Mémoire L3 : Modularité des courbes elliptiques

Christopher-Lloyd Simon

29 juin 2016

Résumé

Ce texte résume une partie des travaux que j'ai effectuée pendant mon stage de L3 sous la direction de Jean-Pierre Wintenberger à l'IRMA de Strasbourg et qui avait pour objectif de me faire découvrir, à travers l'étude d'un exemple particulier, le lien entre les formes modulaires et certaines courbes elliptiques. Il s'inscrit pour moi dans la continuité du groupe de lecture animé par M. Pantchichkine autour de [4].

Divers objets arithmétiques et géométriques tels que les formes modulaires, les caractères d'un réseau, les modules quadratiques, les courbes elliptiques ou encore les représentations galoisiennes, donnent lieu à la définition de fonctions L et chaque construction renseigne naturellement sur certaines propriétés qu'elles vérifient : tantôt une factorisation en produit eulérien, tantôt une équation fonctionnelle avec un prolongement méromorphe, etc. L'égalité entre des séries de provenance différentes permet donc de transporter des informations d'un type de structure à l'autre en remontant la construction et ce sont ces relations entre séries L qui on mené Andrew Wiles à prouver le dernier théorème de Fermat ou encore Robert Langlands à formuler son tissu de conjectures. Je me sers ici d'un cas particulier comme fil directeur pour illustrer ces liens. La tonalité employé est celle de l'exposition, destinée à partager les diverses notions rencontrées au cours de mon expérience, les références citées en donnent des constructions rigoureuses.

1 Formes Modulaires et opérateurs de Hecke

1.1 Formes modulaires comme fonction de réseaux

Il est classique d'introduire la notion de forme modulaire comme celle d'une fonction holomorphe sur le demi-plan de Poincaré invariante sous une action qui peut sembler à priori obscure de certains sous-groupes de congruence du groupe modulaire $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Il y a pourtant plusieurs façons naturelles de les introduire qui motivent d'avantage les variations étudiées par la suite. L'une consiste à regarder les différentielles méromorphes définies sur la courbe modulaire $X(\Gamma)$(cf. [2] chap. 2), que l'on peut voir comme le quotient

du disque de Poincaré sous l'action de Γ. De manière plus élémentaire et géométrique encore, on peut considérer les fonctions F homogènes de poids k définies l'espace des sous groupes discrets (des réseaux) de $\mathbb{C}$ c'est à dire telles que pour tout complexe non nul λ et réseau Λ on ait : $F(\lambda\Lambda) = \lambda^{-k}F(\Lambda)$. Si $\omega = (\omega_1, \quad \omega_2)$ est un vecteur à composantes complexes avec $\omega_1/\omega_2 \in \mathbb{H}$, on pose $\Lambda_\omega = \omega_1\mathbb{Z}+\omega_2\mathbb{Z}$ et si $z \in \mathbb{H}$, Λ_z est le réseau engendré par z et 1. On peut alors associer à F les fonctions $\tilde{F}(\omega) = F(\Lambda_\omega)$et $f(z) = F(\Lambda_z)$. Deux bases dont la matrice de passage appartient au groupe modulaire définissent le même réseau et réciproquement. Par conséquent les fonctions de réseaux homogènes de poids k sont en bijection avec les $\tilde{F}$ homogènes qui sont en plus invariantes par changement de base ainsi qu'avec les f qui vérifient (sous l'action par transformations de Möbius) :

$$f(\gamma z) = (cz + d)^k f(z) \text{ pour toute matrice } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma \tag{1.1}$$

Il est désormais facile d'introduire des conditions d'holomorphie (ce qu'on aurait pu faire avant en considérant une structure riemannienne sur l'espace des réseaux) et on dit que f est une *forme modulaire* si elle est holomorphe sur $\mathbb{H}$ ainsi qu'en l'infini, ce qui signifie que son développement $f(q) = \sum a_n(f)\, q^n$ en la variable $q = e^{2i\pi z}$ est holomorphe à l'origine (f est 1-périodique d'après 1.1 avec $\gamma : z \mapsto z+1$). Si de plus $a_0(f) = 0$ alors la forme est dite *parabolique*. Les espaces $M_k(\Gamma)$et $S_k(\Gamma)$ des formes modulaires et paraboliques de poids k sont de dimension finis le fait que ces dimensions soient assez petites pour certains poids permet de découvrir des identités spectaculaires entre des expressions de nature arithmétique apparaissant dans les coefficients de Fourier. Une famille d'exemples importante de formes modulaires est donnée par les séries d'Eisenstein pour $k > 2$ pair :

$$G_k(\Gamma) = \sum_{\gamma\in\Gamma}{}' \gamma^{-k} = 2\zeta(k)\left(1 - \frac{2k}{B_k}\cdot\sum_{n\geqslant 1}\sigma_{k-1}(n)q^n\right)$$

Le prime signifie souvent que l'on somme sur un ensemble implicitement modifié, ici sur les éléments non nuls du réseau. ζ est la fonction de Riemann, B_k sont les nombres de Bernoulli, et $\sigma_k(n)$ la somme des puissances $k^{\text{ièmes}}$ des diviseurs de n.

Si désormais $N > 0$ est un entier et que l'on s'intéresse aux fonctions homogènes sur des espaces de réseaux munis d'une information supplémentaire de N-torsion (appelés espaces de module car on quotiente les vecteurs de $\mathbb{C}^2$ par l'action d'un groupe), alors les fonctions définies sur le demi-plan correspondantes seront modulaires pour des sous-groupes de Γ (ie. vérifieront 1.1 avec Γ remplacé par Γ').

