Unités elliptiques et série d'Eisenstein

sous la direction de Pierre Charollois

Nicolas Provost

30 octobre 2009

Table des matières

Résumé

Les unités elliptiques ont un rôle crucial dans les calculs sur les courbes elliptiques sur un corps quadratique. Elles correspondent, via une représentation simple, au générateur de ce groupe de type fini sur $\mathbb{Z}$. Lorsque le corps est quadratique réel, la construction de telles unités se fait par introduction d'une mesure sur un espace $\mathbb{X}$. Cette mesure est caractérisée par certaine spécification de E_2 la série d'Eisenstein standard de poids 2 et de niveau 1. Son évaluation sur une base correspondent à une variation de niveau et ces moments à une variation du poids.

1 Formes modulaires classiques

1.1 Quelques généralités

Le demi-plan de Poincaré est noté $\mathcal{H} := \{z \in \mathbb{C}; Im(z) > 0\}$ et le groupe de Hecke de niveau N se note $\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}); N|c\}$.
Une action de SL_2 sur $\mathcal{H}$ est alors donnée par : $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).z = \frac{az+b}{cz+d}$.
Une application holomorphe $f : \mathcal{H} \to \mathbb{C}$ est appelée forme modulaire de poids k et de niveau N dès lors que :

$$\forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N), f(\gamma.z) = (cz+d)^k f(z),$$

$$\forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}), \exists h \in \mathbb{Z}_{>0}, \frac{f(\gamma.z)}{(cz+d)^k} = \sum_{n \geq 0} a_n^\gamma e^{2i\pi nz/h}.$$

De plus, une forme modulaire est une forme pointe si : $\forall \gamma \in SL_2(\mathbb{Z}), a_0^\gamma = 0$.
Le $\mathbb{C}$-espace vectoriel des formes pointes de poids k et de niveau N est noté $S_k(N)$.

Une application $f \in S_k(N)$ est 1-périodique, en effet $f(z+n) = f((\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}).z) = f(z)$.
Le développement en série de Fourier, $f(z) = \sum a_n e^{2i\pi nz}$, permet de définir alors la série de Dirichlet :

$$L(f,s) := \sum_{n>0} a_n n^{-s}.$$

Un calcul simple de transformée de Mellin donne la relation plus intrinsèque :

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

Proposition 1. *L'ensemble des orbites $Y_0(N)(\mathbb{C}) := \mathcal{H}/\Gamma_0(N)$ est une surface de Riemann dont les pointes sont en bijection avec $\mathbb{P}_1(\mathbb{Q})/\Gamma_0(N)$.*
On note désormais $\mathcal{H}^* := \mathcal{H} \sqcup \mathbb{P}_1(\mathbb{Q})$.
La surface obtenue $X_0(N)(\mathbb{C}) := \mathcal{H}^*/\Gamma_0(N)$ est une surface de Riemann compacte.
Et $S_2(N) \to \Omega^1(X_0(N)(\mathbb{C})), f \mapsto \omega_f := 2i\pi f(z)dz$ est un isomorphisme.

Définition 1. *Les opérateurs de Hecke sont définis comme les endomorphismes continus des fonctions holomorphes sur $\mathbb{H}$ donnés, pour p premier, par :*

$$T_p f(z) := \begin{cases} \frac{1}{p}\sum_{i=0}^{p-1} f(\frac{z+i}{p}) + pf(pz) & \text{si } p \nmid N \\ \frac{1}{p}\sum_{i=0}^{p-1} f(\frac{z+i}{p}) & \text{sinon} \end{cases}.$$

Le développement suivant étend la définition à n entier :

$$\sum T_n n^{-s} := \prod_{p\nmid N}(1 - T_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - T_p p^{-s})^{-1}.$$

1.2 Lien avec les courbes elliptiques

Définition 2. *Pour une courbe elliptique E définie sur $\mathbb{Z}$, on dispose de la réduction modulo p pour tout entier p premier. Elles permettent de définir le conducteur N de la courbe E puis les entiers $a_p := p + 1 - \#E(\mathbb{F}_p)$ si E a bonne réduction mod p et 0, 1 ou -1 selon la dégénérescence. La série de Dirichlet suivante permet de les combiner et d'étendre la définition des a_n pour n entier naturel quelconque :*

$$L(E,s) := \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p p^{-s})^{-1} = \sum_{n>0} a_n n^{-s}.$$

Théorème 1 (Eichler-Shimura)**.** *Soit $f \in S_2^{new}(N)$ une fonction propre normalisée à coefficients de Fourier entiers. Alors il existe une courbe elliptique E_f définie sur $\mathbb{Q}$ telle que $L(f,s) = L(E_f, s)$*

Remarque 1. *La démonstration du Théorème* 1 *donne lieu à une paramétrisation $\Phi_N : \mathcal{H}/\Gamma_0(N) \to E_f(\mathbb{C})$. On recherche ainsi les $u \in \mathcal{H}/\Gamma_0(N)$, appelés unités elliptiques, s'envoyant sur les générateurs du groupe de type fini $E_f(K)$ pour K extension finie de $\mathbb{Q}$.*

Théorème 2 (Wiles)**.** *Pour toute courbe elliptique E définie sur $\mathbb{Q}$ de conducteur N, il existe une forme modulaire $f \in S_2(N)$ telle que $L(E,s) = L(f,s)$.*
De plus, E est $\mathbb{Q}$-isomorphe à E_f.

