Formes modulaires et courbes elliptiques : les points de Heegner

Exposé au séminaire étudiant de théorie des nombres de Bordeaux.

Jérôme Gärtner
2007 – 2008

Table des matières

1 Introduction **3**

2 Formes modulaires **3**
2.1 Motivation . . . 3
2.2 Définitions . . . 4
2.3 Equation fonctionnelle . . . 7
2.4 Opérateurs de Hecke . . . 8
2.5 La théorie d'Atkin-Lehner : les formes nouvelles . . . 9

3 Rappels sur les courbes elliptiques **11**
3.1 Différents types de réduction . . . 11
3.2 Selmer et Tate-Shafarevich . . . 11
3.3 Fonctions L et conjecture BSD . . . 12
3.4 Courbes elliptiques sur $\mathbb{C}$ . . . 13

4 Lien avec les formes modulaires **14**
4.1 Aspect géométrique . . . 14
4.2 Modularité des courbes elliptiques . . . 14
4.3 Problèmes de modules . . . 15

5 Points de Heegner **16**
5.1 Aspect historique . . . 16
5.2 Les points de Heegner, d'après Birch . . . 17
5.3 La théorie de la multiplication complexe . . . 18
5.4 Définition des points de Heegner, d'après Darmon (entre autres) . . . 20
5.5 Quelques propriétés . . . 21
5.6 Applications . . . 21

1 Introduction

Le but de cet expoé est d'aborder la notion de points de Heegner. Pour cela je compte commencer par exposer la théorie des formes modulaires (opérateurs de Hecke, d'Atkin-Lehner, fonctions L...) dans le but de comprendre le théorème de modularité des courbes elliptiques. La deuxième partie consistera en un bref survol de ce que je sais des points de Heegner.

Vu l'urgence dans laquelle je tappe ces notes, je me dispense de taper les preuves car elles n'auront pas le temps d'être exposées au tableau... mais j'essayerai un jour de renvoyer à la bibliographie. Je m'excuse aussi par avance pour l'aspect brouillon de ce qui suit...

2 Formes modulaires

Pour cette section je renvoie à [6],[9][11] et [2] pour un introduction [3], [7] pour des choses plus complètes.

2.1 Motivation

Commençons par une définition :

Définition 2.1. Un caractère de Dirichlet est un morphisme $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}$ où $N \geqslant 2$. On l'étend en une application : $\mathbb{Z} \longrightarrow \mathbb{C}$ par $n \mapsto \chi(n)$ si n et N sont premiers entre eux, 0 sinon.

On connaît deux théorèmes classiques : le théorème des nombres premiers et le théorème de Dirichlet. Chacun utilise des fonctions trés proches de ce que l'on rencontre dans la théorie des formes modulaires... Rappellons d'abord tout ça :

Théorème 2.2 (TNP)**.**

$$\pi(x) = \sum_{p \leqslant x} 1 \sim \frac{x}{\ln x}$$

La démonstration utilise le fait que la fonction ζ de Riemann $\zeta(s) = \sum \frac{1}{n^s}$ admet un développement en produit eulerien $\prod \frac{1}{1-\frac{1}{p^s}}$, une équation fonctionnelle, un prolongement...

Théorème 2.3 (Dirichlet)**.** *Si a et b sont premiers entre eux, il existe une infinité de nombres premiers p avec $p \equiv a \mod b$.*

Ici la preuve utilise les fonctions L de Dirichlet $L(s, \chi) = \sum_{n \geqslant 1} \frac{\chi(n)}{n^s}$ où χ est un caractère de Dirichlet modulo b. Cette fonction aussi (dont ζ est un cas particulier) admet un développement en produit eulerien $\prod \frac{1}{1-\frac{\chi(p)}{p^s}}$, a un prolongement etc... et on utilise le fait que $L(\chi, 1) \neq 0$ si $\chi \neq 1$.

Entre autres on utilise tout le temps le fait que ces fonctions on un produit eulerien de la forme $\prod \frac{1}{aT+b}$. C'est quelque chose de dimension 1...

La théorie des formes modulaires aliée à celle des opérateurs de Hecke va étudier les fonctions qui ont un développement en produit eulérien de "dimension 2" : $\prod \frac{1}{aT^2+bT+c}$.

Comment traduire "dimension 2" ? en remarquant que $\mathbb{C}^\times = GL_1(\mathbb{C})$... on va donc utiliser quelque part GL_2 (voir GL_n dans le cas des formes automorphes).

2.2 Définitions

On notera $GL_2(\mathbb{R})_+$ l'ensembles des matrices carrées réelles d'ordre 2, de déterminant > 0, et $\mathcal{H}$ le demi-plan de Poincaré : $\mathcal{H} = \{z \in \mathbb{C} \text{ Im } z > 0\}$.

Proposition 2.4. *La fonction $GL_2(\mathbb{R})_+ \longrightarrow Aut(\mathcal{H})$ ($Aut(\mathcal{H})$ est l'ensemble des fonctions biholomorphes de $\mathcal{H}$) :*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(z \mapsto Az = \frac{az+b}{cz+d} \right)$$

est un morphisme surjectif de groupes de noyau $\mathbb{R}^* I_2$.

Corollaire 2.5.

$$\mathcal{H} \simeq GL_2(\mathbb{R})_+ / \mathbb{R}^* \simeq SL_2(\mathbb{R}) / \{\pm 1\}$$

Définition 2.6. On notera

$$\rho(a) = \frac{(\det A)^{1/2}}{cz+d}$$

.

Les formes modulaires sont des fonctions qui admettent une certaine équation fonctionnelle, qui traduit un invariance par un sous-groupe de $SL_2(\mathbb{Z})$. En vue d'applications à la théorie des courbes elliptiques, je peux me restreindre à certains sous-groupes Γ_0 et Γ_1 définis comme suit :

Définition 2.7. Soit $N \geqslant 1$, on pose :

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$$

et on a les inclusions suivantes :

$$\Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$$

Remarque 2.8. Le morphisme $\Gamma_0(N) \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ défini par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \overline{a}$$

est surjectif de noyau $\Gamma_1(N)$.

Utilisons un peu cette remarque : si ε est un caractère de Dirichlet modulo N, on va étendre ε à $\Gamma_0(N)$ en posant : $\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \quad \varepsilon(A) = \varepsilon(\overline{a})$.

Peut être qu'il faut changer ε en ε^{-1} pour que ca marche avec Hecke.

Soit $k \geqslant 2$. On va définir une action à droite de $GL_2(\mathbb{R})_+$ sur l'ensemble des fonctions holomorphes de $\mathcal{H}$ dans $\mathbb{C}$:

$$f|_k A : z \mapsto \rho(A)^k f(Az) = \frac{(ad-bc)^{k/2}}{(cz+d)^k} f\left(\frac{az+b}{cz+d} \right)$$

Remarquons que $f|_k \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (-1)^k f$.

On en vient à la définition des formes modulaires (celle qu j'utiliserai) :

Définition 2.9. Soit $N \geqslant 1$ et ε un caractère de Dirichlet modulo N. Si $k \geqslant 2$, une forme modulaire parabolique de poids k de caractère ε pour $\Gamma_0(N)$ est une fonction $f : \mathcal{H} \longrightarrow \mathbb{C}$ qui vérifie les trois propriétés suivantes :

1. f est holomorphe sur $\mathcal{H}$
2. Equation fonctionnelle : $\forall A \in \Gamma_0(N) \quad f|_k A = \varepsilon(A) f$
3. Parabolicité : $z \mapsto f(z)(\text{Im } z)^{k/2}$ est bornée sur $\mathcal{H}$.

Remarquons que nécessairement, $\varepsilon(-1) = (-1)^k$.

Notation : On notera $C(N, \varepsilon, k)$ l'ensemble de ces formes modulaires. (C pour *cuspidal*).

Exemple :

1. Les séries d'Eisenstein définies pour $k > 2$par $G_k(z) = \sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(cz+d)^k}$ sont des formes modulaires de poids k (non paraboliques).
2. La fonction $\Delta(z) = (60G_4(z)^3 - 27(140G_6(z))^2$ est une forme parabolique de poids 12 (les coefficients sont pris pour annuler le premier terme du développement en séries de Fourier).
3. Un exemple générique est donné par les séries de Poincaré, qui engendrent l'ensemble des formes modulaires, paraboliques ou non. Si h est une fonction sur $\mathcal{H}$, $f(z) = \sum_{\gamma\in\Gamma/\{\pm I\}} \frac{e^{\frac{2i\pi n\gamma(z)}{h}}}{(cz+d)^{2k}}$ où $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Remarque 2.10. Un définition peut-être plus classique est la suivante :

Définition 2.11. On appelle forme modulaire de poids k pour $SL_2(\mathbb{Z})$ une fonction holomorphe sur $\mathcal{H}$ à valeurs dans $\mathbb{C}$ qui vérifie :

1. $\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \quad f(Az) = (cz+d)^k f(z)$ (En particulier, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ donc $f(z+1) = f(z)$ et f a un développement en série de Fourier $f(z) = \sum_{\mathbb{Z}} a_n q^n$ où $q = e^{2i\pi z}$.)
2. f est holomorphe à l'infini, *i.e.* $a_n = 0$ dès que $n < 0$.

Si de plus $a_0 = 0$ on dit que f est parabolique.

Mais il se trouve que la définition que j'ai donnée est plus pratique pour comprendre la cuspidalité en lien avec les représentations automorphes. La condition de parabolicité évite un définition plus compliquée du type :

Définition 2.12. si Γ est un sous-groupe d'indice fini de $SL_2(\mathbb{Z})$, on dit qu'une fonction $f : \mathcal{H} \longrightarrow \mathbb{C}$ est une forme modulaire de poids k pour Γ si elle est holomorphe, vérifie $\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \quad f(Az) = (cz+d)^k f(z)$ et une "condition aux pointes" : pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, il existe un entier h tel que la fonction $z \mapsto (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ s'écrive sous la forme $\sum_{n=0}^{\infty} a_n^\gamma q^{n/h}$ avec $q = e^{2i\pi z}$ (q-développement). On dit que $\gamma^{-1}\infty = -\frac{d}{c}$ est une pointe et la série ci-dessus ne dépend que de $-\frac{d}{c}$ et cette série est appelée série de Fourier de f en $-\frac{d}{c}$.