Points de l'espace des modules	F homogène de poids k, $\tilde{F}$, f	Sous-groupe de congruence Γ'de Γ
un réseau $\Lambda \subset \mathbb{C}$	$F(\lambda\Lambda) = \lambda^{-k}F(\Lambda)$ $\tilde{F}(\omega) = F(\Lambda_\omega)$ $f(z) = \tilde{F}(z,1)$	$\Gamma = SL_2(\mathbb{Z})$ $M_k(\Gamma)$, $S_k(\Gamma)$
(Λ, S) réseau muni d'un sous-groupe cyclique d'ordre N du quotient $\mathbb{C}/\Lambda$	$F(\lambda\Lambda, \lambda S) = \lambda^{-k}F(\Lambda, S)$ $\tilde{F}(\omega) = F\left(\Lambda_\omega, \mathbb{Z}\frac{\omega_2}{N}\right)$ $f(z) = \tilde{F}(z,1)$	$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \star & \star \\ 0 & \star \end{bmatrix} \pmod N \right\}$ $M_k(\Gamma_0(N))$, $S_k(\Gamma_0(N))$
(Λ, t) réseau muni d'un point d'ordre N du quotient $\mathbb{C}/\Lambda$.	$F(\lambda\Lambda, \lambda t) = \lambda^{-k}F(\Lambda, t)$ $\tilde{F}(\omega) = F\left(\Lambda_\omega, \frac{\omega_2}{N}\right)$ $f(z) = \tilde{F}(z,1)$	$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & \star \\ 0 & 1 \end{bmatrix} \pmod N \right\}$ $M_k(\Gamma_1(N))$, $S_k(\Gamma_1(N))$
$(\Lambda, \{t, u\})$ réseau muni d'une paire génératrice du sous-groupe de N-torsion du quotient $\mathbb{C}/\Lambda$.	$F(\lambda\Lambda, \lambda\{t,u\}) = \lambda^{-k}F(\Lambda, \{t,u\})$ $\tilde{F}(\omega) = F\left(\Lambda_\omega, \left\{\frac{\omega_1}{N}, \frac{\omega_2}{N}\right\}\right)$ $f(z) = \tilde{F}(z,1)$	$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N \right\}$ $M_k(\Gamma(N))$, $S_k(\Gamma(N))$

Pour qu'une fonction modulaire soit une forme modulaire, il faut ajouter les conditions d'holomorphie sur $\mathbb{H}$ ainsi qu'au voisinage des *pointes* (avec annulation si paraboliques), c'est à dire des classes de points de $\mathbb{Q}\cup\{\infty\}$ modulo l'action du *sous-groupe de congruence* en question, qui par définition est un sous-groupe de Γ contenant $\Gamma(N)$ (ces détails techniques sont traités dans [2] et [7]). Ce sont précisément les conditions requises pour que les formes modulaires préservent leur bonne interprétation en tant que différentielles méromorphes sur les espaces de modules (des surfaces de Riemann compactes) et qui par ailleurs restreignent les dimensions des espaces de formes dont le calcul repose essentiellement sur les formules de Riemann-Hurwitz et de Riemann-Roch.

1.2 Opérateurs de Hecke comme correspondances sur l'espace des modules

L'algèbre de Hecke est une famille d'opérateurs linéaires agissant sur les espaces de formes modulaires. Afin de poursuivre dans la veine géométrique, on se restreint au sous-groupe $\Gamma_1(N)$ et les construits à partir d'une action sur le $\mathbb{Q}$-espace vectoriel ayant pour base l'espace des modules $X_1(N)$ associé : $\mathscr{L} = \bigoplus \mathbb{Q} e_{\Lambda,t}$. On définit trois types d'opérateurs linéaires sur cet espace par leurs valeurs sur cette base :

$\forall n \in \mathbb{N}^*$, $T_n\left(e_{\Lambda,t}\right) = \frac{1}{n}\sum e_{\Lambda',t'}$ (la somme étant sur les $(\Lambda', t') \in X_1(N)$ tels que $[\Lambda' : \Lambda] = n$).

$\forall n \in \mathbb{N}^*$, $n \wedge N = 1$, $T_{n,n}\left(e_{\Lambda,t}\right) = \frac{1}{n^2} e_{1/n\Lambda',t'}$ (la primalité assure que t' reste d'ordre N)

$\forall d \in \mathbb{Z}$, $d \wedge N = 1$, $\langle d\rangle\, e_{\Lambda,t} = e_{\Lambda,dt}$ (idem pour dt)

On tire immédiatement les égalités : $T_{n_1,n_1}T_{n_2,n_2} = T_{n_1n_2,n_1n_2}$ et $T_{n,n}T_m = T_mT_{n,n}$ et la commutativité de *l'algèbre de Hecke* $\mathscr{H}$ (tous ces opérateurs) se déduit de la

Proposition 1. *La structure des sous-groupes d'un réseau du plan fournit les relations :*

Si $m \wedge n = 1$, *alors* $T_mT_n = T_{mn}$ *et commutent donc.*

Si $p \mid N$ *est premier, alors* $T_{p^l} = T_p^l$.

Si $p \nmid N$ *est premier et* $l \geqslant 2$, *alors* $T_{p^l} = T_{p^{l-1}}T_p - pT_{p^{l-2}}T_{p,p}$

Cela équivaut essentiellement à la formule (voir [7] pour le sens précis des variables n^{-s}) :

$$\sum_{n\geqslant 1} T_n n^{-s} = \prod_{p\mid N} \frac{1}{1-T_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-T_p p^{-s}+T_{p,p}p^{1-2s}}$$

On peut désormais faire opérer$(T\colon e_P \mapsto \sum a_n e_{P_n}) \in \mathscr{H}$ contre les fonctions F définies sur notre espace de modules par $TF(e_P) = \sum a_n F(P_n)$et s'en déduit naturellement une action (linéaire) de l'algèbre de Hecke sur l'espace vectoriel $M_k(\Gamma_1(N))$ (il s'avère en effet que le poids et les conditions d'holomorphies ou d'annulation aux pointes sont préservées).