Corollaire 1 (Fermat-Wiles)**.** *Pour tout $n > 2$, il n'existe pas de solution entière non trivial à l'équation $a^n + b^n = c^n$.*

1.3 Unités elliptiques pour un corps quadratique imaginaire

Définition 3. *Une fonction holomorphe sur $\mathcal{H}/\Gamma_0(N)(\mathbb{C})$ qui ne s'annule pas et qui se prolonge en une application méromorphe à $X_0(N)(\mathbb{C})$ est appelée unité modulaire pour $\Gamma_0(N)$.*

Exemple 1. *Soit Δ la forme modulaire de niveau 1 et de poids 12.*

$$\Delta(z) := q \prod (1-q^n)^{24} \text{ où } q = e^{2i\pi z}.$$

Pour tout diviseur $\delta = \sum_{d|N} n_d[d] \in D_N^0$ de degré 0, $\Delta_\delta(z) = \prod_{d|N} \Delta(dz)^{n_d}$ est une unité modulaire pour $\Gamma_0(N)$.

Soit $K = \mathbb{Q}(\tau)$ corps quadratique imaginaire tel que $\tau \in \mathcal{H}$.

Soient $M_0(N) \subset M_2(\mathbb{Z})$ l'ensemble des matrices triangulaires supérieures modulo N et $\mathcal{O}_\tau := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_0(N); a\tau + b = \tau(c\tau + d)\}$ le sous-anneau de $M_0(N)$ identifié à un sous-anneau de $\mathbb{C}$ via l'application : $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto c\tau + d$. Il est isomorphe soit à $\mathbb{Z}$ soit à un ordre de K.

Pour un ordre $\mathcal{O}$ de K fixé de discriminant $-D$ premier à N, le sous-espace $\mathcal{H}^{\mathcal{O}} := \{\tau \in \mathcal{H}$ tel que $\mathcal{O}_\tau = \mathcal{O}\}$ est préservé par $\Gamma_0(N)$. L'ensemble $\mathcal{H}^{\mathcal{O}}/\Gamma_0(N)$ ainsi considéré est alors fini.

Décomposant $\tau = u + iv$, la forme quadratique $\tilde{Q_\tau}(x, y) = v^{-1}(x - y\tau)(x - y\bar{\tau})$ permet de définir Q_τ la forme quadratique primitive qui lui est proportionnelle.
Ainsi $Q_\tau(x, y) = Ax^2 + Bxy + Cy^2$ vérifie : $A > 0$, N divise A, $B^2 - 4AC = -D$ et A, B et C sont premiers entre eux.

Le théorie des corps de classes fournit une extension abélienne H/K et une application rec : $Pic(\mathcal{O}) \to Gal(H/K), \mathfrak{P} \cap \mathcal{O} \mapsto (Fr_{\mathfrak{P}})^{-1}$.

L'unité $u(\delta, \tau) := \Delta_\delta(\tau)$ vérifie alors $u(\delta, \tau) \in \mathcal{O}_H[1/N]^\times$.

Définition 4. *Soit $\zeta_Q(s) := \sum\limits_{(m,n)\neq(0,0)} Q(m, n)^{-s}$ où Q est une forme quadratique. La fonction zeta associée à l'unité modulaire Δ_δ est alors :*

$$\zeta(\delta, \tau, s) := \sum_{d|N} n_d d^{-s} \zeta_{Q_{d\tau}}(s),$$

pour $\tau \in \mathcal{H}$ quadratique et $Re(s) > 1$.

Théorème 3. *Soit $\tau \in \mathcal{H}^{\mathcal{O}}/\Gamma_0(N)$.*
La fonction $\zeta(\delta, \tau, s)$ se prolonge de manière holomorphe au plan complexe sauf en $s = 1$ où elle admet un pôle simple.
De plus elle s'annule en 0 et :

$$\zeta'(\delta, \tau, 0) = -\frac{1}{12} \log Norm_{\mathbb{C}/\mathbb{R}}(u(\delta, \tau)).$$

1.4 Conjectures de Stark

Soient K un corps de nombres et χ un caractère de Dedekind généralisé pour l'anneau de Dedekind $\mathcal{O}_K$. On dispose de la fonction L associée à χ :

$$L(s, \chi) := \sum_{I \subset \mathcal{O}_K} \frac{\chi(I)}{N(I)^s} = \sum_{k=1}^{r} \chi(I_k) \sum_{I \equiv I_k} N(I)^{-s}.$$

où $Cl(K) = \{I_1, ..., I_r\}$ est le groupe des classes d'idéaux de K et $I \equiv I_k$ si et seulement s'il existe $a \in I_k$ tel que $II_k^{-1} = (a)$.

Il est alors naturel de considérer la fonction zeta partielle associée à $I_k \in Cl(K)$:

$$\zeta(s, I_k) := \sum_{I \equiv I_k} N(I)^{-s} = N(I_k)^{-s} \sum_{a \in I_k} N(a)^{-s}.$$

Pour $K = \mathbb{Q}(\tau)$ quadratique imaginaire, tout $I_k \in Cl(K)$ est un ordre de K. Supposons τ choisi de sorte que $I_k = \mathbb{Z} + \tau\mathbb{Z}$, alors :

$$\zeta(s, I_k) = \sum_{m,n} N(I_k)^{-s} N_{K/\mathbb{Q}}(m + n\tau)^{-s} = \sum_{m,n} Q_\tau(m,n)^{-s}.$$

On peut tordre cette définition pour annuler $\zeta(s, I_k)$ en $s = 0$ grâce à un diviseur $\delta \in D_N^0$ et alors la formule limite de Kronecker vu précédemment donne :

$$\zeta'_\delta(0, I_k) = \zeta'(\delta, \tau, 0) = -\frac{1}{12} \log N_{\mathbb{C}/\mathbb{R}}(u(\delta, \tau)).$$

où $u(\delta, \tau)$ est une unité dans H, le corps de classe de Hilbert de K. Ce résultat nous suggère la généralisation :

Conjecture 1 (Stark)**.** *Pour tout corps de nombres K, pour toute fonction zeta partielle $\zeta(s, I)$ associée à une classe d'idéaux de K (resp. au sens étroit), si $\zeta(0, I) = 0$ alors il existe une unité $u(I)$ du corps de classe de Hilbert de K (resp. au sens étroit) telle que :*

$$\zeta'(0, I) = \log |u(I)|.$$

L'unité $u(I)$ est appelée unité de Stark.

