Astérisque

BERNADETTE PERRIN-RIOU

Fonctions Lp-adigues et points de Heegner

Astérisque, tome 147-148 (1987), p. 151-171

<http://www.numdam.org/item?id=AST_1987__147-148__151_0>

Société Mathématique de France
Astérisque 147-148 (1987), p.151-171.

Fonctions L p-adiques et points de Heegner

Bernadette PERRIN-RIOU

Soit E une courbe elliptique modulaire de conducteur N, c'est-à-dire admettant une paramétrisation par la courbe modulaire $X_0(N)$:

$$\pi : X_0(N) \longrightarrow E$$

définie sur $\mathbb{Q}$ et envoyant la pointe $i\infty$ sur l'origine de E. Nous cherchons ici à proposer un analogue p-adique du théorème principal de [4] démontré par Gross et Zagier. Ce théorème relie la dérivée de la fonction L complexe de la courbe E sur un corps quadratique imaginaire k à la hauteur de Néron-Tate de certains points de Heegner sur la courbe. Soit p un nombre premier impair tel que E est ordinaire en p. La fonction L p-adique attachée à E et à k a été construite par Haran [5]. Nous en esquisserons ici une construction différente en utilisant une méthode due à Hida ([7], voir [12] pour les démonstrations complètes). Nous proposerons alors une conjecture reliant la dérivée d'une telle fonction à la hauteur p-adique de ces mêmes points de Heegner. Nous étudierons en même temps le lien avec la conjecture p-adique de Birch et Swinnerton-Dyer. Enfin, nous esquisserons ce qui nous semble être un début de démonstration.

On suppose choisis dans tout le texte un plongement de la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$ et un plongement de $\overline{\mathbb{Q}}$ dans la clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$.

1 - Fonctions L p-adiques.

Soit k un corps quadratique imaginaire de discriminant D. La fonction L complexe de E/k est définie par

$$L(E/k,s) = \prod_{\mathfrak{q}} P_{\mathfrak{q}}(\mathbf{N}\mathfrak{q}^{-s})^{-1};$$

ici, $\mathfrak{q}$ parcourt les idéaux premiers de k et on a posé

$$P_{\mathfrak{q}}(X) = 1 - a_{\mathfrak{q}}X + \psi(\mathfrak{q})\mathbf{N}\mathfrak{q}X^2$$

où $\mathbf{N}\mathfrak{q}$ désigne la norme de l'idéal $\mathfrak{q}$, où $\mathbf{N}\mathfrak{q} + 1 - a_{\mathfrak{q}}$ est le nombre de points de la réduction d'un modèle minimal de Weierstrass de E en $\mathfrak{q}$ sur le corps résiduel de k en $\mathfrak{q}$ et où $\psi(\mathfrak{q})$ vaut 1 si la courbe a bonne réduction et 0 sinon. Soit W un caractère de Hecke d'ordre fini de conducteur $\mathfrak{f}$ c'est-à-dire un caractère sur le groupe $I_{\mathfrak{f}}$ des idéaux de k premiers à $\mathfrak{f}$ à valeurs dans $\bar{\mathbb{Q}}$. La fonction L de E/k tordue par W est alors

$$L(E/k,W,s) = \prod_{\mathfrak{q}} P_{\mathfrak{q}}(W(\mathfrak{q})\mathbf{N}\mathfrak{q}^{-s})^{-1}.$$

Lorsque E est une courbe de Weil associée à une forme modulaire f primitive pour $\Gamma_0(N)$ ($f = \Sigma\, a_n q^n$), ce que nous supposerons désormais, ces fonctions L, définies a priori pour $\mathrm{Re}(s) > 3/2$, admettent un prolongement holomorphe à $\mathbb{C}$ et une équation fonctionnelle([14])

Nous ferons désormais les hypothèses suivantes :

(i) N et D sont premiers entre eux,

(ii) p ne divise pas D,

(iii) E est ordinaire en p c'est-à-dire a_p est une unité en p.