Si χ est un caractère modulo N, et que l'on dénote par $M_k(N,\chi)$ l'espace des formes $\Gamma_1(N)$-modulaires obtenues à partir d'un fonction de réseaux F vérifiant pour tout $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ la relation $\langle d\rangle F = \chi(d)F$ (autrement dit, $F(\Lambda, dt) = \chi(d)F(\Lambda,t)$), alors d'après des résultats généraux en représentation des groupes abéliens finis, on a $M_k(\Gamma_1(N)) = \bigoplus M_k(N,\chi)$ (idem en remplaçant M par S). Cette décomposition est préservée par tous les opérateurs de Hecke et vus comme agissant sur un $M_k(N,\chi)$ fixé, ils vérifient l'identité formelle :

$$\sum_{n\geqslant 1} T_n n^{-s} = \prod_p \frac{1}{1-T_p p^{-s}+\chi(p)\,p^{k-1-2s}} \tag{1.2}$$

1.3 Série L d'une fonction propre de l'algèbre de Hecke

Cette relation est la clé de voute qui relie les propriétés arithmétiques des coefficients de Fourier d'une forme modulaire avec les lois régissant sa série L. Toute forme $f \in M_k(\Gamma_1(N))$ admet un développement en la variable q ($\mathrm{car}(\gamma\colon z \mapsto z+1) \in \Gamma(N)$) et si l'on note a_n ses coefficients de Fourier on peut définir la série L associée par l'expression $L(f,s) = \sum_{n\geqslant 1} a_n n^{-s}$ qui converge lorsque $\Re s$ est plus grand qu'une fonction linéaire de k (elle découle d'un lemme dû à Hecke estimant les a_n, voir par exemple [4] chap. VII, 4.3). L'identité 1.2 permet d'exprimer les coefficients du développement $T_mf = \sum_{n\geqslant 0} b_n q^n$ en fonction de ceux de $f \in M_k(N,\chi)$ par la formule :

$$b_n = \sum_{d\mid m\wedge n} \chi(d) d^{k-1} a_{mn/d^2}$$

et d'en déduire qui si f est une fonction propre normalisée (ie. $a_1 = 1$) de l'algèbre de Hecke, alors les valeurs propres pour les T_m sont les a_m. En faisant agir chacun des membres de 1.2 sur f on en déduit la

Proposition 2. *La série* L *d'une fonction propre normalisée* $f \in M_k(N, \chi)$ *pour l'algèbre de Hecke admet la factorisation en produit eulérien :*

$$\sum_{n \geqslant 1} a_n n^{-s} = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p)\, p^{k-1-2s}}$$

Ses coefficients vérifient donc pour $m \wedge n = 1$ *et* $l \geqslant 2$ *les relations :*
$a_{mn} = a_m a_n$
$a_{p^l} = a_{p^{l-1}} a_p - \chi(p)\, p^{k-1} a_{p^{l-2}}$

On voit donc qu'à une forme modulaire f on peut associer une une série L et qu'il existe un lien étroit entre les équations fonctionelles vérifiées par f (être fonction propre de l'algèbre de Hecke) et les propréiétés de sa série L ou, ce qui revient au même, des relations arithmétiques existant entre les coefficients de son développement de Fourier. Cependant écrire les a_n sous forme de série L permet d'exploiter les outils de l'analyse complexe et par exemple de la prolonger méromorphiquement au plan. Ceci permet ensuite de considérer ses valeurs en des points particuliers, dont l'étude est au coeur de la théorie des courbes elliptiques pourvu que cette série L soient aussi associée à un telle courbe : le véritable problème est de savoir quand est-ce qu'une série L obtenue par la voie des courbes elliptiques provient en fait d'une forme modulaire, autrement dit qu'elle est une *courbe elliptique modulaire*. Une classe de courbes (dites à multiplication complexe) pour laquelle la réponse est bien connue provient des extensions quadratiques imaginaires du corps de rationels et des lois de réciprocité qui en découlent.

2 Loi de réciprocité et série de Dirichlet d'un caractère cubique

2.1 Structure de l'anneau $\mathbb{Z}[\mu_3]$, caractère cubique et loi de réciprocité

Si $\left(\frac{\cdot}{p}\right)$désigne le symbole de Legendre d'un nombre premier $p \neq 2$ et si p, q sont des premiers distincts impairs, la loi de réciprocité quadratique s'énonce : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\epsilon(p).\epsilon(q)}$ où $\epsilon(a) \equiv \frac{a-1}{2} \pmod 2$. Il existe diverses loi de réciprocité et celle qui nous intéresse ici est la loi cubique. On peut dresser une analogie entre l'arithmétique des anneaux $\mathbb{Z}[i]$ et $A = \mathbb{Z}[\mu_3]$ des entiers algébriques des corps de nombres $\mathbb{Q}[\sqrt{-1}]$ et $\mathbb{Q}[\sqrt{-3}]$, tout deux des extensions cyclotomiques et quadratiques de $\mathbb{Q}$.

Propriétés	$\mathbb{Z}[i]$	$\mathbb{Z}[\mu_3]$
Réseau	carré	triangulaire
Forme quadratique $N(a+b\mu_n)$	a^2+b^2	a^2-ab+b^2
Inversibles $N^{-1}\{1\}$	$\mathbb{U}_4$	$\mathbb{U}_6$
Idéaux premiers (tous principaux), leurs générateurs s'obtiennent en factorisant les premiers de $\mathbb{Z}$	$q \equiv 3 \pmod 4$ est inerte, $Nq = q^2$	$q \equiv 2 \pmod 3$ est inerte, $Nq = q^2$
	$p \equiv 1 \pmod 4$ se décompose : $p = \pi\overline{\pi} = N\pi = a^2+b^2$	$p \equiv 1 \pmod 3$ se décompose : $p = \pi\overline{\pi} = N\pi = a^2-ab+b^2$
	2 ramifie : $\pi = 1+i$, $N\pi = 2$, $(2) = -i(\pi)^2$	3 ramifie : $\pi = 2+\mu_3$, $N\pi = 3$, $(3) = -\mu_3(\pi)^2$
Loi de reciprocité	quadratique	cubique