2 Construction d'une p-unité pour un corps quadratique réel

Étant donné qu'il n'y a pas de point de K dans $\mathcal{H}$, on privilégie l'analyse p-adique.

Soit p un nombre premier inerte sur K (ne divisant pas N) totalement décomposé sur H le corps de classe de Hilbert. Soient $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la norme ultramétrique $|.|_p$ et $\mathbb{C}_p$ le complété de sa clôture algébrique $\overline{\mathbb{Q}_p}$. Un plongement de K dans $\mathbb{C}_p$ est fixé. Soit $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ le demi-plan supérieur p-adique. On préfère l'action d'un plus grand groupe que $\Gamma_0(N)$ sur $\mathcal{H}_p$:

$$\Gamma := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}[1/p]); N|c \}.$$

Pour un $\tau \in \mathcal{H}_p \cap K$, on associe désormais un ordre dans $M_0(N)[1/p]$ par :

$$\mathcal{O}_\tau := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_0(N)[1/p] \text{ tel que } a\tau + b = \tau(c\tau + d) \}.$$

Il est identifié à un $\mathbb{Z}[1/p]$-ordre dans K permettant de définir :

$$\mathcal{H}_p^{\mathcal{O}} := \{ \tau \in \mathcal{H}_p \text{ tel que } \mathcal{O}_\tau = \mathcal{O} \}.$$

où $\mathcal{O}$ est un $\mathbb{Z}[1/p]$-ordre dans K fixé.

L'ensemble $\mathcal{H}_p^{\mathcal{O}}$ est préservé sous l'action de Γ et $\mathcal{H}_p^{\mathcal{O}}/\Gamma$ est fini.

2.1 Formes analytiques rigides

L'affinoïde standard de $\mathcal{H}_p$ est l'ensemble $\mathcal{A} := red^{-1}(\mathbb{P}_1(\overline{\mathbb{F}_p}) - \mathbb{P}_1(\mathbb{F}_p))$ où $red : \mathbb{P}_1(\mathbb{C}_p) \to \mathbb{P}_1(\overline{\mathbb{F}_p})$ est la réduction modulo l'idéal maximal de l'anneau des entiers de $\mathbb{C}_p$. Ceci se traduit par la description en termes de normes p-adiques :

$$\mathcal{A} = \{ \tau \in \mathcal{H}_p; |1/\tau|_p \geq 1 \text{ et } |\tau - t|_p \geq 1, \forall t = 0, ..., p-1 \}.$$

On dispose alors de la famille des affinoïdes étant l'orbite de $\mathcal{A}$ par $PGL_2(\mathbb{Q}_p)$.

Définition 5. *Une application $f : \mathcal{H}_p \to \mathbb{C}_p$ est dite analytique rigide si sa restriction à tout affinoïde est limite uniforme d'applications rationnelles dont les pôles sont hors de l'affinoïde.*

De plus une forme analytique rigide de poids k sur $\mathcal{H}_p/\Gamma$ est une application analytique rigide f sur $\mathcal{H}_p$ vérifiant :

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \text{ pour tout } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma.$$

L'ensemble de ces formes est noté $S_k(\Gamma)$.

Comme dans le cas classique, $S_2(\Gamma)$ peut être identifié avec l'espace des formes différentielles analytiques rigides de $\mathcal{H}_p/\Gamma$. Ainsi la dimension de $S_2(\Gamma)$ sur $\mathbb{C}_p$ est le genre g de la courbe $\mathcal{H}_p/\Gamma$.

Toutefois l'utilisation de ces formes est moins pratique que dans le cas classique. On construit ainsi une nouvelle représentation via certaines mesures sur $\mathbb{P}_1(\mathbb{Q}_p)$.

2.2 Mesures sur $\mathbb{P}_1(\mathbb{Q}_p)$

Définition 6. *Tout ouvert compact de $\mathbb{P}_1(\mathbb{Q}_p)$ peut être recouvert par un nombre fini de boules ouvertes compactes de la forme :*

$$\begin{aligned} B(a,r) &:= \{t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ tel que } |t-a|_p < p^{-r}\} \\ B(\infty,r) &:= \{t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ tel que } |t|_p > p^{r}\} \end{aligned}.$$

Une mesure sur $\mathbb{P}_1(\mathbb{Q}_p)$ est une application additive bornée :

$$\mu : \{U \subset \mathbb{P}_1(\mathbb{Q}_p) \text{ ouvert et compact}\} \to \mathbb{C}_p \text{ telle que } \mu(\mathbb{P}_1(\mathbb{Q}_p)) = 0.$$

Une telle mesure permet de définir l'intégrale sur $\mathbb{P}_1(\mathbb{Q}_p)$ d'une application continue $\lambda : \mathbb{P}_1(\mathbb{Q}_p) \to \mathbb{C}_p$ par :

$$\int_{\mathbb{P}_1(\mathbb{Q}_p)} \lambda(t) d\mu(t) := \lim_{C=\{U_\alpha\}} \sum_\alpha \lambda(t_\alpha)\mu(U_\alpha).$$

où la limite est prise pour des recouvrements de plus en plus fins par des ouverts compacts disjoints et où t_α est un point quelconque de U_α.