Par contre, nous ne supposerons pas pour l'instant N et p premiers entre eux : on pose $N = N'p^{\gamma}$ avec $(p,N') = 1$. La condition (iii) implique que γ est égal à 0 ou 1. On notera α_p la racine du polynôme

$$X^2 - a_pX + p\psi(p)$$

qui est une unité dans $\mathbb{Z}_p$ (avec

$$\psi(p) = \begin{cases} 1 & \text{si } p \nmid N \\ 0 & \text{si } p \mid N \end{cases}$$

et on pose $\alpha_{p^r} = \alpha_p^r$ pour tout entier r positif.

Soit k_∞ l'unique $\mathbb{Z}_p^2$-extension de k. Pour tout idéal $\mathfrak{q}$ premier à p, notons $\sigma_{\mathfrak{q}}$ l'image de $\mathfrak{q}$ dans $G(k_\infty/k)$ par l'homomorphisme d'Artin. Soient ε le caractère quadratique associé au corps

k et $\mathfrak{D}$ la différente de k. Enfin, si ω est la forme différentielle $2i\pi f dz$ sur la courbe modulaire $X_0(N)$, posons

$$\Omega_f = \int_{X_0(N)} \omega \wedge i\bar{\omega}.$$

Nous aurons finalement besoin d'un entier C auxiliaire premier à NDp.

Théorème 1. Il existe un élément d de $\mathbb{Z}_p$ et une mesure μ_E^C sur $G(k_\infty/k)$ à valeurs dans $d^{-1}\mathbb{Z}_p$ tels que pour tout caractère ψ d'ordre fini de $G(k_\infty/k)$ à valeurs dans $\bar{\mathbb{Q}}$ et dont le composé avec l'homomorphisme d'Artin est de conducteur f, on ait

$$\int_{G(k_\infty/k)} \psi d\mu_E^C = (1-C\,\bar{\psi}(\sigma_C)\varepsilon(C))\psi(N')\bar{\psi}(\mathfrak{D})V_p(\psi)\,\frac{(|D|\mathbf{N}f)^{\frac{1}{2}}}{\alpha_{\mathbf{N}f}}\,W(\psi)\,\frac{L(E/k,\bar{\psi},1)}{\Omega_f}$$

où $W(\psi)$ est l'"Artin root number" associé à ψ et où on a posé

$$V_p(\psi) = \prod_{\mathfrak{p}|p} \left(1 - \frac{\psi(\sigma_\mathfrak{p})}{\alpha_{\mathbf{N}\mathfrak{p}}}\right)\left(1 - \frac{\bar{\psi}(\sigma_\mathfrak{p})\psi(\mathfrak{p})}{\alpha_{\mathbf{N}\mathfrak{p}}}\right).$$

Donnons une autre formulation de ce théorème en termes de fonctions d'Iwasawa. Soit $\mathcal{C}(k_\infty/k)$ le groupe des caractères de $G(k_\infty/k)$ à valeurs dans $\mathbb{Z}_p^\times$ et soit $Iw(k_\infty/k)$ l'algèbre d'Iwasawa de $G(k_\infty/k)$ c'est-à-dire la $\mathbb{Z}_p$-algèbre topologique engendré par les fonctions de $\mathcal{C}(k_\infty/k)$ dans $\mathbb{Z}_p$ du type $\nu \to \nu(\gamma)$ pour $\gamma \in G(k_\infty/k)$. Par extension des scalaires, on pourra prendre la valeur d'un élément de $Iw(k_\infty/k)$ sur n'importe quel caractère de $G(k_\infty/k)$ à valeurs dans $\bar{\mathbb{Q}}_p^\times$. D'autre part, si τ désigne la conjugaison complexe, on désigne par ι l'involution de $Iw(k_\infty/k)$ définie par

$$h^\iota(\lambda) = h(\lambda^{-\tau})$$

pour tout λ appartenant à $\mathcal{C}(k_\infty/k)$.