La forme f est dite parabolique si $a_0^\gamma = 0$ pour tout γ. On note parfois $S_k(\Gamma)$ l'espace des formes paraboliques pour Γ, de poids k.

Le lien entre la définition adoptée et celle de la remarque est précisé par la proposition suivante, qui est conséquence de calculs de coefficients de Fourier :

Proposition 2.13. *Si $f \in C(N,k,\varepsilon)$ il existe une unique suite $(a_n)_{n\geqslant 1} \in \mathbb{C}^{\mathbb{N}^\times}$ telle aue $f(z) = \sum_{n\geqslant 1} a_n e^{2i\pi z}$ où la série converge absolument et uniformément sur tous compacts. Il existe $c > 0$ tel que $|a_n| \leqslant cn^{k/2}$.*

Tout ceci permet de définir la fonction suivante, dont l'importance n'est plus à prouver :

Définition 2.14. On défini la fonction L associée à f par :

$$L(f,s) : s \in \mathbb{C} \mapsto \sum_{n\geqslant 1} \frac{a_n}{n^s}$$

Cette série converge absolument et uniformément sur tout compact de $\{s \in \mathbb{C},\ \text{Re}\ s > \frac{k}{2} + 1\}$.

La convergence étant une conséquence de la conjecture de Ramanujan-Peterson (cette conjecture est maintenant un théorème de Deligne– plus exactement un corollaire des conjectures de Weil, mais le cas $k = 2$ était connu d'Eichler).

Théorème 2.15.

$$|a_n| \leqslant Cn^{\frac{k-1}{2}}$$

On en vient au cas de $\Gamma_1(N)$ (c'est la même définition, si on remarque que pour $\Gamma_1(N)$ il ne peut pas y avoir de caractère central).

Définition 2.16. Soit $N \geqslant 1$ et $k \geqslant 2$. Une forme modulaire parabolique de poids k pour $\Gamma_1(N)$ est une fonction $f : \mathcal{H} \longrightarrow \mathbb{C}$ qui vérifie les trois propriétés suivantes :

1. f est holomorphe sur $\mathcal{H}$
2. Equation fonctionnelle : $\forall A \in \Gamma_1(N) \quad f|_k A = f$
3. Parabolicité : $z \mapsto f(z)(\text{Im}\ z)^{k/2}$ est bornée sur $\mathcal{H}$.

On notera l'espace de telles formes $C(N,k)$.

Un résultat très interessant, et dont on trouvera des applications dans l'exposé de Cécile Armana de l'an dernier est le suivant :

Théorème 2.17. *Le $\mathbb{C}$-espace vectoriel $C(N,k)$ est de dimension finie... et on sait calculer les dimensions (elles dépendent du genre de la courbe associée et des points elliptiques).*

Exemple :

1. On peut montrer que $C(1,k)$ est de dimension $\left[\frac{k}{12}\right] - 1$ si $k \equiv 2 \bmod 12$ et $k \geqslant 12$, $\left[\frac{k}{12}\right]$ sinon.
2. Si $k = 12$ il y a donc qu'une seule forme modulaire parabolique de poids 12 pour $SL_2(\mathbb{Z})$, normalisée par $a_1 = 1$. C'est la forme Δ déjà mentionnée. Profitons-en pour mentionner quelques résultats :

– $\Delta = \sum_{n\geqslant 1} \tau(n) q^n$ où τ est la fonction de Ramanujan : $\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \ldots$. On peut montrer que $\Delta(z) = (2\pi)^{12} q \prod_{n\geqslant 1}(1-q^n)^{24}$.

– $\tau(mn) = \tau(n)\tau(m)$ si n et m sont premiers entre eux

– $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ si p est premier et $n \geqslant 1$.

– $L(\Delta, s) = \sum_{n \geqslant 1} \frac{\tau(n)}{n^s}$ a un développement en produit eulérien convergeant pour Re $s > 7$: $L(\Delta, s) = \prod_p \frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}$.

– Hecke a montré que $L(\Delta, s)$ se prolonge en un fonction entière vérifiant une équation fonctionnelle "au facteur archimédien près" : Si $\Lambda(\Delta, s) = (2\pi)^{-s}\Gamma(s)L(\Delta, s)$ (où $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ est la fonction d'Euler usuelle... dont les propriétés sont connues...), alors :

$$\Lambda(\Delta, s) = \Lambda(\Delta, 12 - s)$$

Ces résultats sont assez révélateurs de ce que l'on souhaite pour les formes modulaires.

2.3 Equation fonctionnelle

Pourquoi faire intervenir les formes avec caractère central ? entre autres pour la proposition suivante :

Proposition 2.18.

$$C(N, k) = \bigoplus_{\varepsilon:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} C(N, k, \varepsilon)$$

qui va permettre de prouver l'existence d'une équation fonctionnelle pour les fonctions $L(f, s)$.

Soit $f \in C(N, k, \varepsilon)$, on pose :

$$\Lambda(f, s) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s)L(f, s)$$

cette expression étant inspirée de la fonction Δ. Un changement de variables permet de voir que $a^{-1}\Gamma(s) = \int_0^\infty e^{-at}t^{s-1}dt$ (Re $s > 0$). Comme $f = \sum_{n \geqslant 1} a_n e^{2i\pi mz}$ et $L(f, s) = \sum_{n \geqslant 1} \frac{a_n}{n^s}$ (Re $s > \frac{k}{2} + 1$), on a :

$$\Lambda(f, s) = \int_0^\infty f\left(\frac{it}{\sqrt{N}}\right) t^{s-1}dt$$

On a le lemme suivant, qui montre l'intérêt de la proposition 2.18 :

Lemme 2.19. *Soit* $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$.

Alors l'application : $f \mapsto f|_k W_N$ *est un isomorphisme*

$$C(N, k, \varepsilon) \xrightarrow{\sim} C(N, k, \varepsilon^{-1})$$

Remarque 2.20. L'opération W_N intervient dans la définition des points de Heegner...

Une fois que l'on a mis $\Lambda(f, s)$ sous forme intégrale, on peut faire un raisonnement analogue à celui qui montre le prolongement de ζ : on découpe l'intégrale en 1, la partie $\int_0^1$ peut se tranformer en $\int_1^\infty$ par l'action de W_N. On obtient alors :

Théorème 2.21. *La fonction* $\Lambda(f, s)$*, a priori définie pour Re* $s > \frac{k}{2} + 1$ *se prolonge en une fonction entière qui vérifie l'équation fonctionnelle :*

$$\Lambda(f, s) = i^k \Lambda(f|_k W_N, k - s)$$

Remarque 2.22. Si $k \equiv 0 \bmod 2$, le facteur est ± 1 on parle du signe de la fonction L pour le signe de son équation fonctionnelle. C'est le cas pour l'espace des formes modulaires $C(N, 2, 1)$ en lien avec les courbes elliptiques.

On peut ré-écrire la partie $L(f,s)$ comme suit :

Corollaire 2.23. *$L(f,s)$ se prolonge en une fonction entière, s'exprime comme :*

$$L(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^{s-1} dt$$

et vérifie l'équation :

$$\left(\frac{2\pi}{\sqrt{N}}\right)^s \Gamma(s) L(f,s) = i^k \left(\frac{2\pi}{\sqrt{N}}\right)^{s-k} \Gamma(s-k) L(f,s-k)$$

2.4 Opérateurs de Hecke

Les opérateurs de Hecke (et la théorie d'Atkin-Lehner qui va suivre) permettent de répondre au problème des produits euleriens.

Définition 2.24. Soit $f \in C(N,k,\varepsilon)$ et p un nombre premier. On pose :

$$f|_k T_p = p^{\frac{k}{2}-1} \left[\sum_{u=0}^{p-1} f|_k \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix} + \varepsilon(p) f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right]$$

Remarque 2.25. Tout d'abord $\varepsilon(p) = 0$ si $p|N$.

D'autre part, les matrices qui interviennent dans la définition ci-dessus forment un système de représentants des doubles classes : $\Gamma_0(N) \backslash \Gamma_0(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_0(N)$. (il y a p telles matrices si $p|N$ et $p+1$ sinon). En passant, on peut voir que $\Gamma_0(N)$ est d'indice $N \prod_{p|N} \left(1 + \frac{1}{p}\right)$ dans $SL_2(\mathbb{Z})$.

Les proposition suivante affirme que l'on a bien des opérateurs :

Proposition 2.26. *On a $f|_k T(p) \in C(N,k,\varepsilon)$.*

Un calcul utilisant une réindexation et le fait que $\sum_{u=0}^{p-1} e^{2i\pi n \frac{u}{p}}$ est 0 si $p \nmid n$ et p sinon fournit :

Proposition 2.27. *On a $f|_k T(p) = \sum_{n \geqslant 1} a_{np} e^{2i\pi nz} + \varepsilon(p) p^{k-1} \sum_{n \geqslant 1} a_n e^{2i\pi npz}$. Autrement dit les coefficients de Fourier de $f|_k T(p)$ sont $a_{np} + \varepsilon(p) p^{k-1} a_{\frac{n}{p}}$ avec $a_{\frac{n}{p}} = 0$ si $p \nmid n$.*

Corollaire 2.28. *Les opérateurs de Hecke commutent.*

Si $f \in C(N,k,\varepsilon)$ est propre pour $T(p)$ (i.e. $f|_k T(p) = \lambda(p) f$) on a si $n = mp^r$ avec $p \nmid m$ $a_n = a_m \lambda(p^r)$ La réciproque est vrai.