Lemme 1. *Soit μ une mesure sur $\mathbb{P}_1(\mathbb{Q}_p)$.*
Alors l'application définie par $f_\mu(z) := \int_{\mathbb{P}_1(\mathbb{Q}_p)} \frac{d\mu(t)}{z-t}$ est analytique rigide sur $\mathcal{H}_p$.
De plus, si μ est Γ-invariante alors f_μ est une forme analytique rigide de poids 2.

Théorème 4 (Schneider-Teiltelbaum)**.** *L'application $Mes(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{C}_p)^\Gamma \to S_2(\Gamma)$, $\mu \mapsto f_\mu$ est un isomophisme de $\mathbb{C}_p$-espace vectoriel.*

Remarque 2. *Ce théorème permet de définir $S_2(\Gamma)^{\mathbb{Z}}$ comme étant l'image de $Mes(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{Z})^\Gamma$. C'est l'analogue de l'ensemble des formes modulaires à coefficients de Fourier entiers.*

L'unité elliptique étant l'évaluation d'une forme modulaire à coefficients de Fourier entiers dans le cas imaginaire. On utilisera ici l'intégration sous une mesure de $Mes(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{Z})^\Gamma$.

2.3 Intégration sur $\mathcal{H}_p$

Soit $\log_p : \mathbb{C}_p^\times \to \mathbb{C}_p$ une branche du logarithme p-adique. C'est l'homomorphisme de groupe étendant la formule $\log_p(1-z) = \sum \frac{z^n}{n}$ au voisinage de 0 et vérifiant $\log_p(p) = 0$.

Définition 7. *L'intégrale multiplicative d'une fonction analytique rigide $f \in S_2(\Gamma)^{\mathbb{Z}}$ entre τ_1 et τ_2 de $\mathcal{H}_p$ est définie par :*

$$⨰_{\tau_1}^{\tau_2} f(z)dz := ⨰_{\mathbb{P}_1(\mathbb{Q}_p)} \Big(\frac{t-\tau_2}{t-\tau_1}\Big) d\mu_f(t) := \lim_{C=\{U_\alpha\}} \prod_\alpha \Big(\frac{t_\alpha-\tau_2}{t_\alpha-\tau_1}\Big)^{\mu_f(U_\alpha)}.$$

De plus cette intégrale vérifie les propriétés classiques de $\mathbb{C}_p$-linéarité par rapport à l'intégrande et d'additivité par rapport aux bornes d'intégration.

Application : L'intégrale multiplicative permet de définir :

$$\begin{aligned} \Phi_{N,p} : & Div^0(\mathcal{H}_p) \to Hom(S_2(\Gamma)^{\mathbb{Z}}, \mathbb{C}_p^\times) \simeq (\mathbb{C}_p^\times)^g \\ & D \mapsto \Big(f \mapsto ⨰_D f(z)dz\Big) \end{aligned}$$

De plus l'image de $Ker(Div^0(\mathcal{H}_p) \to Div^0(\mathcal{H}_p/\Gamma))$ par cette application est un réseau Λ de $Hom(S_2(\Gamma)^{\mathbb{Z}}, \mathbb{C}_p^\times)$.

Ainsi $\Phi_{N,p} : Div^0(\mathcal{H}_p/\Gamma) \to (\mathbb{C}_p^\times)^g/\Lambda$ devient une paramétrisation semblable au cas classique.

2.4 Séries d'Eisenstein

Dans cette partie, on introduit une famille particulière de formes modulaires.

Définition 8. *Les séries d'Eisenstein standards de poids k pair sont données par :*

$$E_k(z) = \frac{(k-1)!}{2(2i\pi)^k} \sum_{(m,n)\neq 0} \frac{1}{(mz+n)^k} = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2i\pi nz}.$$

Remarque 3. *La première formule permet de voir que E_k est une forme modulaire formelle de poids k pour $SL_2(\mathbb{Z})$.*

Lemme 2. *Les fonctions Δ et E_2 sont reliés par la formule :*

$$d \log \Delta(z) = -24.2i\pi E_2(z) dz.$$

Proposition 2. *La série d'Eisenstein E_2 est un vecteur propre de T_p de valeur propre $p+1$. Il suit que $d\log\Delta$ et $d\log\Delta_\delta$ sont aussi vecteur propre.*

Définition 9. *On considère une nouvelle unité modulaire mieux adaptée :*

$$\Delta_\delta^*(z) = \Delta_\delta(z)/\Delta_\delta(pz).$$

Remarque 4. *On peut ajouter une condition supplémentaire à $\delta = \sum_{d|N} n_d[d]$: $\sum_{d|N} dn_d = 0$. Il existe alors un $\xi \in \mathbb{P}_1(\mathbb{Q})$ tel que Δ_δ n'a pas de pôle ni de zéro sur $\Gamma\xi$ et comme p est premier à N alors $\Gamma\xi = \Gamma_0(Np)\xi$.*

Et Δ_δ^* est bien une unité modulaire pour $\Gamma_0(Np)$.

Corollaire 2. *Les formes différentielles logarithmiques peuvent s'exprimer par :*

$$d\log\Delta_\delta(z) = 2i\pi F_2(z)dz \text{ et } d\log\Delta_\delta^*(z) = 2i\pi F_2^*(z)dz.$$

où F_2 est une série d'Eisenstein de poids 2 pour $\Gamma_0(N)$ et F_2^* pour $\Gamma_0(Np)$.