On construit désormais *le* caractère cubique modulo N de l'anneau A, la présentation suit celle de [5]. Soit $\alpha \in A$ et π premier de A qui ne divise pas α. Le quotient $A/\pi A$ est un corps de cardinal $N\pi$ (le nombre d'éléments dans un domaine fondamental du réseau A sous l'action de πA, on pourra consulter [6] pour un point de vue géométrique sur les extensions quadratiques), et on a donc $\alpha^{N\pi-1} \equiv 1 \pmod \pi$. Si $N\pi \neq 3$ alors 1, μ_3 et μ_3^2 sont distincts modulo π car la différence de deux d'entre eux qui est de norme 3 et $N\pi \mid 3$ est exclu, ainsi $3 \mid N\pi - 1$. En factorisant $\alpha^{N\pi-1} - 1 = \left(\alpha^{N\pi-1/3} - 1\right)\left(\alpha^{N\pi-1/3} - \mu_3\right)\left(\alpha^{N\pi-1/3} - \mu_3^2\right)$, on en déduit par intégrité du quotient $A/\pi A$ qu'il existe un $k \in \mathbb{Z}/3\mathbb{Z}$ tel que $\alpha^{N\pi-1/3} \equiv \mu_3^k \pmod \pi$ et l'argument précédent montre qu'il est unique. On peut donc définir un *caractère cubique* $\left(\frac{\cdot}{\pi}\right)_3$ modulo π (c'est à dire un élément d'ordre trois dans le dual de $(A/\pi A)^\times$), et l'étendre à A tout entier par les conditions :

$$\left(\frac{\cdot}{\pi}\right)_3 \in \left\{0, 1, \mu_3, \mu_3^2\right\}$$
$$\alpha^{N\pi-1/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod \pi$$

Le symbole employé est destinée à rappeler celui de Legendre mais comme ce paragraphe ne concerne que la loi cubique on adoptera la notation plus légère χ_π. Remarquons que $\chi_\pi(\alpha) = 1$ équivaut toujours de manière analogue au cas quadratique, au fait que α est un résidu cubique modulo π autrement dit que l'équation $x^3 \equiv \alpha \pmod{\{\}\pi}$ admet des solutions. Afin de pouvoir donner une version propre de la loi de réciprocité il convient de remarquer que parmi les associés de π, il en existe un unique qui soit congru à 2 modulo

3 et on le qualifie alors de primaire. Pour s'en convaincre on pourra dessiner le réseau A, et distinguer selon que l'idéal engendré par π soit inclu dans $\mathbb{Z}$ ou non.

Théorème 3. *Si π_1 et π_2 sont des nombres primaires distincts, alors :*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

2.2 Série L pour le caractère cubique

Forts de ce théorème, pour $d \in \mathbb{Z}_+$ sans facteur cubique on peut désormais construire comme suggéré fin du 4.11 de [2] et selon la méthode employée dans [4] (chap. VI proposition 5) dans l'analogue quadratique, un unique caractère cubique χ modulo $N = 3\prod_{p|d} p$ dont le prolongement à A est trivial sur $A^\times$ ainsi que sur les $p \mid N$, et tel que si $\pi\overline{\pi} = p \nmid N$, alors $\chi(\pi) = 1$ équivaut à d est un résidu cubique modulo p. Une fois χ construit, essentiellement à partir de l'analogue cubique du symbole de Jacobi modulo N, on peut définir la *série* L *de Hecke* de ce caractère (analogue des séries L de Dirichlet sur un anneau d'entiers quelconque) par la formule (qui converge si $\Re s > 3/2$) :

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})\,N\mathfrak{p}^{-s}} \tag{2.1}$$

La somme porte sur tous les idéaux non nuls de A et le produit sur ses idéaux premiers. En regroupant les termes selon leur norme dans la somme et en choisissant un système de représentants $S = \{\pi_p, \overline{\pi}_p : p \equiv 1 \pmod 3\} \cup \{\pi_q : q \equiv 2 \pmod 3\} \cup \left\{\pi_3 = \sqrt{-3}\right\}$ pour réarranger le produit on obtient les formes plus explicites :

$$L(s,\chi) = \sum_{n>0} \frac{a_n(C)}{n^s} = \prod_{p} L_p(s,\chi)^{-1}$$

où $a_m(C) = \frac{1}{6}\sum_{Nn=m} \chi(n)\, n^{-s}$est aussi le nombre de solutions à$C : x^3 \equiv d \pmod m$ lorsque m est premier : $a_p(C) = \begin{cases} 2 & p \equiv 1 \pmod 3 \text{ et } d \text{ résidu non nul } \pmod p \\ 0 & p \equiv 1 \pmod 3 \text{ et } d \text{ non résidu } \pmod p \\ -1 & p = 2 \pmod 3 \text{ ou } p \mid 3d \end{cases}$, et pour p premier de $\mathbb{Z}$:

$$L_p(s,\chi) = \begin{cases} 1 - (\chi\pi_p + \chi\overline{\pi}_p)\,p^{-s} + \chi(p)\,p^{-2s} & \text{si } p \equiv 1 \pmod 3 \\ 1 - \chi(q)\,q^{-s} & \text{si } p = q \equiv 2 \pmod 3 \\ 1 - \chi\left(\sqrt{-3}\right)3^{-s} & \text{si } p = 3 \end{cases}$$

En résumé, la recherche de résidus cubiques modulo les entiers (solutions de $C : x^3 \equiv d \pmod n$) mène naturellement (on veut factoriser) à étudier la loi de réciprocité dans $\mathbb{Z}[\mu_3]$.