Corollaire 2.29. *$f \in C(N,k,\varepsilon)$ est propre pour tous les opérateurs de Hecke ssi $a_n = a_1 \prod_p \lambda(p^r)$ où $n = \prod_p p^r$. En particulier $f = 0$ ssi $a_1 = 0$. Ceci est vérifié en particulier si $C(N,k,\varepsilon)$ est de dimension 1.*

Souvent on normalise $f \neq 0$ par $a_1 = 1$ on a alors $a_p = \lambda(p)$ et $a_{p^{r+1}} = a_p a_{p^r} - \varepsilon(p) p^{k-1} a_{p^{r-1}}$, $a_{mn} = a_m a_n$ si m et n sont premiers entre eux... à rapprocher des propriétés de la fonction τ déjà mentionnées.

Proposition 2.30. *Soit $f \in C(N,k,\varepsilon)$ propre pour tous les $T(p)$, p premier et normalisée par $a_1 = 1$ (donc $a_p = \lambda(p)$). Alors pour tout Re $z > \frac{k}{2} + 1$*

$$L(f,s) = \prod_p \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s}}$$

Introduisons maintenant une structure hermitienne sur $C(N,k,\varepsilon)$ en vu d'utiliser un théorème spectral :

Définition 2.31. Soit $dv(z) = \frac{dxdy}{y^2}$. C'est une mesure sur $\mathcal{H}$ qui est $SL_2(\mathbb{Z})$-invarainte. En particulier $\Gamma_0(N)\backslash\mathcal{H}$ est de mesure finie et si $f,g \in C(N,k,\varepsilon)$,

$$< f,g >= \frac{1}{v\left(\Gamma_0(N)\backslash\mathcal{H}\right)} \int_{\Gamma_0(N)\backslash\mathcal{H}} f(z)\overline{g(z)}(\text{Im } z)^k dv(z)$$

définit un produit scalaire hermitien : le produit de Peterson.

Proposition 2.32. *L'adjoint de $T(p)$ pour le produit de Peterson est, si $p \nmid N$, $\varepsilon(p)T(p)$.*

Corollaire 2.33. *Il existe une base de $C(N,k,\varepsilon)$ propre pour tous les $T(p)$, $p \nmid N$.*

Remarque 2.34. Si $N = 1$ on a donc une base pour $SL_2(\mathbb{Z})$ propre pour tous les opérateurs de Hecke.... Ce qui est faux en général et l'étude de ce problème est la théorie d'Atkin-Lehner : obtenir des formes propres pour tous les opérateurs de Hecke, donc dont la fonction L admet un produit eulerien.

Je vais conclure cette section avec la compatibilité entre les $T(p)$ et W_N :

Proposition 2.35. *Si $p|N$ on a $\lambda(p) = \varepsilon(p)\overline{\lambda(p)}$.*
On a $W_N^2 = -NI_2$ et $< f|_k W_N, g >= (-1)^k < f, g|_k W_N >$
Le diagramme suivant commute :

$$\begin{array}{ccc} C(N,k,\varepsilon) & \xrightarrow{|_k W_N} & C(N,k,\overline{\varepsilon}) \\ {\scriptstyle T(p)}\downarrow & & \downarrow{\scriptstyle T(p)\varepsilon(p)} \\ C(N,k,\varepsilon) & \xrightarrow[|_k W_N]{} & C(N,k,\overline{\varepsilon}) \end{array}$$

Remarquons que $\varepsilon \in \mathbb{U}$ donc $\overline{\varepsilon} = \varepsilon^{-1}$.

2.5 La théorie d'Atkin-Lehner : les formes nouvelles

Motivation : Reprennons un instant la théorie des caractères de Dirichlet : un caractère de Dirichlet modulo N est non primitif s'il se factorise par un caractère modulo $M|N$: autrement dit si on a la situation suivante :

$$(\mathbb{Z}/N\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}$$

Dans le cas contraire le caractère est dit primitif.

Proposition 2.36. *Tout caractère de Dirichlet ε est issu d'un unique caractère primitif par "inflation". Le niveau de ce conducteur primitif est un diviseur du niveau de ε et s'appelle le conducteur de ε.*

On a interêt à traiter avec les caractères primitifs car une fois étendus à $\mathbb{Z}$, ils ont moins de zéros (les zéros sont obtenus pour les diviseurs du niveau).

D'une manière analogue on va chercher à voir si une forme modulaire admet un "conducteur" avec des propriétés proches de celles d'un caractère de Dirichlet. Ce qui va permettre d'obtenir une base canonique de $C(N,k,\varepsilon)$.

Définition 2.37. Soit ε un caractère de Dirichlet et N un multiple de son conducteur. Soit $\delta_a = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ où $a > 0$. On a $f|_k\delta_a(z) = a^{k/2}f(az)$.

Proposition 2.38. *Soit N' un multiple du conducteur de ε et M avec $N'M|N$. On a $\Gamma_0(N) \subset \Gamma_0(N')$ et $C(N', k, \varepsilon) \subset C(N, k, \varepsilon)$. Alors l'appplication $|_k\delta_M : C(N', k, \varepsilon) \to C(N, k, \varepsilon)$:*

$$f \mapsto f|_k\delta_M$$

est bien définie.

Exemple : Si $f \in C(1, k, 1)$, on a $z \mapsto f(z)$ et $z \mapsto f(pz)$ dans $C(p, k, 1)$.

Définition 2.39. L'espace des formes anciennes est l'espace engendré par les formes du type $f|_k\delta_M$ où $N' \neq N$. L'espace des formes nouvelles est l'orthogonal pour le produit de Peterson.

Dans le cas où ε est primitif (c'est-à-dire conducteur=niveau=N), toutes les formes sont nouvelles

Remarque 2.40. Je dirai que f est primitive si elle est nouvelle, propre pour tous les opérateurs de Hecke $T(p)$ et normalisée ($a_1 = 1$). L'ensemble des formes primitives n'est pas un ev...

Proposition 2.41. *Le diagramme suivant commute si p et N sont premiers entre eux.*

$$\begin{array}{ccc} C(N', k, \varepsilon) & \xrightarrow{|_k\delta_M} & C(N, k, \varepsilon) \\ {\scriptstyle T(p)}\downarrow & & \downarrow{\scriptstyle T(p)\varepsilon(p)} \\ C(N', k, \varepsilon) & \xrightarrow[|_k\delta_M]{} & C(N, k, \varepsilon) \end{array}$$

Corollaire 2.42. *L'espace des formes anciennes est stable par $T(p)$ pour $p \nmid N$ de même que l'espace nouveau. Ces deux espaces admettent une base propre pour les $T(p)$ où $p \nmid N$.*

Un théorème très important en lien avec la théorie des représentations automorphes :

Théorème 2.43. *Supposons que $f, g \in C(N, k, \varepsilon)$ sont propres pour les $T(p)$ et de mêmes valeurs propres, pour tous les premiers $p \notin S$ où S est un ensemble fini, alors si f est nouvelle, il existe $c \in \mathbb{C}$ tel que $g = cf$. i.e. les espaces propres sont de dimension 1.*

Le corollaire suivant vient de la diagonalisation simultanée :

Corollaire 2.44. *Si f est nouvelle et propre pour les $T(p)$ sauf un nombre fini, elle est propre pour tous les $T(p)$. L'ensemble des formes primitives est une base des formes nouvelles.*

Exemple : Pour $SL_2(\mathbb{Z})$ tout est nouveau... mais pour $\Gamma_0(p)$? une base de $C(p, k, 1)$ est constituée des formes primitives de $C(p, k, 1)$ et des $f|_k\delta_p$ où f est primitive de $C(1, k, 1)$.

Le théorème suivant est une amélioration de 2.43.

Théorème 2.45. *Si f, g sont primitives de mêmes valeurs propres pour tous les $T(p)$ sauf un nombre fini alors $f = g$*

On en déduit une base canonique de $C(N, k, \varepsilon)$:

Corollaire 2.46. *Une base canonique de $C(N,k,\varepsilon)$ est donnée par les formes primitives de niveau $N'|N$ de caractère ε de poids k et par leurs images sous dilatation (les $f|_k\delta_M$) où $MN'|N$.*

On a pour finir le vrai théorème de multiplicité 1 :

Théorème 2.47. *Si $f \in C(N,k,\varepsilon)$ et $g \in C(N',k',\varepsilon')$ sont primitives. Si leurs valeurs propres sous $T(p)$ sont les mêmes sauf pour p dans un ensemble de densité 0, alors $f = g$.*

Remarque 2.48. L'opération $|_kW_N$ respecte l'espace ancien et l'espace nouveau.

On retiendra entre autre qu'en utilisant les formes normalisées, l'espace $C(N,2,1)$ admet une base de formes modulaires dont les coefficients de Fourier sont entiers (utiliser les relations liant les coefficients).

3 Rappels sur les courbes elliptiques

On se référera à [2] et [10].

Les courbes elliptiques sont des objets qui apparaissent naturellement en géométrie arithmétique :

Définition 3.1. Une courbe elliptique E sur un corps F est un groupe algébrique complet de dimension 1. On note $E(F)$ l'ensemble de ses points rationnels.

Si F est de caractéristique différente de 2 et 3, on peut décrire une courbe elliptique par son équation affine $y^2 = x^3+ax+b$ où $a,b \in F$ et $\Delta = -2^4(4a^3+27b^2) \neq 0$ On peut définir à partir de E/F un invariant, appelé invariant j, qui classifie les classes d'isomorphie de courbes elliptiques sur $\bar{F}$. Il est donné par la formule $j = -\frac{2^{12}3^3a^3}{\Delta}$. On peut aussi associer une forme différentielle, la différentielle de Néron ω_E.