De plus le Lemme 2 permet d'établir les formules :

$$F_2(z) = -24 \sum_{d|N} dn_d E_2(dz) \text{ et } F_2^*(z) = F_2(z) - pF_2(pz).$$

2.5 Définition de $u(\delta, \tau)$

La construction qui suit est dû est Darmon (voir [3]). Il choisit de remplacer l'évaluation simple de Δ_δ par l'intégration dans un domaine connu.

Définition 10. *Les symboles modulaires sont les fonctions sur $G\xi \times G\xi$ à valeurs dans $\mathbb{Z}$, $(r,s) \mapsto m\{r \to s\}$, vérifiant la propriété de transitivité suivante :*

$$m\{r \to t\} = m\{r \to s\} + m\{s \to t\}.$$

On note $\mathcal{M}_{G\xi}$ l'ensemble de ces fonctions.

Précisons la définition pour un G-module M, $\mathcal{M}_{G\xi}(M)$ est alors l'ensemble des fonctions sur $G\xi \times G\xi$ à valeurs dans M vérifiant la propriété de transitivité et muni de l'action définie pour $g \in G$ par $(gm)\{r \to s\} = g(m\{g^{-1}r \to g^{-1}s\})$.

Proposition 3. *Il existe une unique famille de mesures $\mu_\delta\{r \to s\}$ à valeurs dans $\mathbb{Z}$ sur $\mathbb{P}_1(\mathbb{Q}_p)$ indexée par $r, s \in \Gamma\xi$ vérifiant :*

$$\mu_\delta\{r \to s\}(\mathbb{P}_1(\mathbb{Q}_p)) = 0,$$
$$\mu_\delta\{r \to s\}(\mathbb{Z}_p) = \frac{1}{2i\pi}\int_r^s d\log\Delta_\delta^*(z),$$
$$\mu_\delta\{\gamma r \to \gamma s\}(\gamma U) = \mu_\delta\{r \to s\}(U).$$

Définition 11. *Intégrale double*
Pour $\tau_1, \tau_2 \in \mathcal{H}_p$ *et* $r, s \in \Gamma\xi$*, on définit :*

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_r^s d\log \Delta_\delta = \times\!\!\!\!\!\!\int_{\mathbb{P}_1(\mathbb{Q}_p)} (\frac{t-\tau_2}{t-\tau_1}) d\mu_\delta\{r \to s\}(t).$$

Cette intégrale multiplicative a un sens car μ_δ *est à valeurs entières.*

Remarque 5. *L'intégrale double est invariante sous action de* Γ *au sens où :*

$$\times\!\!\!\!\!\!\int_{\gamma\tau_1}^{\gamma\tau_2} \int_{\gamma r}^{\gamma s} d\log \Delta_\delta = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_r^s d\log \Delta_\delta.$$

De plus il y a additivité des bornes par rapport aux deux variables.

Définition 12. *Soit* K_p *le complété p-adique de* K*. Pour* τ_1 *et* τ_2 *dans* $K_p \cap \mathcal{H}_p$*, l'intégrale multiplicative est limite d'éléments de* $K_p^\times$ *donc à valeurs dans* $K_p^\times$*.*

Ceci permet de définir le 2*-cocycle* $\kappa_\tau \in \mathcal{Z}^2(\Gamma, K_p^\times)$ *par la formule :*

$$\kappa_\tau(\gamma_1, \gamma_2) = \times\!\!\!\!\!\!\int_{\gamma_1\gamma_2\tau}^{\gamma_1\tau} \int_x^{\gamma_1 x} d\log \Delta_\delta.$$

où $\tau \in \mathcal{H}_p \cap K_p$ *et* $x \in \Gamma\xi$ *est un point base.*

L'action de Γ *sur* $K_p^\times$ *est ici prise triviale.*

Proposition 4. *On peut expliciter le changement de point base de* $\Gamma\xi$*.*

Pour tout $x, y \in \Gamma\xi$*, il existe* $\rho_{x,y} \in \mathcal{Z}^1(\Gamma, K_p^\times)$ *scindant* κ_x/κ_y *(on place ici en indice le point base de* $\Gamma\xi$*). De plus* $\rho_{x,y}$ *est trivial sur* Γ_τ *le stabilisateur de* τ *dans* Γ*.*

Démonstration: Un calcul simple montre que $\rho_{x,y}(\gamma) = \times\!\!\!\!\!\int_\tau^{\gamma\tau} \int_x^y d\log \Delta_\delta$ scinde κ_x/κ_y qui est bien trivial pour tout γ stabilisant τ.

Pour définir l'unité $u(\delta, \tau)$, il nous faut scinder κ_τ. Pour cela, il nous suffit de construire une mesure au-dessus de μ_δ sur un espace de dimension 2. Cela généralise le travail de Washington dans le chapitre 12 de [11]. Cette partie utilise des idées de Greenberg et Stevens (Voir [8]) relevant certain symbole modulaire et de Dasgupta (Voir [6]) l'appliquant à notre cas.

Soit $\mathbb{X} := (\mathbb{Z}_p \times \mathbb{Z}_p)'$ l'ensemble des couples (x, y) primitifs (i.e. x et y ne sont pas tous les deux divisible par p). Il existe notamment une application $\pi : \mathbb{X} \to \mathbb{P}_1(\mathbb{Q}_p)$. Elle est $GL_2(\mathbb{Z}_p)$-équivariante et les fibres de π sont stables sous l'action de $\mathbb{Z}_p^\times$.