Corollaire. Il existe un élément de $d^{-1}Iw(k_\infty/k)$ noté $L_p(E/k)$ tel que pour tout caractère ψ d'ordre fini de $G(k_\infty/k)$ à valeurs dans $\bar{\mathbb{Q}}$ (et de conducteur f) on ait

$$L_p(E/k)(\psi) = \bar{\psi}(\mathfrak{D})\,\frac{(|D|\mathbf{N}f)^{\frac{1}{2}}}{\alpha_{\mathbf{N}f}}\,V_p(\psi)\,W(\psi)\,\frac{L(E/k,\bar{\psi},1)}{\Omega_f}$$

De plus la fonction d'Iwasawa $\Lambda_p(E/k)$ définie par

$$\Lambda_p(E/k)(\lambda) = \lambda^{\frac{1}{2}}(N')\lambda(\mathfrak{D})L_p(E/k)(\lambda)$$

vérifie l'équation fonctionnelle

$$\Lambda_p(E/k)^{\iota} = -\varepsilon(N')\Lambda_p(E/k).$$

Remarque. L'image du caractère λ étant contenue dans $1+p\mathbb{Z}_p$, sa racine carrée est bien définie dans $\mathcal{C}(k_\infty/k)$. Quant au lien entre la mesure μ_E^C et la fonction $L_p(E/k)$, il est donné par

$$L_p(E/k)(\lambda) = (1-C\lambda^{-1}(\sigma_C)\varepsilon(C))^{-1}\lambda(\sigma_{N'})^{-1}\int_{G(k_\infty/k)} \lambda\, d\mu_E^C .$$

Nous allons maintenant faire le lien entre cette fonction L et celle introduite par Mazur et Swinnerton-Dyer ([9], cf. aussi [11]).

Soit ω_E une forme différentielle minimale de E et γ_E^+ (resp. γ_E^-) un générateur du sous-espace propre de $H_1(E,\mathbb{Z})$ pour la conjugaison complexe et pour la valeur propre +1 (resp. -1). On le choisit de manière que si

$$\Omega_E^+ = \int_{\gamma_E^+} \omega_E \quad (\text{resp. } \Omega_E^- = \int_{\gamma_E^-} \omega_E),$$

Ω_E^+ (resp. $-i\Omega_E^-$) soit positif. Notons L_E le $\mathbb{Z}_p$-module engendré par Ω_E^+.

On notera $\mathbb{Q}_\infty$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$; soit $\nu_{\mathbb{Q}}$ un caractère de $G(\bar{\mathbb{Q}}/\mathbb{Q})$ se factorisant par $G(\mathbb{Q}_\infty/\mathbb{Q})$ et ν sa restriction à $G(\bar{\mathbb{Q}}/k)$.

Rappel et définition ([9], [11]). Il existe une unique fonction d'Iwasawa $L_p(E/\mathbb{Q})$ dans $Iw(\mathbb{Q}_\infty/\mathbb{Q}) \otimes_{\mathbb{Z}_p} L_E$ vérifiant pour tout caractère de Dirichlet de conducteur p^r et se factorisant par $G(\mathbb{Q}_\infty/\mathbb{Q})$

$$L_p(E/\mathbb{Q})(\chi) = \alpha_p^{-r}p^r\left(1-\frac{\bar{\chi}(p)\psi(p)}{\alpha_p}\right)\left(1-\frac{\chi(p)}{\alpha_p}\right)\frac{L(E/\mathbb{Q},\bar{\chi},1)}{\tau(\bar{\chi})} .$$

Ici $\tau(\bar{\chi})$ est la somme de Gauss (de module $p^{r/2}$)

$$\sum_{m \bmod p^r} \bar{\chi}(m)\, e^{2i\pi m/p^r}$$

et $$L(E/\mathbb{Q},\chi,s) = \sum_{n>0} a_n \chi(n) n^{-s} .$$

La proposition suivante est l'analogue de la formule complexe

$$L(E/k,s) = L(E/\mathbb{Q},s)L(E^{(\varepsilon)}/\mathbb{Q},s)$$

où la courbe $E^{(\varepsilon)}$ est la tordue de E par le caractère ε.