Ceci conduit à définir un caractère modulaire dont la série de Hecke associée hérite certaines propriétés : factorisation en produit eulérien, formule explicite pour ses coefficients (remarquons que les valeurs $a_p(C)$ aux entiers premiers déterminent toutes les autres en développant le produit eulérien, cette idée sera réutilisée par la suite). Il se trouve, comme annoncé en fin de section 1, que cette série L est en fait associée à une forme modulaire d'un type particulier : une série thêta de Hecke. Les séries thêta vérifient des équations fonctionelles qui se traduisent en des relations de symétrie pour leurs fonctions L permettant de les prolonger méromorphiquement. On a donc à présent rencontré deux des trois protagonistes principaux dans notre exploration des séries L à savoir les formes modulaires et les extensions quadratiques imaginaires. Le lien étant donné par les séries thêta que nous étudions à présent.

3 Série thêta d'une module quadratique

3.1 Équation fonctionnelle et modularité de la série thêta

Si $\mathfrak{m}$ est un idéal de l'anneau A des entiers d'une extension quadratique imaginaire, on appelle *Grössencharacter* un morphisme χ du groupe $J(\mathfrak{m})$ des idéaux fractionnaires premiers à $\mathfrak{m}$ dans $\mathbb{C}^*$ et on lui associe sa *série thêta de Hecke* :

$$\theta_\chi(z) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})\, q^{N(\mathfrak{a})}$$

La théorie des séries thêta permet de montrer que $\theta_\chi(z) \in M_1(DN(\mathfrak{m}), \psi)$ où D est la valeur absolue du discriminant de l'extension et ψ est une torsion de χ par un caractère linéaire. L'ingrédient principal est l'obtention d'une équation fonctionnelle vérifiée par la série thêta en appliquant la formule de Poisson au réseau A (cf. [7] chapitre II.5 ou [2] proposition 4.10.1 et paragraphe 4.11). On expose les techniques employées et le genre d'équations trouvées dans le cas de la dimension 1 au paragraphe suivant. Le fait que cette série thêta, dont on sait désormais qu'elle est modulaire, possède une série L se factorisant en produit eulérien (2.1) implique d'après la proposition 2 que c'est une fonction propre pour l'algèbre de Hecke et donc que ses coefficients satisfont les relations de récurrence correspondantes.

Dans l'exemple du paragraphe précédent l'anneau est principal donc les deux notions de caractères coïncident, et on obtient en regroupant les termes, $\theta_\chi(z) = \sum_{n\geqslant 0} a_n(\theta_\chi)\, q^n$ où les $a_m(\theta_\chi)$ ne sont en fait rien d'autre que les $a_n(C)$. Le discriminant vaut -3 tandis que le caractère ψ est la torsion de χ par le symbole de Legendre $\left(\frac{\cdot}{3}\right)$ ce qui permet d'effectuer le calcul explicite des coefficients en utilisant les relations de récurrence.

3.2 Équation fonctionnelle et prolongement méromorphe de sa série L

On illustre dans cette partie les méthodes générales utilisées pour établir l'équation fonctionnelle d'une série thêta, celle de sa série L associée ainsi que le prolongement analytique de cette dernière sur le cas plus parlant de la dimension 1 : $\vartheta(t) = \sum_{n\in\mathbb{Z}} q^{\frac{1}{2}n^2}$ (où $q = e^{2i\pi t}$). On commence par appliquer la formule de Poisson à la somme de gaussiennes $\Theta(t) = \vartheta(it) = \sum_{n\in\mathbb{Z}} e^{-\pi t n^2}$ en vue d'obtenir l'équation-thêta :

$$\Theta(t) = t^{-\frac{1}{2}}\Theta\left(-\frac{1}{t}\right) \tag{3.1}$$

La formule de Poisson préserve sont élégance en toute généralité ie. en sommant sur un réseau de dimension quelconque, elle est rappelée dans [4]. Ensuite il s'agit d'appliquer la *transformée de Mellin* aux deux membres de cette équation. La transformée de Mellin d'une fonction $f\colon \mathbb{R}_+ \to \mathbb{C}$ est donnée par l'intégrale, lorsqu'elle converge (dans notre cas pour $\Re s > 1$) :

$$g(s) = \int_0^\infty f(t)\, t^s \frac{dt}{t} \tag{3.2}$$

Essentiellement, c'est un moyen analytique qui permet de passer d'une série thêta à la série L associée puisque qu'on a $q = e^{2i\pi t} \overset{Mellin}{\longrightarrow} \Gamma(s)\, n^{-s}$ où $\Gamma(s)$ désigne la fonction d'Euler. En posant $f = \frac{1}{2}(\Theta - 1)$ on obtient $g(s) = \pi^{-s}\Gamma(s)\,\zeta(2s)$ mais si d'autre part on découpe l'intégrale 3.2 en 1 et qu'on applique un changement de variable dans le premier morceau pour ramener les bornes entre 1 et ∞, on voit que l'on peut appliquer l'identité 3.1 pour obtenir l'expression :

$$\xi(s) \overset{def}{=} g(s/2) = \int_1^\infty f(t)\left(t^{\frac{s}{2}} + t^{\frac{1-s}{2}}\right)\frac{dt}{t} - \frac{1}{s} - \frac{1}{1-s}$$

On remarque alors deux choses. D'une part, le terme donné par l'intégrale définit une fonction entière (f est dans l'espace de Schwartz) et l'on déduit qu'elle peut être considérée sur tout le plan complexe, au total on obtient pour ξ une fonction méromorphe dont les seuls pôles sont simples, 1 et -1 ayant pour résidus -1. La définition classique de ζ n'est valable que pour $\Re s > 1$ et comme la fonction Γ est bien connue (en particulier elle ne s'annule pas), cette relation permet non seulement de prolonger ζ analytiquement au plan complexe, mais elle fournit aussi des informations précises concernant ses zéros triviaux ainsi que la nature de ses pôles. D'autre part, cette expression est invariante par la symétrie $s \mapsto 1 - s$ et fournit donc l'équation fonctionnelle de la fonction zêta (peu ou prou la fonction L associée à ϑ) :