3.1 Différents types de réduction

Si F est un corps p-adique, on peut faire un changement de variables dans l'équation pour que les coefficients soit dans l'anneau des entiers $\mathcal{O}_F$ de F, et tel que le discriminant Δ_{min} de cette équation soit de valuation minimale dans $\mathcal{O}_F$. Soit π une uniformisante de $\mathcal{O}_F$. On peut classifier le comportement de la courbe obtenue par réduction modulo π, courbe définie sur $k = \mathcal{O}_F/(\pi)$. En particulier, si $\Delta_{min} \in \mathcal{O}_F^\times$, on obtient encore une courbe elliptique, et on dit que E/F est à bonne réduction. Si Δ_{min} n'est pas une unité, mais si la courbe réduite présente un point double comme seule singularité, on dit qu'elle est à réduction multiplicative (déployée si les tangentes sont définies sur k, non déployée sinon). Si on a une pointe, on dit que la réduction est additive.

Dans le cas arithmétiquement intéressant, celui des corps de nombres, on peut utiliser une complétion p-adique pour parler de réduction modulo p.

3.2 Selmer et Tate-Shafarevich

Parmi les théorèmes fondamentaux pour les courbes elliptiques sur les corps de nombres, on se doit de citer celui qui définit le rang de la courbe :

Théorème 3.2 (Mordell-Weil)**.** *Si F est un corps de nombres, $E(F)$ est un groupe abélien de type fini. Il est donc isomorphe à $\mathbb{Z}^r \oplus E(F)_{tors}$ et on appelle r le rang de la courbe.*

La démonstration de ce théorème se fait en deux étapes, dont l'une est le théorème de Mordell-Weil faible, qui affirme que pour tout $n \geqslant 1$, $E(F)/nE(F)$ est fini. L'application multiplication par n est surjective sur $E(\bar{F})$ (cloture algébrique). Notons $E_n = E_n(\bar{F})$ le noyau de cette application. On a la suite exacte :

$$\{0\} \longrightarrow E_n \longrightarrow E(\bar{F}) \xrightarrow{n} E(\bar{F}) \longrightarrow \{0\}$$

Si on note $H^i(F, M) = H^i(Gal(\bar{F}/F), M)$ les groupes de cohomologie galoisienne, on obtient la suite exacte longue (les H^0 sont invariants) :

$$\{0\} \longrightarrow E_n(F) \longrightarrow E(F) \xrightarrow{n} E(F) \xrightarrow{\delta} H^1(F, E_n) \longrightarrow H^1(F, E) \xrightarrow{n} H^1(F, E)$$

qui fournit la suite exacte de descente :

$$\{0\} \longrightarrow E(F)/nE(F) \xrightarrow{\delta} H^1(F, E_n) \longrightarrow H^1(F, E)_n \longrightarrow \{0\}$$

On voit donc que $E(F)/nE(F)$ se plonge dans $H^1(F, E_n)$, qui n'est malheureusement jamais fini si F est un corps de nombres. L'idée est donc alors de regarder les informations locales : soit v une place de F. On note F_v la completion de F en v, et comme $\bar{F}_v$ contient $\bar{F}$, on a $G_{F_v} \subset G_F$. On a donc une suite exacte de descente locale, qui fournit le diagramme commutatif suivant :

$$\begin{array}{ccccccccc}
\{0\} & \longrightarrow & E(F)/nE(F) & \xrightarrow{\delta} & H^1(F, E_n) & \longrightarrow & H^1(F, E)_n & \longrightarrow & \{0\} \\
 & & \downarrow & & \downarrow{\scriptstyle res_v} & \searrow^{\partial_v} & \downarrow{\scriptstyle res_v} & & \\
\{0\} & \longrightarrow & E(F_v)/nE(F_v) & \xrightarrow{\delta} & H^1(F_v, E_n) & \longrightarrow & H^1(F_v, E)_n & \longrightarrow & \{0\}
\end{array}$$

Définition 3.3. Si F est un corps de nombres, le $n$ième groupe de Selmer de F $Sel_n(E/F)$ est l'ensemble des classes $c \in H^1(F, E_n)$ qui vérifient $\partial_v(c) = 0$ pour toutes les places v de F. Le groupe de Tate-Shafarevich $Ш(E/F)$ est l'ensemble des classes $c \in H^1(F, E)$ qui vérifient $res_v(c) = 0$ pour toutes les places v de F.

On obtient alors la suite exacte :

$$\{0\} \longrightarrow E(F)/nE(F) \xrightarrow{\delta} Sel_n(E/F) \longrightarrow Ш(E/F)_n \longrightarrow \{0\}$$

Et le théorème de Mordell-Weil faible est alors une conséquence de la finitude du groupe de Slemer $Sel_n(E/F)$. Donc l'étude de $E(F)/nE(F)$ se ramène à l'étude de $Sel_n(E/F)$ et de $Ш(E/F)_n$. Comment quantifier l'approximation de $E(F)/nE(F)$ par $Sel_n(E/F)$? on a la conjecture suivante :

Conjecture 3.4. *Le groupe* $Ш(E/F)$ *est fini*

On conjecture même plus précisément que $E(F)/nE(F)$ est égal à $Sel_n(E/F)$ pour presque tous les entiers n.

3.3 Fonctions L et conjecture BSD

Soit E une courbe elliptique sur $\mathbb{Q}$ (on prend $\mathbb{Q}$ ici par simplicité). On définit des nombres a_p, pour tout nombre premier p, de la manière suivante :

– $a_p = p + 1 - E(\mathbb{F}_p)$ si E est de bonne réduction en p.

– $a_p = 1$ si E est à réduction multiplicative déployée en p.

– $a_p = -1$ si E est à réduction multiplicative non déployée en p.

– $a_p = 0$ si E est à réduction additive en p.

On définit aussi un entier N, le *conducteur arithmétique* de E, qui vérifie $v_p(N) = 0$ ssi E est à bonne réduction en p, $v_p(E) = 1$ ssi E est à réduction multiplicative en p, et enfin $v_p(E) = 2$ si E est à réduction additive et $p > 3$. Dans le cas d'une réduction additive pour $p = 2$ ou 3, on prend des valuations plus grandes qui sont données par l'algorithme de Tate.

Définition 3.5. La fonction L de E est définie par un produit Eulerien : $L(E,s) = \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p p^{-s})^{-1}$, qui définit formellement les nombres a_n pour tout n par la série de Dirichlet : $L(E,s) = \sum \frac{a_n}{n^s}$. Le produit Eulerien converge pour $Re(s) > \frac{3}{2}$

On peut montrer (Wiles) que la fonction L se prolonge analytiquement en une fonction entière, qui vérifie une certaine équation fonctionnelle.

Si N_p est le nombre de points non-singuliers de $E(\mathbb{F}_p)$, on a formellement en $s = 1$ $L(E,1) = \prod_p \frac{p}{N_p}$, ce qui mène à formuler la conjecture suivante :

Conjecture 3.6 (Birch et Swinnerton-Dyer)**.** *On a* $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = C$ *où* r *est le rang de* $E(\mathbb{Q})$ *et* C *une constante entièrement déterminée, qui dépend en particulier du cardinal de* $Ш(E/\mathbb{Q})$ *et du régulateur de* E*, pour ceux qui connaissent.*

On a le résultat suivant, qui est le seul cas connu de BSD :

Théorème 3.7 (Gross-Zagier, Kolyvagin)**.** *Soit* $E/\mathbb{Q}$ *une courbe elliptique. Si* $L(E,1) \neq 0$*, alors* $r = 0$*. Si* $L(E,1) = 0$ *et* $L'(E,1) \neq 0$*, alors* $r = 1$*. Dans les deux cas* $Ш(E/\mathbb{Q})$ *est fini.*

Ce théorème utilise la notion de points de Heegner, qui est la notion que j'aimerais aborder dans cet exposé.

3.4 Courbes elliptiques sur $\mathbb{C}$

Le but de cette sous-section est juste de rappeler que toute courbe elliptique sur $\mathbb{C}$ est un tore complexe : ses points complexes s'identifient au quotient de $\mathbb{C}$ par un réseau :

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}).$$

Cette application appelée *uniformisation de Weierstrass* est construite explicitement à l'aide de la fonction $\wp$ de Weierstrass du réseau. On a

$$\forall z \in \mathbb{C}\backslash\Lambda \quad \wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

L'application $\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ annoncée est donnée par $z \mapsto (\wp(z), \wp'(z))$.

Entre autres, le développement en série de Laurent de la fonction $\wp$ fait intervenir les séries d'Eisenstein.

Deux courbes elliptiques $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes ssi il existe $m \in \mathbb{C}$ avec $\Lambda = m\Lambda'$.

Un résultat (pseudo)-classique sur $SL_2(\mathbb{Z})$ est que les classes d'équivalences de points de $\mathcal{H}$ modulo $SL_2(\mathbb{Z})$ sont en bijection avec les classes d'homothéties réseaux de $\mathbb{C}$. On en

déduit donc que $\mathcal{H}/SL_2(\mathbb{Z})$ classifie les classes d'isomorphismes de courbes elliptiques sur $\mathbb{C}$.

En particulier, pour toute courbe elliptique sur $\mathbb{C}$ il existe $\tau \in \mathcal{H}$ tel que $E \simeq E_\tau$, où $E_\tau(\mathbb{C}) = \mathbb{C}/\Lambda_\tau$ avec $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$.

4 Lien avec les formes modulaires

Cet aspect est particulièrement bien traité dans [3].

On voit apparaître un lien entre les courbes elliptiques et les formes modulaires si l'on remarque que les nombres N_p de la section précédente sont liés entre eux par une relation de modularité. Le caractère modulaire des courbes elliptiques est le seul moyen des informations intéressantes sur leurs fonctions L...