Proposition 2. On a l'égalité de fonctions d'Iwasawa

$$L_p(E/k)(\nu) = L_p(E/\mathbb{Q})(\nu_{\mathbb{Q}})L_p(E^{(\varepsilon)}/\mathbb{Q})(\nu_{\mathbb{Q}}) \frac{|D|^{\frac{1}{2}}}{\Omega_f} .$$

Remarque. Les deux membres sont des fonctions d'Iwasawa à coefficients dans $\mathbb{Q}_p$ avec mêmes dénominateurs. On a en effet

$$\int_{E(\mathbb{C})} \omega_E \wedge i\bar{\omega}_E = [E(\mathbb{R}) : E^o(\mathbb{R})]\, \Omega_E^+ \, (-i\,\Omega_E^-)$$

$$= [E(\mathbb{R}) : E^o(\mathbb{R})]\, \Omega_E^+ \, \Omega^+_{E^{(\varepsilon)}} \sqrt{|D|}$$

si $E^o(\mathbb{R})$ est la composante connexe de $E(\mathbb{R})$. D'autre part, à la paramétrisation π est associé un nombre $c_{E,\pi}$ défini par $\pi^*\omega_E = c_{E,\pi}\omega_f$. On a alors

$$\int_{E(\mathbb{C})} \omega_E \wedge i\bar{\omega}_E = c_{E,\pi}^2 \, \Omega_f/\deg \pi .$$

d'où

$$|D|^{-\frac{1}{2}}\Omega_f = c_{E,\pi}^{-2} \deg \pi \, [E(\mathbb{R}) : E^o(\mathbb{R})]\, \Omega_E^+ \, \Omega^+_{E^{(\varepsilon)}} .$$

Ici, la constante de Manin $c_{E,\pi}$ et le nombre de composantes connexes $[E(\mathbb{R}) : E^o(\mathbb{R})]$ de $E(\mathbb{R})$ sont des unités en p. Quant à la constante d du théorème 1, c'est celle intervenant dans la formule (à un élément de $\mathbb{Z}_p^\times$ près)

$$\Omega_f = d\, c_{A,\pi_A}^{-2} [A(\mathbb{R}) : A^o(\mathbb{R})]\, \Omega_A^+ \, (-i\Omega_A^-)$$

où A est la courbe de Weil forte associée à la forme modulaire f et π_A une paramétrisation minimale (pour la démonstration voir [4] paragraphe 6 et [7] ou [12]). On en déduit que d est égal au degré de π_A. Les propriétés d'intégralité sont donc les mêmes (les fonc-

tions L p-adiques de E ne dépendent que de sa classe d'isogénie).

Démonstration de la proposition. On compare les définitions des différentes fonctions prises en un caractère de Dirichlet χ en remarquant que

$$\alpha_p(E^{(\varepsilon)}) = \varepsilon(p)\alpha_p(E),$$

$$L(E/k,\chi\circ\mathbf{N},1) = L(E/\mathbb{Q},\chi,1)L(E^{(\varepsilon)}/\mathbb{Q},\chi,1) = L(E/\mathbb{Q},\chi,1)L(E/\mathbb{Q},\chi\varepsilon,1),$$

$$W(\chi\circ N) = \chi(D)\varepsilon(p^r)p^{-r}\tau(\chi)^2.$$

2 - Conjectures et points de Heegner.