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

Dans le cas d'une extension quadratique imaginaire, l'équation obtenue est de la forme $\Xi(s) = \Xi(2-s)$ où $\Xi(s) = (\alpha\pi)^{-s}\,\Gamma(s)\,L(s,\chi)$ et α un nombre qui dépend du réseau, elle vient aussi avec un prolongement analytique. Ce prolongement analytique porte tout son intérêt lorsqu'il est replacé dans le cadre de l'étude des courbes elliptiques, il permet par exemple de relier les valeurs spéciales de la fonction L ainsi prolongée (valeurs prises parfois en dehors du domaine de définition initial) à certaines propriétés concernant la structure de groupe d'une courbe ayant la même série L. Le lien entre les réseaux du plan, formés par exemple les anneaux d'entiers déjà rencontrés, et les courbes elliptiques est effectué via l'étude des fonctions elliptiques et en particulier de la fonction $\wp$ de Weierstrass.

4 Courbes elliptiques, fonctions zêta et série de Hasse-Weil

4.1 Des réseaux aux courbes elliptiques

Si l'on se donne $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ un réseau du plan, on peut construire le tore complexe $E = \mathbb{C}/\Lambda$. C'est une surface de Riemann compacte de genre 1, et l'ensemble des fonctions méromorphes sur ce tore s'identifie celui des fonctions méromorphes Λ-périodique du plan complexe aussi nommées Λ-elliptiques. Une telle fonction f non constante est contrainte par le théorème des résidus à vérifier certaines relations :

$\sum_{z\in f^{-1}\{\infty\}} \text{rés}_z(f) = 0$, et elle a donc au moins deux pôles (avec multiplicité)

$\sum_{x\in E} \nu_x(f) = 0$, ainsi f prend autant de fois la valeur ∞ que 0 et donc que tout autre $cste \in \mathbb{S}^1$

$\sum_{x\in E} \nu_x(f) = 0$ dans E, autrement dit appartient à Λ

La fonction Λ-elliptique non constante la plus simple que l'on puisse construire est par conséquent la fonction de Weierstrass (du réseau) définie par la somme qui converge uniformément localement :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda}{}' \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$$

Sa périodicité provient de celle de sa dérivée $\wp'_\Lambda(z) = -2\cdot\sum_{\lambda\in\Lambda}(z-\lambda)^{-3}$, de sa parité et des évaluations en $\omega_i/2$. Elle a un unique pôle de multiplicité 2 en 0 et son degré, c'est à dire le nombre de fois qu'elle prend chaque valeur de la sphère, est donc de 2. Il s'avère que ces deux fonctions sont essentiellement les deux seuls exemples élémentaires dont nous ayons besoin puisque l'espace des fonctions Λ-elliptiques est égal à l'ensemble des fractions rationnelles en $\wp_\Lambda$ et sa dérivée et [7] présente même un procédé simple pour calculer la fraction associée à une fonction elliptique dont on connait les zéros et les pôles. Un calcul

classique fournit le développement en série de Laurent à l'origine, valable sur un voisinage isolant 0 du réseau :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{n \geqslant 2 \\ pair}} (n+1)\, G_{n+2}(\Lambda)\, z^n$$

Ceci permet de montrer que $\wp_\Lambda$ vérifie l'équation différentielle : $\wp'^2_\Lambda = 4\wp^3_\Lambda - g_2(\Lambda)\wp_\Lambda - g_3(\Lambda)$ où $g_2 = 60G_2$ et $g_3 = 140G_6$. Autrement dit, les points $\mathscr{P}_\Lambda(z) = \begin{pmatrix} \wp_\Lambda(z) \\ \wp'_\Lambda(z) \end{pmatrix}$ reposent sur la cubique projective non singulière d'équation $E_\Lambda : y^2 = 4x^3 - g_2 x - g_3$ (on laisse tomber les Λ pour alléger) aussi appelée courbe elliptique. Projective signifie qu'il faut la considérer dans $\mathbb{P}^2(\mathbb{C})$ et on voit alors qu'elle contient un seul point à l'infini : $\mathscr{P}_\Lambda(0)$, tandis que non singulière signifie que son discriminant $\Delta(\Lambda) = g_2^3 - 27g_3^2$ n'est pas nul. De plus, le fait que $\wp_\Lambda$ et sa dérivée soient respectivement de degré 2 et 3 entraine que $\mathscr{P}_\Lambda$ est un biholomorphisme et permet donc de transporter la structure de groupe du tore à la courbe elliptique (cette structure correspond par ailleurs à celle que l'on peut construire géométriquement à l'aide du théorème de Bézout). A chaque réseau Λ du plan correspond donc une équation de la forme $E_\Lambda$et l'étude des séries d'Eisenstein permet de montrer que réciproquement, si g_2 et g_3 vérifient $\Delta \neq 0$ alors il existe un unique réseau Λ en lequel les séries d'Eisenstein (renormalisées) prennent ces valeurs. Notons enfin que deux tores sont isogènes si et seulement si les courbes correspondantes s'obtiennent l'une de l'autre par un changement de variable admissible (on pourra consulter [2] pour les définitions). On a donc via $\mathscr{P}$ une identification entre les réseaux du plan (ou les tores complexes), et les courbes projectives complexes non singulières. C'est ce lien qui permet de passer de l'arithmétique des corps de nombre à celle des courbes elliptiques.