Le lien entre les courbes elliptiques et les formes modulaires se fait en utilisant les formes modulaires de poids 2, pour $\Gamma_0(N)$ et de caractère central trivial. On utilisera donc exclusivement dans cette section et les suivantes l'espace

$$S_2(N) = C(N, 2, 1)$$

4.1 Aspect géométrique

L'action de $\Gamma_0(N)$ sur $\mathcal{H}$ est propre et discrete. On peut montrer que $\mathcal{H}/\Gamma_0(N)$ hérite ainsi d'une structure de surface de Riemann. On peut la compactifier en ajoutant un nombre fini de pointes qui correspondent aux orbites sour $\Gamma_0(N)$ des points de $\mathbb{P}^1(\mathbb{Q})$ (il faut bien entendu adapter la topologie etc...). Si on note $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, $\mathcal{H}^*/\Gamma_0(N)$ est une surface de Riemann compacte, points complexes d'une courbe algébrique que l'on note $X_0(N)$.

Géométriquement, une forme modulaire f pour $SL_2(\mathbb{Z})$ laisse fixe la métrique hyperbolique sur $\mathcal{H}$ $ds^2 = (dx^2 + dy^2)/y^2$. En fait, à $f \in S_2(N)$, on peut associer $\omega_f = 2i\pi(z)dz$ qui est une forme différentielle holomorphe sur $X_0(N)(\mathbb{C})$.

Le théorème de Riemann-Roch, associé à l'identification de $S_2(N)$ avec $\Omega^1(X_0(N)(\mathbb{C}))$, permet de montrer que $S_2(N)$ est de dimension le genre de $X_0(N)$.

Je finis par deux notations qui serviront plus tard :

$$Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \text{ et } Y_1(N)(\mathbb{C}) = \Gamma_1(N)\backslash\mathcal{H}.$$

4.2 Modularité des courbes elliptiques

Le lien entre courbes elliptiques et formes modulaires se fait par leurs fonctions L, qui vérifient (au moins conjecturellement) les même propriétés. On a le théorème suivant :

Théorème 4.1 (Eichler-Shimura)**.** *Si f est une forme normalisée, propre pour les opérateurs de Hecke, dont les coefficients de Fourier sont entiers. Alors il existe une courbe elliptique sur $\mathbb{Q}$ telle que $L(E_f, s) = L(f, s)$.*

En fait la construction d'Eichler-Shimura fournit une projection de la jacobienne $J_0(N)$ de $X_0(N)$ sur la courbe E_f. Si on envoit $X_0(N)$ dans sa jacobienne en associant à $P \in X_0(N)$ la classe du diviseur de degré 0 $(P) - (i\infty)$, on obtient une uniformisation $\Phi_N : X_0(N) \longrightarrow E_f$, appelée paramétrisation modulaire. Le pullback de la forme de Néron ω_E, $\Phi_N^*(\omega_E)$ est proportionnelle à $\omega_f = 2i\pi f(z)dz$. La constante de proportionnalité $c \in \mathbb{Q}^\times$ est la constante de Manin de f. (on conjecture que $c = 1$, c'est montré si N est sans

facteurs carré). Pour les calculs explicites, on considère que $\Phi_N : \mathcal{H}/\Gamma_0(N) \longrightarrow E_f(\mathbb{C})$. Mais une courbe elliptique sur $\mathbb{C}$ est quotient de $\mathbb{C}$ par un réseau (dit de Néron) Λ_E. soit $\Phi_w : \mathbb{C}/\Lambda_E \longrightarrow E(\mathbb{C})$ l'uniformisation de Weierstrass (avec les fonctions $\wp$). Si c est la constante de Manin, on a :

Proposition 4.2. *On a $\Phi_N(\tau) = \Phi_w(z_\tau)$ où $z_\tau = c\int_{i\infty}^{\tau} 2i\pi f(z)dz = c\sum_{n=1}^{\infty}\frac{a_n}{n}e^{2i\pi\tau n}$.*

Le résultat de la conjecture de Shimura-Taniyama-Weil est le théorème de Wiles suivant :

Théorème 4.3. *Si E est une courbe elliptique sur $\mathbb{Q}$ de conducteur N, il existe une forme nouvelle $f \in S_2(N)$ telle que $L(E,s) = L(f,s)$. De plus E est isogène à E_f de la construction d'Eichler-Shimura. (E_f est la courbe de Weil de la classe d'isogénie).*

On peut donc parler du signe de l'équation fonctionnelle de $L(E,s)$, c'est celui de $L(f,s)$. On le note $signe(E,\mathbb{Q})$. Le signe donne déjà une information sur l'ordre d'annulation de $L(E,s)$ en 1 : il est pair si $signe(E,\mathbb{Q}) = 1$, impair sinon.

4.3 Problèmes de modules

Les courbes modulaires répondent à certains problèmes de modules concernant les courbes elliptiques (sur $\mathbb{C}$). Comme je l'ai déjà mentionné un exemple est que $\mathcal{H}/SL_2(\mathbb{Z})$, autrement dit $X_0(1)(\mathbb{C})$ classifie les classes d'isomorphismes de courbes elliptiques sur $\mathbb{C}$.

A quoi correspondent les courbes $X_0(N)$ et $X_1(N)$? elles classifient les courbes elliptiques munies d'une information sur la torsion :

Notons dans cette partie $S_0(N)$ l'ensemble des classes d'équivalence de courbes elliptiques E munies d'un sous groupe cyclique C d'ordre N. L'équivalence étant : $(E,C) \sim (E',C')$ ssi il existe un isomorphisme de E sur E' qui envoie C sur C'.

$$S_0(N) = \{(E,C),\ \text{E courbe elliptique, C sous groupe cyclique d'ordre } N\}/\sim$$

Notons $S_1(N)$ l'ensemble des classes d'équivalence de courbes elliptiques E munies d'un point Q d'ordre N. L'équivalence étant : $(E,Q) \sim (E',Q')$ ssi il existe un isomorphisme de E sur E' qui envoie Q sur Q'.

$$S_1(N) = \{(E,Q),\ \text{E courbe elliptique, Q point d'ordre } N\}/\sim$$

Théorème 4.4. 1. *L' espace de modules pour $\Gamma_0(N)$ est*

$$S_0(N) = \{[E_\tau, < \frac{1}{N} + \Lambda_\tau >], \tau \in \mathcal{H}\}.$$

$[E_\tau, < \frac{1}{N} + \Lambda_\tau >] = [E_{\tau'}, < \frac{1}{N} + \Lambda_{\tau'} >]$ ssi $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Il y a donc une bijection

$$S_0(N) \xrightarrow{\sim} Y_0(N)$$

qui envoie $[E_\tau, < \frac{1}{N} + \Lambda_\tau >]$ sur $\Gamma_0(N)\tau$.

2. *L' espace de modules pour $\Gamma_1(N)$ est*

$$S_1(N) = \{[E_\tau, \frac{1}{N} + \Lambda_\tau], \tau \in \mathcal{H}\}$$

$[E_\tau, \frac{1}{N} + \Lambda_\tau] = [E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}]$ ssi $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Il y a donc une bijection

$$S_1(N) \xrightarrow{\sim} Y_1(N)$$

qui envoie $[E_\tau, \frac{1}{N} + \Lambda_\tau]$ sur $\Gamma_1(N)\tau$.

Remarque 4.5. Les courbes modulaires $Y(N)$ pour $\Gamma(N)$ sont en général associées au problème de module : pour l'ensemble des courbes elliptiques ;unies d'une paire de points (P,Q) qui engendrent le sous-groupe de torsion $E[N]$ et dont le pairing de Weil est $e_N(P,Q) = e^{2i\pi/N}$ ie $S(N) = \{[\mathbb{C}/\Lambda_\tau], (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)\}$.

5 Points de Heegner

On ira voir [1] qui est l'un des premiers articles, [2] pour approche un peu plus moderne. [11] pour la multiplication complexe.

La théorie du corps de classe, fondamentale en théorie des nombres, admet dans certains cas une formulation explicite. C'est la théorie de la multiplication complexe, qui donne une construction explicite de corps de classe pour les corps quadratiques imaginaires. Si on utilise en plus la paramétrisation modulaire, on obtient des points de la courbe définis sur de tels corps de classe. Ce sont les points de Heegner, qui sont au centre de la démonstration du théorème de Gross-Zagier et Kolyvagin.

5.1 Aspect historique

Le 12ème problème de Hilbert consiste en la recherche d'une théorie de corps de classe explicite : c'est-à-dire que si on se donne un corps de nombre K, on cherche une fonction qui fournisse toutes les extensions abéliennes de K.

On connaît le théorème de Kronecker-Weber, qui peut se formuler de la manière suivante : "toute extension abélienne de $\mathbb{Q}$ est dans un corps cyclotomique". En fait, un léger changement de point de vue fournit l'énoncé suivant : "La fonction $x \mapsto e^{i\pi x}$ épuise toutes les extensions abéliennes de $\mathbb{Q}$".

Le théorème de Kronecker-Weber est donc à la fois le résultat de base qui suggéra l'idée de la conjecture à Hilbert, mais aussi un premier cas... et il y en a peu. Hilbert proposa la fonction j comme fonction pour le cas où K est un corps quadratique imaginaire... et il se trompait (cf le livre sur l'histoire du pb, SMF), il faut en effet ajouter les racines de l'unité, et certaines valeurs spéciales d'autres fonctions, par exemple la fonction $\wp$ de Weierstrass. C'est la théorie de la multiplication complexe, qui peut se généraliser au cas d'extensions CM (extensions totalement imaginaires de corps totalement réels.), mais on en sait pas vraiment aller plus loin.