Proposition 5. *Il existe* $\nu \in \mathcal{M}_{\Gamma\xi}(Mes(\mathbb{X}, \mathbb{Z}))$ *un symbole modulaire de mesure sur* $\mathbb{X}$ *étant* $\Gamma_0(N)$*-invariant et vérifiant :*
$\forall r, s \in \Gamma\xi,$

$$\nu\{r \to s\}(\mathbb{Z}_p^\times \times p\mathbb{Z}_p) = \mu_\delta\{r \to s\}(\mathbb{P}_1(\mathbb{Q}_p) - \mathbb{Z}_p) = -\psi\{r \to s\}.$$

où $\psi\{r \to s\} := \frac{1}{2i\pi} \int_r^s d\log \Delta_\delta^* \in \mathcal{M}_{\Gamma\xi}$*.*

Démonstration: Il suffit de trouver un élément ν de $M := \mathcal{M}_{\Gamma\xi}(H^0(\Gamma_0(N), Mes(\mathbb{X}, \mathbb{Z})))$ au dessus de μ_δ. On décompose cet espace.

Soient $X_n := (\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z})'$ des couples primitifs au sens précédent. Ainsi $\mathbb{X} = \varprojlim X_n$ permet de décomposer $Mes(\mathbb{X}, \mathbb{Z}) = \varprojlim Mes(X_n, \mathbb{Z})$.

Soient $\Gamma_1(p^n) := \{A \equiv (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}) \bmod p^n\}$ et $\Gamma_n := \Gamma_0(N) \cap \Gamma_1(p^n)$. L'application surjective $\phi_n : \Gamma_0(N) \to X_n, (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \mapsto (\begin{smallmatrix} \tilde{a} \\ \tilde{c} \end{smallmatrix})$ donne l'isomorphisme suivant : $\Gamma_0(N)/\Gamma_n \simeq X_n$.

La famille des symboles modulaires Γ_n-invariant définit par :

$$\varphi_n\{\gamma r \to \gamma s\} := \nu\{r \to s\}(\{x \in \mathbb{X}; x \equiv (\begin{smallmatrix} a \\ c \end{smallmatrix}) \mod p^n\}), \text{ où } \gamma = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}).$$

constitue une suite compatible codant exactement la mesure ν dès lors que :

$$\forall n > 0 \sum_{\gamma \in \Gamma_n/\Gamma_{n+1}} \varphi_{n+1}\{\gamma r \to \gamma s\} = \varphi_n\{r \to s\}.$$

La condition devient alors $\varphi_0 = \psi$.

On définit une série d'Eisenstein E_2^n de niveau $p^n N$ par :

$$E_2^n(z) = \frac{1}{12p^n} + \sum_{k=1}^{\infty} \sum_{\substack{l \equiv 1 mod p^n \\ l>0}} l e^{2i\pi klz}.$$

On lui associe les séries tordues par δ : $F_2^n(z) := -24 \sum_{d|N} dn_d E_2^n(dz)$.

Le symbole modulaire $\varphi_n\{r \to s\} = \frac{1}{2i\pi} \int_r^s F_2^n(z)dz$ convient alors comme suite compatible relevant ψ.

En effet on a la modularité de E_2^n en Γ_n et la relation pour tout $n > 0$:

$$E_2^n(z) = \sum_{a=0}^{p-1} (1 + ap^n) E_2^{n+1}((1 + ap^n)z).$$

On obtient par un calcul analogue :

$$E_2(z) = \sum_{a=1}^{p-1} a E_2^1(az) + pE_2(pz).$$

Ainsi les mêmes égalités sont valides pour les F et $F_2^*(z) = \sum_{a=1}^{p-1} aF_2^1(az)$.

D'où pour tout $r, s \in \Gamma\xi$, on a :
$\sum_{a=1}^{p-1} \varphi_1\{\left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right)r \to \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right)s\} = \frac{1}{2i\pi} \sum_{a=1}^{p-1} \int_r^s F_2^1(a^{-1}z)a^{-1}dz = \frac{1}{2i\pi} \int_r^s F_2^*(z)dz = \psi\{r \to s\}$

Remarque 6. *Il existe un opérateur U_p sur les symboles modulaires analogues à T_p donné par la formule :*

$$(U_p\phi_n)\{r \to s\} := \sum_{i=1}^{p-1} \phi_n\{\left(\begin{smallmatrix} p & 0 \\ iNp^n & 1 \end{smallmatrix}\right)r \to \left(\begin{smallmatrix} p & 0 \\ iNp^n & 1 \end{smallmatrix}\right)s\}.$$

Les séries d'Eisenstein F_2^* et F_2^n étant vecteur propre de T_p de valeur propre $p+1$, les symboles modulaires ψ et φ_n sont stables par U_p par la formule liant les opérateurs de Hecke :$U_p^2 - T_pU_p + S_p = 0$. On obtient ainsi $U_p\varphi_n = \varphi_n$.

La $\Gamma_0(N)$-invariance signifie : $\forall U \subset \mathbb{X}, \forall \gamma \in \Gamma_0(N)$,

$$\nu\{\gamma r \to \gamma s\}(\gamma U) = \nu\{r \to s\}(U).$$

Et la décomposition en composantes disjointes $\mathbb{Q}_p^2 - \{0\} = \bigcup_{k \in \mathbb{Z}} p^k \mathbb{X}$ permet d'étendre chaque mesure à $\mathbb{Q}_p^2 - \{0\}$ par la formule :

$$\nu\{r \to s\}(pU) = \nu\{r \to s\}(U).$$

Proposition 6. *Le symbole modulaire ν est Γ invariant :*

$$\nu\{\gamma r \to \gamma s\}(\gamma U) = \nu\{r \to s\}(U), \forall U \subset \mathbb{X}, \forall \gamma \in \Gamma.$$

Démonstration: Soit $P := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$. La décomposition du groupe $\Gamma =< P^{-n}\gamma P^n; \gamma \in \Gamma_0(N), n \geq 0 >$ et la symétrie en les coordonnées dans $\mathbb{X}$ permet de réduire le calcul au cas où a premier à p, c multiple de p et $U := \{x \in \mathbb{X}; x \equiv \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \mod p^n\} \subset \mathbb{Z}_p^\times \times p\mathbb{Z}_p$:

$$\nu\{Pr \to Ps\}(PU) = (U_p\varphi_n)\{\left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right)r \to \left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right)s\} = \nu\{r \to s\}(U).$$

Par l'invariance de la suite φ_n par l'opérateur U_p.