4.2 Fonctions zêta d'une variété projective sur un corps fini

Les courbes elliptiques comme celles rencontrées au paragraphe précédent sont un cas particulier de variétés projectives. De tels objets peuvent êtres définis sur un corps K quelconque : une variété algébrique projective V sur K dans l'espace de dimension m est l'ensemble des points de $\mathbb{P}^m\left(\overline{K}\right)$ solutions d'un système fini d'équations polynomiales homogènes en $m+1$ variables $f_j \in K[x_0, \ldots, x_m]$. Si L/K est une extension de corps, les L-points de V sont ceux qui appartiennent à $\mathbb{P}^m(L)$, on les note $V(L)$. Supposons que $K = \mathbb{F}_q$ soit un corps fini. On peut alors définir une série génératrice dénombrant les points qui s'ajoutent à la variété lorsque l'on considère des extensions de plus en plus grandes du corps de base, on l'appelle la fonction zêta de V sur $\mathbb{F}_q$:

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{r \geqslant 1} N_r \frac{T^r}{r}\right), \text{ où } N_r = \#V(\mathbb{F}_{q^r})$$

Remarquons qu'en multipliant par T la dérivée logarithmique de cette série, une opération courante dans l'étude combinatoire des séries de Lambert et de Dirichlet, on retombe sur la série génératrice ordinaire de la suite des N_r. L'intérêt de formuler ces idées dans un cadre aussi général est de pouvoir observer une courbe elliptique sur plusieurs corps différents. Il est par exemple courant d'essayer de déduire des propriétés globales de sa structure de groupe ie. celle qui est donnée sur le corps des rationnels, par la compréhension de ses structures locales ie. obtenues après réduction modulo un nombre premier : c'est le principe local global. Le théorème de HASSE-MINKOWSKI concernant les formes quadratiques illustre parfaitement ce genre de phénomènes, c'est l'objectif atteint dans la première partie de [4]. Pour toute courbe elliptique E sur $\mathbb{F}_q$, c'est à dire une courbe algébrique projective non singulière de genre un (le système est formé d'un seul polynôme homogène en trois variables et de discriminant non nul), la fonction zêta admet une factorisation de la forme :

$$Z(E/\mathbb{F}_q;T) = \frac{1-2a_E+qT^2}{(1-T)(1-qT)} = \frac{(1-\alpha T)\left(1-\frac{q}{\alpha}T\right)}{(1-T)(1-qT)} \tag{4.1}$$

où $2a_E \in \mathbb{Z}$ ne dépend que de E , et caractérise donc tous les coefficients N_r. On voit alors que la connaissance de $N_1 = q+1-2a_E$ (prendre la dérivée logarithmique de 4.1) renseigne sur les valeurs de tous les N_r. Ce fait est un cas particulier des conjectures de WEIL prouvées par DELIGNE concernant des variétés algébriques quelconques sur un corps fini. On les énonce dans un cas intermédiaire.

Théorème 4. *Soit V une courbe projective lisse.*

i) $Z(V/\mathbb{F}_q;T)$ est de la forme $\frac{P(T)}{(1-T)(1-qT)}$ avec $P \in 1+T\mathbb{Z}[T]$.

ii) Si V a été obtenue en réduisant modulo p une variété $\tilde{V}$ définie sur $\mathbb{Q}$ alors $\deg P = 2g$ où g est le genre de la variété complexe $\tilde{V}$.

iii) Si α est une racine du polynôme réciproque de P (ie. de $T^{\deg P}P(1/T)$) alors q/α aussi.

iv) Toutes les racines réciproques du numérateur ont pour module $\sqrt{q}$.

Avec les notations du théorème, $i)$ revient à dire que $N_r = 1+q^r-\sum_\alpha \alpha^r$, autrement dit les cardinaux des complémentaires de V dans les droites projectives des extensions successives de $\mathbb{F}_q$ sont données par les sommes de Newton du polynôme réciproque. Ces conjectures ont d'étonnant le fait qu'elles établissent un lien entre des propriétés topologiques (le genre) de la courbe, et ces propriétés arithmétiques (le nombre de points dans chaque extension). Elles disent essentiellement que plus la complexité topologique de la courbe est grande, plus il faudra déterminer de valeurs N_r avant de pouvoir inférer les autres.

4.3 Série de Hasse-Weil d'une courbe projective lisse

Si une courbe elliptique est définie sur $\mathbb{Q}$ alors on peut la réduire modulo un nombre premier p pour lequel la nouvelle équation obtenue devient une courbe elliptique sur $\mathbb{F}_p$. Cela ne se produit pas toujours car il est possible qu'une fois l'équation réduite modulo p son discriminant soit nul, on dit alors qu'elle admet une mauvaise réduction en p, néanmoins de telles situations ne se produisent qu'un nombre fini de fois. Les diverses bonnes réductions fournissent des informations locales sur la structure de la courbe encodées dans les fonctions zêta correspondantes et il est ensuite naturel de vouloir les regrouper pour espérer pourvoir en déduire des informations globales. Afin de garder en mémoire le nombre premier p auquel est associé chaque suite N_r, la fonction zêta est prise en $T = p^{-s}$. Tout cela suggère de définir comme suit la fonction L de Hasse-Weil de la courbe E :

$$L(E, s) = \frac{\zeta(s)\,\zeta(s-1)}{\prod_p Z(E/\mathbb{F}_q;\, p^{-s})} = \prod_p \frac{1}{1 - 2a_{E,p}p^{-s} + \epsilon(p)\,p^{1-2s}}$$

Les produits portent sur tous les nombres premiers et $\epsilon(p)$ est nul lorsqu'il y a une mauvaise réduction, sinon il vaut 1. Il y a une manière naturelle de définir les valeurs de $a_{E,p}$ et de $Z(E/\mathbb{F}_q;\, T)$ aux premiers de mauvaise réduction de telle sorte à ce qu'on ait l'égalité entre les deux expressions.