Un des plus vieux problèmes de théorie des nombres est la détermination du groupe des points rationnels d'une courbe elliptique sur $\mathbb{Q}$. On ne sait toujours pas le résoudre en général, sauf dans des cas particuliers. En général la théorie ou les calculs affirment qu'il doit exister des points rationnels, mais on est incapables d'en construire. Le problème des nombres congruents (un entier B est il l'aire d'un triangle rectangle dont les côtés sont rationnels ?) se ramène en quelque sorte a savoir si la courbe elliptique $y^2 = x^3 - B^2x$ a un point rationnel d'ordre infini (ce qui est équivalent a trouver un point rationnel (x,y) avec $y \neq 0$). La conjecture BSD prédit que la courbe elliptique a un point d'ordre infini si B est congru à 5,6 ou 7 mod 8. (ie que le rang de la courbe est impair). Par contre on ne sait pas construire de tels points...

Pour l'équation de Pell on sait écrire des solutions à l'aide des fonctions circulaires... Heegner a eu l'idée d'utiliser des fonctions modulaires pour construire des points rationnels sur des courbes elliptiques. Cette idée lui a permis de déterminer tous les corps quadratiques imaginaires de nombre de classes 1. Birch a étendu les idées de Heegner pour construire

des points rationnels d'ordre infini sur certaines courbes elliptiques. Les seules méthodes connues jusqu'alors étant d'écrire les coordonnées et de vérifier que ça marche. Malheureusement les points de Heegner ne fournissent pas toujours des points d'ordre infini...

5.2 Les points de Heegner, d'après Birch

Dans cette partie je vais introduire les points de Heegner d'une courbe elliptique *via* les points de Heegner d'une courbe modulaire. Je suis de très près l'article de Birch [1].

Rappelons les notations :$Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$, $X_0(N)$ est sa completion. Si $z \in \mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$, on garde z pour désigner le point de $X_0(N)$. W_N était l'involution d'Atkin-Lehner $z \mapsto -1/Nz$ sur $X_0(N)$, et $J_0(N)$ est la jacobienne de $X_0(N)$. $j(z)$ est l'invariant modulaire et $j_N(z) = j(Nz)$. On peut montrer que les fonctions de $X_0(N)$ (*i.e.* les fonctions méromorphes sur $\mathcal{H}$ invariantes par $\Gamma_0(N)$) sont exactement les fonctions rationnelles en j et j_N (ce résultat pourrait être énoncé dans la section sur les courbes elliptiques sur $\mathbb{C}$). Il existe un polynôme $F_N \in \mathbb{Z}[u,v]$ qui lie j et j_N : $F_N(j, j_N) = 0$. La courbe $Z_0(N)$ d'équation $F_N(u,v) = 0$ est un modèle pour $X_0(N)$. Soit $\theta : z \mapsto (j(z), j(Nz))$ l'application de $X_0(N)$ sur $Z_0(N)$.

Soit $\omega \in \mathcal{H}$ de degré 2 sur $\mathbb{Q}$. Il existe $A, B, C \in \mathbb{Z}$ premiers entre eux dans leur ensemble, avec $B^2 < 4AC$. Donc $\Delta(\omega) = B^2 - 4AC$, le discriminant de ω est négatif.

Définition 5.1. On dit que ω est un *point de Heegner* de $X_0(N)$ si $\Delta(\omega) = \Delta(N\omega)$. C'est-à-dire si il correspond à un couple de courbes elliptiques munies d'une isogénie cyclique d'ordre N, toutes deux de même multiplication complexe.

Rappelons que l'anneau des endomorphismes d'une courbe elliptique $E = \mathbb{C}/\Lambda$ sur $\mathbb{C}$ est $\{\alpha \in \mathbb{C}, \alpha\Lambda \subset \Lambda\}$. En utilisant l'interprétentation de $X_0(N)$ en termes d'espaces de modules, on peut dire qu'un point de Heegner correspond à un couple de courbes elliptiques N-isogènes $(E, E') = (\mathbb{C}/\Lambda_\tau, \mathbb{C}/\Lambda_{N\tau})$ de même multiplication complexe, c'est-à-dire que $\mathrm{End}(E) = \mathrm{End}(E') = \mathcal{O}$ où $\mathcal{O}$ est un ordre d'un certain corps quadratique imaginaire... $\mathbb{Q}(\omega)$.

Précisons un peu les choses : si ω est un point de Heegner de $X_0(N)$, il vérifie l'équation $NA'\omega^2 + B\omega + C = 0$ avec $(NA', B, C) = (A', B, NC) = 1$, alors $W_N(\omega)$ est le point de Heegner vérifiant $NC\widetilde{\omega}^2 - B\widetilde{\omega} + A' = 0$, et si l'image de ω dans $Z_0(N)$ est (u,v) celle de $W_N(\omega)$ est (v,u). Une condition nécessaire non suffisante pour qu'il existe un point de Heegner de discriminant $\Delta = B^2 - 4AC$ est que Δ soit un entier négatif, carré modulo $4N$.

La théorie du corps de classe dit que $K(\omega) = \mathbb{Q}(\omega, j(\omega))$ est le ring class field de l'ordre $R(\omega) = \mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right]$ de discriminant Δ. Soit $H = \mathrm{Gal}(K(\omega)/\mathbb{Q})$ et $G = \mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega))$. G est isomorphe au groupe des classes d'idéaux de l'anneau $R(\omega)$, et H est un groupe diédral, extension de G par la conjugaison complexe. A ω on associe le réseau $\mathbb{Z} + \omega\mathbb{Z}$ et donc une classe d'idéaux. Si $\mathbb{Z} + \omega_1\mathbb{Z}, \ldots, \mathbb{Z} + \omega_h\mathbb{Z}$ est un système de représentants des classes d'idéaux de $R(\omega)$, alors $j(\omega_1), \ldots, j(\omega_h)$ est un ensemble de complexes conjugués sous G.

On peut voir j comme une fonction des classes d'idéaux en posant , si $\alpha\mathbb{Z} + \beta\mathbb{Z}$ est un réseau avec $\mathrm{Im}\,(\alpha/\beta) > 0$ correspondant à la classe $\mathfrak{a}$, $j(\mathfrak{a}) = j(\alpha/\beta)$. Si $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ sont des représentants des classes d'idéaux de $R(\omega)$, les $j(\mathfrak{a}_k)$ forment un système complet de conjugués de $K(\omega)/\mathbb{Q}(\omega)$. On peut remarquer que $j(\mathfrak{a}^{-1}) = \overline{j(\mathfrak{a})}$. Les points de Heegner de $Z_0(N)$ sont les points $\Sigma(\mathfrak{n}) = \{(j(\mathfrak{a}_k), j(\mathfrak{n}\mathfrak{a}_k),\ k = 1, \ldots, h\}$ où $\mathfrak{n}$ est un idéal de $R(\omega)$

de norme N. Le nombre de points de Heegner de $Z_0(N)$ de discriminant Δ est νh, où ν est le nombre de classes d'idéaux de $R(\omega)$ représentés par des idéaux de norme N. $\Sigma(\mathfrak{n})$ est un système de conjugués sur $\mathbb{Q}(\omega)$, donc $\Sigma(\mathfrak{n}) = \{\sigma\theta(\omega),\ \sigma \in G\}$, si ω est un point de Heegner. W_N envoie $\Sigma(\mathfrak{n})$ sur $\Sigma(\mathfrak{n}^{-1}) = \{(j(\mathfrak{n}\mathfrak{a}_k), j(\mathfrak{a}_k), k = 1, \ldots, h\}$ qui est en fait l'ensemble des conjugués complexes de $\Sigma(\mathfrak{n})$. De même, si ω est un point de Heegner de $X_0(N)$, $T(\omega) = \sum_{\sigma\in G} \sigma\theta(\omega)$ est un point de $J_0(N)$ fixé par G donc est à coordonnées dans $\mathbb{Q}(\omega)$, et $T(W_N\omega)$ est le conjugué complexe de $T(\omega)$.

Si E est une courbe elliptique sur $\mathbb{Q}$ et $\varphi : X_0(N) \longrightarrow E$ définie sur $\mathbb{Q}$ avec $\varphi(i\infty) = 0$. W_N agit sur E. Nous supposerons que cette action est non triviale (on dit dans ce cas que E est paire... le cas impair étant celui où W_N agit trivialement). Alors $\varphi(i\infty) + \varphi(0) = \varphi(z) + \varphi(W_N(z))$ et donc comme $\varphi(i\infty) = 0$ on a $\varphi(W_N(z)) = \varphi(0) = \varphi(z)$. Remarquons que $\varphi(0)$ est un point de torsion de E.

Remarque 5.2. Si E est paire, la conjecture BSD prédit que le rang de E doit être pair et que si $\Delta < 0$ est un carré modulo $4N$ le rang du twist $E^{(\Delta)}$ de E par $\sqrt{\Delta}$ devrait être impair. C'est pourquoi on cherche à construire des points rationnels de $E^{(\Delta)}$. Rappelons que le twist est une courbe sur $\mathbb{Q}$ qui est équivalente à E sur $\mathbb{Q}(\sqrt{\Delta})$ mais pas sur $\mathbb{Q}$.

Si ω est un point de Heegner de $X_0(N)$ de discriminant Δ, $\varphi(\omega)$ est un point de E qui est $K(\omega)$-rationnel. Soit $P(\omega) = \sum_{\sigma\in G} \sigma\varphi(\omega)$, alors $P(\omega)$ est $\mathbb{Q}(\omega)$-rationnel et $\overline{P(\omega)} = P(W_N(\omega)) = h\varphi(0) - P(\omega)$. Donc ce point $P(\omega)$ n'est pas réel sauf éventuellement si $h\varphi(0)$ est divisible par 2. Si h est impair et $\varphi(0)$ non divisible par 2, $P(\omega) - \overline{P(\omega)}$ est un point $\mathbb{Q}$-rationnel de $E^{(\Delta)}$. On en déduit le

Théorème 5.3. *Si $\varphi(0)$ n'est pas divisible par 2 sur E et si p est premier avec $-p \equiv a^2 \bmod 4N$, then $E^{(-p)}$ a un point rationnel non trivial.*

La preuve utilise le fait que les corps quadratiques imaginaires de nombre de classes impair autres que $\mathbb{Q}(i)$ et $\mathbb{Q}(i\sqrt{2})$ sont ceux de discriminant premier.