Nous allons maintenant énoncer une conjecture p-adique de Birch et Swinnerton-Dyer dans le cas particulier qui nous intéresse ([1], [10]). Nous supposerons désormais que p et N sont premiers entre eux. On note $1\!\!1$ le caractère trivial de $G(k_\infty/k)$ et λ un caractère tel que $\lambda^\tau \neq \lambda^{-1}$. Posons

$$D_{p,\lambda}(E/k) = \frac{d}{ds} L_p(E/k)(\lambda^s)\Big|_{s=0}.$$

Soit $<\ ,\ >_\infty$ (resp. $<,>_{\lambda,p}$) la hauteur complexe de Néron-Tate (resp. la hauteur p-adique de Mazur et Tate associée au caractère λ, [10]) sur E(k).

Conjecture A. Supposons que le rang de E(k) est égal à 1 et soit P un point de E(k) qui n'est pas de torsion. Alors,

(i) $L_p(E/k)(1\!\!1) = 0$

(ii) $<P,P>_{\lambda,p} \neq 0$

(iii) on a l'égalité de nombres rationnels

$$\prod_{\mathfrak{p}|p}(1-\frac{1}{\alpha_{\mathbf{N}\mathfrak{p}}})^{-2}\frac{D_{p,\lambda}(E/k)}{<P,P>_{\lambda,p}} = \frac{L'(E/k,1)}{<P,P>_\infty}\frac{\sqrt{|D|}}{\Omega_f}.$$

Comme E est définie sur $\mathbb{Q}$, cette conjecture est un simple corollaire de la conjecture analogue sur $L_p(E/\mathbb{Q})$ (voir [1], [11] : nous préférons la formulation de [1] car elle évite l'introduction du groupe de Shafarevitch-Tate et son calcul si l'on désire la vérifier numériquement; les deux formulations sont équivalentes si l'on admet

la conjecture de Birch et Swinnerton-Dyer). Remarquons d'autre part que si $\varepsilon(N) = 1$, ce que l'on attend dans un cas de rang 1, l'équation fonctionnelle de $L_p(E/k)$ implique la nullité de $L_p(E/k)(\rho)$ pour tout caractère ρ diédral (c'est-à-dire tel que $\rho^\tau = \rho^{-1}$). Il est facile de voir que, pour un tel caractère ρ, $<P,P>_{\rho,p}$ est nul (sous les hypothèses de la conjecture A). Ces deux remarques impliquent qu'il suffit par linéarité de vérifier cette conjecture pour un caractère λ vérifiant $\lambda^\tau \neq \lambda^{-1}$. Enfin, il est montré (ii) dans le cas où E a multiplication complexe ([2]).

Plaçons-nous maintenant dans la situation d'existence de points de Heegner sur k. Nous supposerons donc que tout diviseur premier de N se décompose dans k. Comme nous l'avons déjà remarqué, $L_p(E/k)(1)$ est nul. Soit x un point de Heegner de discriminant D dans $X_0(N)$,[3] il est donc représenté dans $X_0(N)(\mathbb{C})$ par une isogénie cyclique de degré N entre deux courbes elliptiques ayant multiplication complexe par l'anneau des entiers $\mathcal{O}$ de k. Il est en fait défini sur le corps de Hilbert H de k. Grâce à la paramétrisation $\pi : X_0(N) \to E$ définie sur $\mathbb{Q}$ et en prenant la trace $tr_{H/k}$ de H à k, on obtient un point de E(k)

$$Q^{(\pi)} = tr_{H/k}(\pi(x)).$$

L'utilisation du théorème de Gross et Zagier montre que dans cette situation la conjecture A est (presque) impliquée par la conjecture suivante (u est égal au cardinal de $\mathcal{O}^\times/\{\pm 1\}$).

