\substack{D\,discriminant \\ D<0}} |D|^{-\frac{3}{4}} \left(\sum_{e \in He_D} {}' u(e) \right) W(|D|y) e^{2i\pi Dx} + \\ &+ c \sum_{\substack{D\,discriminant \\ D>0}} |D|^{-\frac{3}{4}} \left(\sum_{\mathcal{A} \in Cl(D)} {}' \int_{\gamma_{\mathcal{A}}} u ds \right) W(|D|y) e^{2i\pi Dx} \end{aligned}$$

est une forme de Maass parabolique de poids $\frac{1}{2}$ pour $\Gamma_0(4)$.

Les sommes sont sur tous les discrimants, bien qu'on ait défini les objets que dans le cas D fondamental ; c est une constante simple ; W est une fonction Bessel ;

$\sum'$ désigne qu'il faut pondérer très légérement les coefficients de la somme ; $\gamma_{\mathcal{A}}$ est une géodésique fermée de X associée à $\mathcal{A}$; $\Gamma_0(4)$ est un sous-groupe d'indice 6 de $SL_2(\mathbb{Z})$; poids $\frac{1}{2}$ signifie qu'on a un facteur d'automorphie $(cz+d)^{\frac{1}{2}}$.

Remarque: Si le lecteur trouve une preuve de cet énoncé sans la théorie générale, faites m'en part, ça m'intéresse beaucoup.

On doit donc donc maintenant majorer les coefficients de Fourier de la forme automorphe $v = \sum_n a_n W(|n|y) e^{2i\pi nx}$. C'est encore un problème classique de théorie analytique des nombres. On a la 'borne triviale' $a_n \ll_\epsilon |n|^\epsilon$ qui découle du calcul de la norme L^2. Avec plus de calculs et en utilisant la borne de Weil pour lers sommes de Kloosterman, on peut montrer $a_n \ll_\epsilon |n|^{-\frac{1}{4}+\epsilon}$. C'est la borne de convexité. Elle échoue à ϵ près de conclure notre problème. Une borne de sous-convexité a été établie par Duke à partir des travaux d'Iwaniec qui avait trouvé une borne de sous-convexité dans le cas plus usuel des formes modulaires de poids demi-entier.

Théorème 10 (Duke-Iwaniec). *Si $v = \sum_n a_n W(|n|y) e^{2i\pi nx}$ est une forme de Maass de poids $\frac{1}{2}$ sur un sous-groupe de congruence, on a :*

$$a_n \ll_\epsilon |n|^{-\frac{2}{7}+\epsilon}$$

Cela conclut la preuve du théorème 5, et du problème.

11 Remarques sur les deux autres preuves

La première preuve historique est due à Linnik dans les années 50. Il y a d'ailleurs trois problèmes de Linnik, celui de ce mémoire étant le deuxième. La preuve de Linnik utilise de la théorie ergodique, mais n'obtient le théorème d'équidistribution que sous la condition que les D satisfassent à $\left(\begin{array}{c} D \\ p \end{array}\right) = 1$, où p est un nombre premier impair fixé. La preuve est très ingénieuse, écrite dans un language ancien et des travaux sont en cours pour la comprendre en profondeur. Elle est très différente du cheminement suivi par Duke et se fonde sur une théorie ergodique développée par Linnik. Il faut souligner que Linnik avait posé et résolu les trois problèmes sous cette condition plus faible et que ses travaux profonds n'ont pas été appréciés à leur juste valeur pendant très longtemps.

Une autre preuve suit le même chemin que celle de Duke. Cependant la formule de Maass (paragraphe précédent) est remplacée par une autre formule magique due à Waldspurger, un peu mieux comprise et plus générale. Par contre la borne de sous-convexité est plus délicate et due à W.Duke, J. Friedlander et H.Iwaniec.

Références

[Duk88] W. Duke. Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92, 1988.

[Iwa87] Henryk Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Invent. Math.*, 87, 1987.

[Maa59] Hans Maass. Über die räumliche Verteilung der Punkte in Gittern mit indefiniter Metrik. *Math. Ann.*, 138, 1959.

Théorie analytique des nombres

[Ten] Tennenbaum. *Introduction à la théorie analytique et probabiliste des nombres.*

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

Théorie algébrique des nombres

[Zag81] D. B. Zagier. *Zetafunktionen und quadratische Körper*. 1981. Eine Einführung in die höhere Zahlentheorie. Hochschultext. [University Text].

[Wei] Weil. A *Basic number theory.*

Formes automorphes

[Shi] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions.*

[Iwa02] Henryk Iwaniec. *Spectral methods of automorphic forms*, volume 53 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 2002.

[GGPS] I. M. Gelfand, M. I. Graev, and I. I. Pyatetskii-Shapiro. *Representation theory and automorphic functions.*

[JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Springer-Verlag, Berlin, 1970. Lecture Notes in Mathematics, Vol. 114.

[CKM04] James W. Cogdell, Henry H. Kim, and M. Ram Murty. *Lectures on automorphic L-functions*, volume 20 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 2004.

[Gel75] Stephen S. Gelbart. *Automorphic forms on adèle groups*. Princeton University Press, Princeton, N.J., 1975. Annals of Mathematics Studies, No. 83.

[Kat92] Svetlana Katok. *Fuchsian groups*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

Formes automorphes moins classiques

Formes de Jacobi :

[EZ85] Martin Eichler and Don Zagier. *The theory of Jacobi forms*, volume 55 of *Progress in Mathematics*. Birkhäuser Boston Inc., 1985.

Formes modulaires de poids demi entier :

[Shi73] Goro Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97, 1973.

Fonctions théta de Siegel :

[Sie51] Carl Ludwig Siegel. Indefinite quadratische Formen und Funktionentheorie. I. *Math. Ann.*, 124, 1951.

[Zag] Don Zagier. Les séries thétas. Cours au collège de France 2004-2005.

Problème de Gauss, zéro de Siegel

[Sie] *Mathematische Werke, 21.Uber die Classenzahl quadratischer Zahlkorper*, volume 1.

[Oes88] J. Oesterlé. Le problème de Gauss sur le nombre de classes. *Enseign. Math. (2)*, 34, 1988.

[Gol85] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13, 1985.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84, 1986.