Corollaire 3. *Pour tout ouvert compact U de $\mathbb{P}_1(\mathbb{Q}_p)$,*

$$\nu\{r \to s\}(\pi^{-1}U) = \mu_\delta\{r \to s\}(U).$$

On dit que le symbole modulaire ν relève μ_δ.

Démonstration: Les translatés par Γ de $\mathbb{P}_1(\mathbb{Q}_p) - \mathbb{Z}_p$ forment une base des ouverts compacts de $\mathbb{P}_1(\mathbb{Q}_p)$. Et $\forall \gamma \in \Gamma, \pi^{-1}(\gamma U) = \gamma(\pi^{-1}U)$ par Γ-équivariante de π.

Définition 13. *On définit une forme modulaire de poids k pair pour $\Gamma_0(N)$ adaptée à Δ_δ par :*

$$F_k(z) = -24 \sum_{d|N} d n_d E_k(dz).$$

et une forme modulaire de poids k pair pour $\Gamma_0(Np)$ adaptée à Δ_δ^* par :

$$F_k^*(z) = F_k(z) - p^{k-1} F_k(pz).$$

Proposition 7. *Les moments des mesures $\nu\{r \to s\}$ peuvent être exprimés grâce aux séries d'Eisenstein par :*
$\forall h \in \mathbb{Z}[x, y]$ homogène de degré $k-2$,

$$\int_{\mathbb{X}} h(x,y) d\nu\{r \to s\}(x,y) = Re\Big((1-p^{k-2}) \int_r^s h(z,1) F_k(z) dz\Big).$$

La famille vérifie alors la propriété :

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} h(x,y) d\nu\{r \to s\}(x,y) = Re\Big(\int_r^s h(z,1) F_k^*(z) dz\Big).$$

Proposition 8. *Si $\tau \in \mathcal{H}_p^{\mathcal{O}} \subset K_p^\times$ et $r, s \in \Gamma\xi$ alors :*

$$\rho_\tau(\gamma) = \times\!\!\!\!\!\!\int_{\mathbb{X}} (x - \gamma\tau y) d\nu\{r \to \gamma r\}(x,y), \forall r \in \Gamma\xi.$$

scinde le 2-cocycle κ_τ.

Définition 14. *Le théorème des unités de Dirichlet permet d'affirmer que l'anneau des unités de $\mathcal{O}_K$ est de rang 1 car il y a 2 plongements réels. Ainsi on définit $\gamma_\tau \in \mathcal{O}_\tau$ engendrant les unités de $\mathcal{O}_\tau$. La correspondance entre $M_0(N)[1/p]$ et K_p assure l'existence de γ_τ engendrant le stabilisateur Γ_τ de τ dans Γ et l'unicité au signe près (i.e. de la paire $\{\gamma_\tau, \gamma_\tau^{-1}\}$).*

Ceci permet de définir :

$$u(\delta, \tau) = \rho_\tau(\gamma_\tau) \in K_p^\times.$$

3 Fonctions zeta et Conjecture de Gross-Stark

3.1 Fonctions zeta

Soit $\sigma \in Gal(K/\mathbb{Q})$ non trivial. Soit $Q_\tau(x, y)$ la forme quadratique proportionnelle à $(x + \tau y)(x + \sigma(\tau)y)$ de discriminant D.

On définit γ_Q engendrant le sous-groupe de $SL_2(\mathbb{Z})$ stable sous la forme Q et $\mathcal{W}_Q := (\mathbb{Z}^2 - \{0\})/ < \gamma_Q >$.

Définition 15. *La fonction zeta associée à une forme quadratique Q est :*

$$\zeta_Q(s) := \sum_{(m,n) \in \mathcal{W}_Q} sgnQ(m,n) |Q(m,n)|^{-s}.$$

Et pour $\tau \in \mathcal{H}_p^{\mathcal{O}}$, la fonction zeta associée à l'unité modulaire Δ_δ est :

$$\zeta(\delta, \tau, s) := \sum_{d|N} n_d d^s \zeta_{Q_{d\tau}}(s).$$

Proposition 9. *Pour tout n entier naturel impair,*

$$12\zeta(\delta,\tau,1-n) = \int_{\xi}^{\gamma_\tau \xi} Q_\tau(z,1)^{n-1} F_{2n}(z)dz.$$

On trouve une démonstration simple de cette proposition dans [5].

Définition 16. *Soit l'application* $< . >: \mathbb{Z}_p^\times \to 1+p\mathbb{Z}_p, x \mapsto \varepsilon x$ *où* ε *est l'unique racine* $(p-1)$*-ième de l'unité tel que* $\varepsilon x \in 1+p\mathbb{Z}_p$.