Le point non trivial de $E^{(-p)}$ ne peut pas être d'ordre fini. donc $E^{(-p)}$ est de rang positif.

5.3 La théorie de la multiplication complexe

Soit $K \subset \mathbb{C}$ un corps quadratique imaginaire. On se fixe une cloture algébrique $\bar{K}$ dans $\mathbb{C}$. On sait que ces corps sont de la forme $\mathbb{Q}(\omega_D)$ où $D < 0$ est le discriminant de K et $\omega_D = \frac{1+\sqrt{D}}{2}$ si $D = 4k + 1$, $\frac{\sqrt{D}}{2}$ sinon.

Définition 5.4. Un ordre de K est un sous anneau $\mathcal{O}$ de K, qui engendre K comme $\mathbb{Q}$-espace vectoriel, et est de type fini comme $\mathbb{Z}$-module. Tout ordre est inclus dans l'ordre maximal $\mathcal{O}_K = \mathbb{Z}[\omega_D]$ de K, et est entièrement déterminé par son conducteur c, un entier tel que $\mathcal{O} = \mathbb{Z} \oplus c\omega_D\mathbb{Z}$.

Soit $E = \mathbb{C}/\Lambda$ une courbe elliptique sur $\mathbb{C}$. On peut identifier son anneau d'endomorphisme avec $\{\alpha \in \mathbb{C}\ , \alpha\Lambda \subset \Lambda\}$. On peut montrer que cet anneau est soit $\mathbb{Z}$, soit un ordre d'un corps quadratique imaginaire.

Définition 5.5. On dit que la courbe elliptique $E/\mathbb{C}$ est à multiplication complexe par $\mathcal{O}$, si son anneau d'endomorphismes est un ordre d'un corps quadratique imaginaire isomorphe à $\mathcal{O}$.

Si E est à multiplication complexe par $\mathcal{O}$, le réseau des périodes de E est un $\mathcal{O}$-module projectif de rang 1, dont la classe d'isomorphisme ne dépend que de celle de E, et réciproquement... on a donc une bijection entre l'ensemble des classes d'isomorphismes de courbes elliptiques à multiplication complexe par $\mathcal{O}$ et l'ensemble des classes d'isomorphismes de $\mathcal{O}$-modules projectifs. Ce dernier ensemble est le groupe de Picard de $\mathcal{O}$ $Pic(\mathcal{O})$. Si $\mathcal{O} = \mathcal{O}_K$, ce groupe est isomorphe au groupe des classes d'idéaux de K. Dans tous les cas on sait que $Pic(\mathcal{O})$ est fini. Il y a donc un nombre fini de classes d'isomorphismes de courbes elliptiques à multiplication complexe par $\mathcal{O}$. On note $Ell(\mathcal{O}) = \{E_1 \dots E_h\}$ cet ensemble.

Théorème 5.6. *Les invariants $j(E_1), \dots, j(E_h)$ sont algébriques.*

On peut identifier $\mathcal{O} = End(E)$ à un sous-anneau de $\mathbb{C}$ par $\forall \alpha \in \mathcal{O}\ \alpha^* \omega_E = \alpha \omega_E$ SiE et ses endomorphismes sont définis sur un corps L, ceci à un sens et fournit un morphisme $\mathcal{O} \to L$. $Pic(\mathcal{O})$ agit simplement transitivement sur $Ell(\mathcal{O})$ par $[\Lambda] * [E] = Hom(\Lambda, E)$. Si $\mathfrak{p}$ est un idéal premier de K de norme première à c (le conducteur de $\mathcal{O}$), alors l'inclusion $\mathfrak{p} \to \mathcal{O}$ fournit une isogénie $E = Hom(\mathcal{O}, E) \to Hom(\mathfrak{p}, E)$, dont le noyau s'identifie avec la $\mathfrak{p}$-torsion $E[\mathfrak{p}] = Hom(\mathcal{O}, E[\mathfrak{p}])$. (éléments annulés par tous ceux de $\mathfrak{p}$). On a donc $[\mathfrak{p}] * [E] = E/E[\mathfrak{p}]$.

On peut voir que l'action de $Pic(\mathcal{O})$ sur $Ell(\mathcal{O})$ commute avec l'action naturelle de $G_K = Gal(\bar{K}/K)$: cette action ce traduit par un morphisme $\eta : G_K \longrightarrow Pic(\mathcal{O})$ qui vérifie $\sigma(E) = \eta(\sigma) * E$ pour tout $\sigma \in G_K$. Les $j(E_i)$ sont donc définis sur une extension abélienne $H = \bar{K}^{Ker\eta}$ de K.

Soit $\mathbb{A}_f(K) \subset \prod_{l \neq \infty}(K \otimes \mathbb{Q}_l)$ l'anneau des adèles finies de K, et $\widehat{\mathcal{O}} = \prod_{l \neq \infty}(\mathcal{O} \otimes \mathbb{Z}_l)$ l'adhérence de $\mathcal{O}$ dans $\mathbb{A}_f(K)$. Si λ est un premier de K, K_λ est la completion par rapport à λ. On peut voir $K_\lambda^\times$ dans $\mathbb{A}_f^\times(K)$. Si $x \in K_\lambda^\times$ on note $\iota_\lambda(x)$ l'idèle correspondante. On peut identifier $Pic(\mathcal{O})$ à $\mathbb{A}_f^\times(K)/K^\times \widehat{\mathcal{O}}^\times$ où une classe d'idèle α correspond à une classe d'homothétie du réseau $(\alpha^{-1}\widehat{\mathcal{O}}) \cap K \subset \mathbb{C}$. La théorie du corps de classe donne le théorème suivant :

Théorème 5.7. *Il existe une extension abélienne H_c de K qui est non-ramifiée en tout premier ne divisant pas c, et dont le groupe de Galois s'identifie à $Pic(\mathcal{O})$ par l'application d'Artin. On appelle cette extension ring class field de K associé à $\mathcal{O}$ ou ring class field de conducteur c.*

Rappelons que si $\mathfrak{p}$ est un idéal premier de K, premier avec c, si on note $\pi_\mathfrak{p}$ l'uniformisante de $K_\mathfrak{p}$ et par $[\mathfrak{p}]$ la classe de $\iota_\mathfrak{p}(\pi_\mathfrak{p})$ dans $Pic(\mathcal{O})$, l'application de réciprocité d'Artin $rec : Pic(\mathcal{O}) \longrightarrow Gal(H_c/K)$ envoie l'élément $[\mathfrak{p}]$ sur l'inverse $\sigma_\mathfrak{p}^{-1}$ du Frobénius en $\mathfrak{p}$ $\sigma_\mathfrak{p}$.

L'extension H décrite précédemment en tant que corps de définition des invariants $j(E_i)$ est en fait le ring class field H_c. Plus précisemment, si $\mathfrak{p}$ ne divise pas c, on a $\eta(\sigma_\mathfrak{p}) = [\mathfrak{p}] \in Pic(\mathcal{O})$.

Soit $z \in \mathcal{H}$. On défini l'ordre associé à z :

$$\mathcal{O}_z = \{\gamma \in M_2(\mathbb{Z}),\ det(\gamma) \neq 0 \text{ et } \gamma z = z\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Les éléments de $\mathcal{O}_z$ sont exactement les matrices à coefficients entiers qui ont $\begin{pmatrix} z \\ 1 \end{pmatrix}$ et $\begin{pmatrix} \bar{z} \\ 1 \end{pmatrix}$ pour vecteurs propres. $\mathcal{O}_z$ est un sous-anneau commutatif de $M_2(\mathbb{Z})$. On a une application qui associe à $\gamma \in \mathcal{O}_z$ la valeur propre t_γ : $\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = t_\gamma \begin{pmatrix} z \\ 1 \end{pmatrix}$. On peut

donc voir $\mathcal{O}_z$ comme sous-anneau de $\mathbb{C}$. De plus $\mathcal{O}_z$ est un ordre isomorphe à l'anneau des endomorphismes de la courbe $E_z = \mathbb{C}/ < 1, z >$ (car la multiplication par t_γ conserve le réseau $< 1, z >$ et donc induit un endomorphisme complexe m_γ de E_z : $\gamma \mapsto m_\gamma$ identifie $\mathcal{O}_z$ à $End_{\mathbb{C}}(E_z)$.