Conjecture B. Si tout diviseur premier de N se décompose dans k, on a

$$D_{p,\lambda}(E/k) = \prod_{\mathfrak{p}|p} (1 - \frac{1}{\alpha_{\mathbf{N}\mathfrak{p}}})^2 \frac{<Q^{(\pi)},Q^{(\pi)}>_{\lambda,p}}{u^2 \deg \pi} .$$

Rappelons que la formule démontrée par Gross et Zagier est

$$L'(E/k,1) = \frac{\Omega_f}{\sqrt{|D|}} \cdot \frac{<Q^{(\pi)},Q^{(\pi)}>_\infty}{u^2 \deg \pi}$$

Remarque 1. La conjecture B implique en particulier que

(1) $\prod_{\mathfrak{p}|p} (1 - \frac{1}{\alpha_{\mathbf{N}\mathfrak{p}}})^2 <Q^{(\pi)},Q^{(\pi)}>_{\lambda,p}$ appartient à $p\mathbb{Z}_p$

puisqu'il en est de même de $\deg \pi\, D_{p,\lambda}(E/k)$. Cet énoncé est vrai et

nous indiquerons un peu plus loin comment le montrer.

Remarque 2. Nous n'avons considéré ici que le cas des courbes elliptiques modulaires auxquelles on associe donc une forme modulaire pour $\Gamma_0(N)$ définie sur $\mathbb{Q}$ ($a_n \in \mathbb{Q}$). Comme dans le cas complexe, cela se généralise à n'importe quelle forme modulaire parabolique primitive pour $\Gamma_0(N)$ ordinaire pour tout plongement de $\bar{\mathbb{Q}}$ dans $\bar{\mathbb{Q}}_p$.

Remarque 3. Donnons une autre conséquence de la conjecture B.

Si $D_{p,\lambda}(E/k)$ est non nul, alors $E(k)$ contient un point d'ordre infini.

Comme dans le cas complexe, on peut traduire cette conséquence sur $\mathbb{Q}$:

Supposons $L(E/\mathbb{Q},1) = 0$. Alors, si $\frac{d}{ds} L_p(E/\mathbb{Q})(\nu_{\mathbb{Q}}^s)\big|_{s=0}$ est non nul, $E(\mathbb{Q})$ contient un point d'ordre infini et $L'(E/\mathbb{Q},1)$ est non nul.

La fonction L p-adique $L_p(E/k)$ est une fonction sur $\mathcal{C}(k_\infty/k)$. Dans la conjecture B, nous avons donné une formule pour sa dérivée dans une direction donnée en $\mathbb{I}$. Comme nous l'avons déjà remarqué, la valeur de $L_p(E/k)$ sur un caractère diédral ρ est nulle. Il est donc naturel de la généraliser en exprimant sa dérivée dans une direction en un tel caractère. Cela nous amène à introduire un module de points de Heegner de niveau une puissance de p. Soit x_n un point de Heegner de niveau p^n (de discriminant Dp^{2n}) c'est-à-dire un point de $X_0(N)$ représenté par une isogénie cyclique de degré N entre deux courbes elliptiques ayant multiplication complexe par l'ordre $\mathcal{O}_{p^n}$ de k de conducteur p^n. C'est un point défini sur le Ringklassenkörper H_{p^n} de k de conducteur p^n. Notons d'autre part D_∞ la $\mathbb{Z}_p$-extension diédrale de k (c'est aussi l'unique $\mathbb{Z}_p$-extension de k contenue dans la réunion des H_{p^n}). Posons

$$D_\infty \cap H_{p^n} = D_n.$$

A l'aide des points x_n, on construit des points $Q_n^{(\pi)}$ de $E(D_n)$ par la formule

$$Q_n^{(\pi)} = tr_{H_{p^n}/D_n}(\pi(x_n)).$$

Soient $H_n^{(\pi)}$ le $\mathbb{Z}_p[G(D_n/k)]$-module engendré par les points $Q_m^{(\pi)}$ pour $m \leq n$ et $H_\infty^{(\pi)}$ la limite projective des $H_n^{(\pi)}$ relativement aux homomorphismes naturels de norme. La proposition suivante est montrée dans [13].