La similitude entre les fonctions L de Hasse-Weil avec celles que l'on a déjà rencontré n'est pas fortuite et il arrive qu'elles proviennent de séries associées à des fonctions propres de poids 2 de l'algèbre de Hecke pour un certain niveau N. Dans ce cas la courbe elliptique est dite *modulaire* (il y a certaines conditions techniques sur la nature de la forme en question, on demande en fait qu'elle soit une *nouvelle forme* autrement dit qu'elle ne provienne pas de niveaux inférieurs, on trouvera dans [2] plus d'informations à ce sujet).

Par exemple la courbe d'équation $E : y^2 = x^3 - d$ pour $d \in \mathbb{Z}$ est naturellement associée par le calcul des coefficients $a_{E,p}$ au coefficients apparaissant dans la série L de Hecke du caractère cubique rencontré à la section 2 or cette dernière correspond à la fonction L associée à la série thêta du même caractère qui s'avère être une telle nouvelle forme. Par conséquent cette courbe elliptique est modulaire. Ce phénomène s'inscrit dans une série de résultats plus généraux établissant la modularité de certaines classes de courbes elliptiques. Le cheminement employé ici s'appuie sur le fait que les courbes elliptiques à multiplication complexe (dont le tore associé admet des isogénies autres que les multiplications par un entier, c'est à dire des multiplications par un nombre complexe) proviennent de réseaux qui sont les anneaux des entiers d'une extension quadratique et auxquels on peut donc attacher une série thêta ayant la propriété d'être une nouvelle forme. On peut aussi déduire le résultat pour cette courbe en invoquant le théorème de modularité des courbes elliptiques à coefficients rationnels autrement dit de l'énoncé de la conjecture de Shimura-Taniyama-Weil dont la preuve fut achevée par Breuil, Conrad, Diamond et Taylor.

Si une courbe elliptique est modulaire alors comme expliqué dans la section 3, sa fonction L admet un prolongement analytique au plan complexe (et vérifie une propriété de symétrie par rapport au point 2) ce qui permet de considérer son comportement au voisinage de 1 (à priori en dehors du domaine de convergence). Associé au théorème de MORDELL-WEIL affirmant que $E(\mathbb{Q})$ est un groupe abélien de type fini, ceci permet d'énoncer une version faible de la

Conjecture 5. *de* BIRCH *et* SWINNERTON-DYER *: l'ordre d'annulation en* 1 *de la fonction* L *d'une courbe elliptique rationnelle est égal au rang du groupe sous-jacent.*

Des raffinements de cette énoncé relient les premiers coefficients du développement de la fonction L à certaines constantes décrivant la structure du groupe $E(\mathbb{Q})$.

5 Conclusion et autres points de vus sur la modularité

Après ce survol des fonctions L et de leur utilité pour prouver la modularité d'une courbe elliptique, il est naturel de se demander à quoi cela peut-il bien servir de savoir que telle courbe E est modulaire.

Tout d'abord la modularité est en fait une propriété très forte et possède un grand nombre d'énoncés équivalents se formulant souvent dans des langages à priori distincts des mathématiques. Par exemple une courbe E est modulaire si et seulement s'il existe un niveau N pour lequel la surface compacte $X_0(N)$ se surjecte de manière holomorphe sur $E \in \mathbb{P}^2(\mathbb{C})$. Il peut d'ailleurs sembler étonnant à quel point cet formulation cache tout l'aspect arithmétique contenu dans l'énnoncé que nous avons donné en termes de séries de Hasse-Weil et de nouvelles formes de poids 2. C'est en fait l'entier N qui régit la géométrie (la période d'une coordonnée locale) de la surface $X_0(N)$ au voisinage de ses pointes et cette géométrie se transmet aux différentielles holomorphes que l'on peut construire sur cette surface. Or il se trouve que celles-ci peuvent s'identifier aux formes modulaires de l'espace $S_2(\Gamma_0(N))$et une telle surjection permettrait d'effectuer un *push forward* des différentielles de la surface sur celles de la courbe. La modularité fournit donc bel et bien un lien entre ces deux univers éloignés à savoir l'arithmétique des séries L et la géométrie des surfaces de Riemann, mais bien d'autres encore apportent des points de vus fructueux : la géométrie algébrique (nous avons évoqué le théorème de Riemann-Roch) ou encore les représentations galoisiennes etc.

Il y a d'autre part un aspect plus pratique à la propriété de modularité, qui découle en fait de cette flexibilité dans les approches disponibles. En effet, plusieurs conjectures comme certains cas particuliers de celles de BIRCH et SWINNERTON-DYER concernant les courbes elliptiques ont été prouvées pour celles qui sont modulaires. On pourra s'en faire une idée plus précise en consultant la présentation officielle [1] de cette conjecture par ANDREW

WILES sur le site de l'institut Clay. Celles-ci permettent d'établir un bonne fois pour toute le problème antique des nombres congruents servant de fil directeur dans [7] : quels sont les nombres rationnels qui peuvent être l'aire d'un triangle rectangle à côtés rationnels ? La réponse dépend de la finitude ou non du groupe $E(\mathbb{Q})$ d'une courbe elliptique modulaire et donc en fin de compte de l'annulation d'une série de Hasse-Weil en 1.

Pour découvrir l'omniprésence des séries L dans l'univers encore plus grand du programme de LANGLANDS, le site [3] de CEREMONA recense une foule d'informations à leur sujet.

Références

[1] Wiles A. The birch and swinnerton-dyer conjecture. *Clay Mathematical Institute*, 2000.

[2] Diamond F. and Shurman J. *A First Course in Modular Forms*. Springer, 2005.

[3] Ceremona J. www.lmfdb.org.

[4] Serre J.P. *Cours d'arithmetique*. Presses Universitaires de France, 1970.

[5] Ireland K. and Rosen M. *A Classical Introduction to Modern Number Theory*. Springer, 1990.

[6] Artin M. *Algebra*. Pearson, 2010.

[7] Koblitz N. *Introduction to Elliptic Curves and Modular Forms*. Springer, 1993.