La fonction zeta p-adique est définie pour $\tau \in \mathcal{H}_p^{\mathcal{O}}$ *et* $s \in \mathbb{Z}_p$ *par :*

$$\zeta_p(\delta,\tau,s) = \frac{1}{12}\int_{\mathbb{X}} < Q_\tau(x,y) >^{-s} d\nu\{\xi \to \gamma_\tau \xi\}(x,y).$$

Théorème 5. *Si* $\tau \in \mathcal{H}_p^{\mathcal{O}}$ *alors :*

$$\zeta_p'(\delta,\tau,0) = -\frac{1}{12}\log_p N_{K_p/\mathbb{Q}_p} u(\delta,\tau).$$

Proposition 10. *Pour tout entier n négatif tel que* $n \equiv 0 \mod (p-1)$*, les fonctions zeta sont reliées par :*

$$\zeta_p(\delta,\tau,n) = (1-p^{-2n})\zeta(\delta,\tau,n).$$

De plus ces équations suffisent à définir $\zeta_p(\delta,\tau,s)$ *par interpolation.*

L'étude du cas K quadratique réel à donner lieu à une conjecture de Gross (voir [9]). Il utilise alors des fonctions zeta p-adiques qui s'annulent en $s=0$ par construction, où p est choisi comme précédemment non ramifié dans K et H^+ est le corps de classe de Hilbert de K au sens étroit.

Conjecture 2 (Gross-Stark)**.** *Soit p premier de K tel qu'il se décompose totalement dans H. Ainsi H s'injecte dans K_p.*

Il existe une p-unité $u \in U_{H^+,p} = \{x \in H^+; ||x||_{\mathfrak{q}} = 1$ *pour toute place* $\mathfrak{q}$ *ne divisant pas* $p\}$ *telle que :*

$$\zeta_p'(\delta,\tau,0) = \log_p N_{K_p/\mathbb{Q}_p}(u).$$

La p-unité u est ici appelée unité de Gross-Stark.

3.2 Conjecture de Darmon-Dasgupta

Le théorème 10 donne une formule du type recherché dans la conjecture de Gross-stark pour K quadratique réel. Il manque alors le fait que $u(\delta,\tau)$ soit une p-unité.

Darmon et Dasgupta introduisent dans l'article [5] une nouvelle conjecture impliquant celle de Gross-Stark. L'avantage de leurs méthodes est qu'ils explicitent la p-unité $u(\delta,\tau)$ qui est ainsi calculable par ordinateur.

Comme dans le cas classique, il existe H^+/K une extension abélienne et

$$rec : Pic^+(\mathcal{O}) \to Gal(H^+/K).$$

où $Pic^+(\mathcal{O}) := \{\mathcal{O}$ sous-module projectif $\subset K\}/K_+^\times$. On dit que H^+ est le corps de classe de Hilbert de K au sens étroit.

On dispose d'une action de $Pic^+(\mathcal{O})$ sur $\mathcal{H}_p^{\mathcal{O}}/\Gamma$ notée $\star$.

Conjecture 3 (Darmon-Dasgupta)**.** *Si* $\tau \in \mathcal{H}_p^{\mathcal{O}}/\Gamma$*, alors l'unité* $u(\delta,\tau) \in \mathcal{O}_H[1/p]^\times/U$*, et :*

$$u(\delta,\mathfrak{a}\star\tau) = rec(\mathfrak{a})^{-1}u(\delta,\tau) \ (mod\ U),\ \forall \mathfrak{a} \in Pic^+(\mathcal{O}).$$

Proposition 11. *Soient* $\tau_\infty \in Gal(H^+/K)$ *la conjugaison complexe et* $\tau \in \mathcal{H}_p^{\mathcal{O}}$*. Si la Conjecture 3 est vérifiée alors :*

$$\tau_\infty u(\delta,\tau) = u(\delta,\tau)^{-1}.$$

Le nombre $u(\delta,\tau)$ *construit dans* K_p *est alors une p-unité de* H^+ *le corps de classe de Hilbert au sens étroit de K.*

Ainsi la Conjecture de Darmon-Dasgupta implique celle de Gross-Stark.

Références

[1] Pierre Charollois: *Somme de Dedekind et periodes de formes modulaires de Hilbert.* Thèse de doctorat, Université de Bordeaux 1, 2004.

[2] Pierre Charollois et Henri Darmon: *Arguments des unités de Stark et périodes de séries d'Einsenstein.* Algebra and Number Theory, vol.2, No.6, 2008.

[3] Henri Darmon: *Integration on $H_p \times H$ and arithmetic applications.* Annals of Mathematics 154, page 589 à 639, 2001.

[4] Henri Darmon: *Conference on Modular elliptic curves (2001 ; Orlando).* Dans *Rational points on modular elliptic curves*, numéro 101 dans *CBMS Regional Conference Series in Mathematics.* AMS-NSF, 2004.

[5] Henri Darmon et Samit Dasgupta: *Elliptic units for real quadratic fields.* Annals of Mathematics (2) 163, no 1, page 301 à 346, 2006.

[6] Samit Dasgupta: *Stark-Heegner points on modular jacobians.* Annales scientifiques de l'école normale supérieure, 4ème série, tome 38, page 427 à 469, 2005.

[7] Samit Dasgupta: *Computations of elliptic units for real quadratic fields.* Canadian Journal of Mathematics, 59, 2007.

[8] Ralph Greenberg et Glenn Stevens: *p-adic L-functions and p-adic periods of modular forms.* Inventiones mathematicae 111, page 407 à 447, 1993.

[9] Benedict H. Gross: *p-adic L-series at $s = 0$.* Fac. Sci. Univ. Tokyo Sect. IA Math. 28, 1981.

[10] Carl Ludwig Siegel: *Lectures on advanced analytic number theory.* Bombay : Tata Institute of Fundamental Research, 1961.

[11] Lawrence C. Washington: *Introduction to Cyclotomic Fields.* GTM 83. Springer-Verlag, 1982.