Si $\mathcal{O}$ est un ordre d'un corps quadratique imaginaire $K \subset \mathbb{C}$, on a donc $CM(\mathcal{O}) = \{z \in \mathcal{H}/SL_2(\mathbb{Z}),\ \mathcal{O}_z = \mathcal{O}\}$. Si $\alpha \in Pic(\mathcal{O})$, il existe un idéal entier $I \subset \mathcal{O}$ qui représente α et tel que $\mathcal{O}/I$ soit cyclique. Le réseau $< 1, z > I^{-1}$ est un $\mathcal{O}$-module projectif qui admet 1 pour un de ses générateurs. On peut écrire $< 1, z > I^{-1} =< 1, z' >$ où z' est bien défini modulo l'action de $SL_2(\mathbb{Z})$. On pose alors $\alpha \star z = z'$ et on peut vérifier que c'est une action de $Pic(\mathcal{O})$ sur $CM(\mathcal{O})$ qui est compatible avec l'action de $Ell(\mathcal{O})$. On peut alors reformuler le théorème de la multiplication complexe de la façon suivante :

Théorème 5.8. *Si K est un corps quadratique imaginaire et $z \in \mathcal{H} \cap K$ est quadratique sur $\mathbb{Q}$, alors $j(z) \in H$, où H est le ring class field associé à $\mathcal{O} = \mathcal{O}_z$. De plus si $\alpha \in Pic(\mathcal{O})$ et $z \in CM(\mathcal{O})$, on a : $j(\alpha \star z) = rec(\alpha)^{-1} j(z)$.*

5.4 Définition des points de Heegner, d'après Darmon (entre autres)

Soit $N \in \mathbb{N}^\times$ et $M_0(N)$ l'anneau des matrices carrées d'ordre 2 à coefficients entiers, qui sont triangulaires supérieures modulo N ($\Gamma_0(N)$ est le groupe des unités de déterminant 1 de cet anneau).On peut maintenant associer à z un ordre de niveau N :

$$\mathcal{O}_z^{(N)} = \{\gamma \in M_0(N),\ \gamma z = z\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} = \mathcal{O}_z \cap \mathcal{O}_{Nz}.$$

En principe l'uniformisation modulaire $\Phi_N : \mathcal{H} \longrightarrow E(\mathbb{C})$ est de degré infini, on ne s'attend pas à ce qu'elle envoie des nombres algébriques sur des nombres algébriques. Pourtant, on a le théorème suivant :

Théorème 5.9. *Si $z \in \mathcal{H} \cap K$ et $\mathcal{O} = \mathcal{O}_z^{(N)}$ est son ordre de $M_0(N)$, alors $\Phi_N(z) \in E(H)$ où H est le ring class field de K associé à $\mathcal{O}$.*

Démonstration. D'après le théorème de multiplication complexe, on sait que $j(z)$ et $j(Nz)$ sont dans le ring class field H associé à $\mathcal{O}_z \cap \mathcal{O}_{Nz}$. $\Phi_N(z)$ est l'image d'un point de $X_0(N)(H)$ par l'uniformisation modulaire Φ_N. Mais l'application $X_0(N) \longrightarrow E$ induite par Φ_N est un morphisme de courbes algébriques sur $\mathbb{Q}$, donc $\Phi_N(z) \in E(H)$.

Si $\mathcal{O}$ est un ordre d'un corps quadratique imaginaire $K, CM(\mathcal{O}) = \{z \in \mathcal{H}/\Gamma_0(N),\ \mathcal{O}_z^{(N)} = \mathcal{O}\}$. On peut relever l'action de $Pic(\mathcal{O})$ à $CM(\mathcal{O}) \subset \mathcal{H}/\Gamma_0(N)$ en posant $\alpha \star_N z = z'$ où $z' \in \mathcal{H}$ est tel que $\alpha \star z = z'$ et $\alpha \star Nz = Nz'$ modulo $SL_2(\mathbb{Z})$. (z' est déterminé modulo l'action de $\Gamma_0(N)$. On a alors le :

Théorème 5.10 (Loi de réciprocité de Shimura)**.** *Si $z \in CM(\mathcal{O})$ et $\alpha \in Pic(\mathcal{O})$, alors $\Phi_N(\alpha \star z) = rec(\alpha^{-1})\Phi_N(z)$*

Exemple : Un des principaux intérêt de cette théorie est son caractère explicite : on sait construire des points de E sur des ring class field de corps quadratiques imaginaires.

La courbe elliptique de plus petit conducteur $N = 11$ a pour équation $y^2 + y = x^3 - x^2 - 10x - 20$. L'ordre de corps quadratique imaginaire de plus petit discriminant qui se plonge dans $M_0(11)$ est $\mathcal{O}_K = \mathbb{Z}(\frac{1+\sqrt{-7}}{2})$. Le corps K a pour nombre de classe 1, et l'ordre $\mathcal{O} = \mathbb{Z} + \mathbb{Z} \begin{pmatrix} -4 & -2 \\ 11 & 5 \end{pmatrix}$ est un ordre de $M_0(11)$ isomorphe à $\mathcal{O}_K$. (il est unique à conjugaison près

par le normalisateur de $\Gamma_0(11)$ dans $PGL_2(\mathbb{Q})$. Le point fixe z de cet ordre est $z = \frac{-9+\sqrt{-7}}{22}$. On peut calculer les coefficients $a_n(E)$ de la forme modulaire f en comptant les points mod p ou en utilisant $f = \sum_{n\geqslant 1} a_n q^n = q\prod_{n\geqslant 1}(1-q^{11n})^2(1-q^n)^2$. On peut tronquer cette série à l'ordre 1000, si $q = e^{2i\pi z}$, on calcule l'image de $t = \sum_{n=1}^{1000} \frac{a_n}{n} q^n$ dans $E(\mathbb{C})$ par l'uniformisation de Weierstrass qui donne un point (x, y) dont les 35 premières décimales correspondent à $(\frac{1-\sqrt{-7}}{2}, -2-2\sqrt{-7})$.

5.5 Quelques propriétés

On peut montrer que si $\mathcal{O}$ est un ordre de discriminant premier à N, alors $CM(\mathcal{O})$ n'est pas vide ssi tous les premiers divisant N se décomposent dans $K/\mathbb{Q}$. On est donc ammené à faire l'hypothèse de Heegner suivante : Tous les facteurs premiers l de N se décomposent dans $K/\mathbb{Q}$.

Si n est premier avec N, et $\mathcal{O}_n$ l'ordre de K de conducteur n, un point $\Phi_N(z)$ avec $z \in CM(\mathcal{O}_n)$ est appelé point de Heegner de conducteur n. On note $HP(n) \subset E(H_n)$ leur ensemble. (H_n est le ring class field de conducteur n).

Proposition 5.11. *Si $n \in \mathbb{Z}$ et l premier sont premiers avec N. Soit $P_{nl} \in HP(nl)$. Alors il existe des points $P_n \in HP(n)$ (et si l divise n des points $P_{n/l} \in HP(n/l)$) tels que $Tr_{H_{nl}/H_n}(P_{nl} = a_l P_n$ si l ne divise pas n et est inerte dans K, $(a_l - \sigma_\lambda - \sigma_\lambda^{-1})P_n$ si $l = \lambda\bar{\lambda}$ ne divise pas n et se décompose dans K, $(a_l - \sigma_\lambda)P_n$ si $l = \lambda^2$ se ramifie, et $a_l P_n - P_{n/l}$ si l divise n.*

Un élément de $Gal(H/\mathbb{Q})$ qui n'est pas l'identité sur K est appelé réflexion. Toutes les réflexions sont d'ordre 2 et diffèrent par multiplication par un élément de $Gal(H/K)$. On a la :

Proposition 5.12. *Si $\tau \in Gal(H/\mathbb{Q})$ est une réflexion, il existe $\sigma \in Gal(H/K)$ tel que $\tau P_n = -signe(E,\mathbb{Q})\sigma P_n$ modulo $E(H)_{tors}$, où $signe(E,\mathbb{Q})$ est le signe de l'équation fonctionnelle de $E/\mathbb{Q}$.*

Définition 5.13. Un système de Heegner pour (E, K) est un ensemble de points $P_n \in E(H_n)$ indexé par les entiers n premiers à N, qui vérifient les conditions des propositions précédentes. Cette définition a un sens pour tout corps quadratique K (s'il est réel, tout est à prendre au sens restreint). on dit que le système n'est pas trivial s'il un au moins des P_n n'est pas de torsion.

Dans le cas d'un corps quadratique imaginaire satisfaisant l'hypothèse de Heegner, on a existence d'un système de Heegner non trivial.

5.6 Applications

On peut déjà vérifier que l'existence de systèmes de Heegner est liée à la conjecture de Birch et Swinnerton-Dyer, ce que je ne ferai pas.

Gross-Zagier : Si $E/\mathbb{Q}$ est une courbe elliptique et K quadratique imaginaire vérifiant l'hypothèse de Heegner. P_n la collection des points de Heegner issus de $HP(n)$. $P_K = Tr_{H_1/K}(P_1) \in E(K)$. Alors si $<,>$ est la hauteur de Néron-Tate étendue en un accouplement hermitien sur $E(H_n) \otimes \mathbb{C}$, on a $< P_k, P_K >= L'(E/K, 1)$

Kolyvagin : Si P_K n'est pas de torsion, $E(K)$ est de rang 1 et P_K engendre un sous groupe d'indice fini de $E(K)$. De plus Ш(E/K) est fini.

Gross-Zagier et Kolyvagin : Si $ord_{s=1}(L(E,s)) \leqslant 1$ alors $rang(E(\mathbb{Q})) = ord_{s=1}(L(E,s))$ et $Ш(E/\mathbb{Q})$ est fini.

Remarque 5.14. Les points de Heegner sont en fait ici utilisés pour construire un point rationnel d'ordre infini dans le cas où $L' = 0$...

Références

[1] **B.J. Birch**, *Heegner points of elliptic curves*, Symp. Mat . vol 15, p 441-445. Academic press, London, 1975.

[2] **H. Darmon**, *Rational points on modular elliptic curves*,CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC.

[3] **Diamond, Shurman**, *A first course in Modular Forms*, Springer GTM 228

[4] **Y. Hellegouarch**, *Invitation aux mathématiques de Fermat-Wiles*, Dunod 2000

[5] **D. Hüsemoller**, *Elliptic curves*, Springer, 1987

[6] **N. Koblitz**, *Elliptic curves and modular forms*, Springer

[7] **J. Milne**, *Modular functions and modular forms*, www.jmilne.org

[8] **J.Milne**, *Elliptic curves*, www.jmilne.org

[9] **J-P. Serre**, *Cours d'arithmétique*, P.U.F

[10] **J.H. Silverman**, *The Arithmetic of Elliptic Curves*, Springer 1986

[11] **J.H. Silverman**, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer 1994