Proposition 3. Le $\mathbb{Z}_p[[G(D_\infty/k)]]$-module $H_\infty^{(\pi)}$ est libre de rang 0 ou 1. En particulier si $Q^{(\pi)}$ (ou l'un quelconque des $Q_n^{(\pi)}$) est d'ordre infini, il est de rang 1.

A l'aide des hauteurs p-adiques usuelles, construisons une forme bilinéaire $\langle\langle , \rangle\rangle_{\lambda_\infty, p}$ sur $H_\infty^{(\pi)}$ attachée à un caractère λ_∞ de $G(k_\infty/D_\infty)$ et à valeurs dans $Iw(D_\infty/k)$. Soit λ un prolongement de λ_∞ à $G(k_\infty/k)$ et λ_n sa restriction à $G(k_\infty/D_n)$. Si $P_\infty = (P_n)$ et $Q_\infty = (Q_n)$ sont deux points de $H_\infty^{(\pi)}$, on peut montrer que

$$\frac{1}{[D_n:k]} \sum_{s,t \in G(D_n/k)} \langle s(P_n), t(Q_n) \rangle_{\lambda_n, p} \, s^{-1}t$$

définit un élément de $\mathbb{Z}_p[[G(D_\infty/k)]]$ (indépendant du choix de λ) et donc de $Iw(D_\infty/k)$ que l'on notera $\langle\langle P_\infty, Q_\infty \rangle\rangle_{\lambda_\infty, p}$.

Conjecture C. Il existe un générateur $R_\infty^{(\pi)}$ de $H_\infty^{(\pi)}$ tel que

$$\frac{d}{ds} L_p(E/k)(\rho\lambda^s)\Big|_{s=0} = \frac{\langle\langle R_\infty^{(\pi)}, R_\infty^{(\pi)} \rangle\rangle_{\lambda_\infty, p}(\rho)}{u^2 \deg \pi}$$

Nous allons maintenant à la fois répondre à la remarque 1 et vérifier une compatibilité entre les conjectures B et C. En étudiant les liens existants entre les points $Q_n^{(\pi)}$, on peut vérifier que le point de $E(k) \otimes_{\mathbb{Z}} \mathbb{Z}_p$

$$\prod_{\mathfrak{p}|p} (1 - \frac{1}{\alpha_{\mathbf{N}\mathfrak{p}}}) Q^{(\pi)}$$

est une norme universelle dans $E(D_\infty) \otimes_{\mathbb{Z}} \mathbb{Z}_p$; cela implique que sa réduction modulo toute place divisant p est nulle et que sa hauteur p-adique appartient à $p\mathbb{Z}_p$. Plus précisément, on peut compléter la proposition 3.

Proposition 3'. Si $Q^{(\pi)}$ est d'ordre infini, le $\mathbb{Z}_p$-module des co-invariants de $H_\infty^{(\pi)}$ pour $G(D_\infty/k)$ est isomorphe à

$$\prod_{\mathfrak{p}|p} (1 - \frac{1}{\alpha_{\mathbf{N}\mathfrak{p}}}) \, \mathbb{Z}_p \, Q^{(\pi)} .$$

Pour une interprétation de la conjecture C en termes de modules d'Iwasawa, nous renvoyons à [13].

3 - Construction dela fonction L p-adique.

3.1. Définition de la mesure μ_E^C.

La définition de la mesure μ_E^C est inspirée de la notion de produit de Rankin. Le principe est dû à Hida ([7]).

Fixons d'abord quelques notations. Soient A un sous-anneau de $\bar{\mathbb{Q}}$ et $\bar{A}$ sa complétion pour la topologie p-adique induite par l'inclusion choisie de $\bar{\mathbb{Q}}$ dans $\bar{\mathbb{Q}}_p$. On définit $M_k(\Gamma,A)$ comme le A-module des formes modulaires de poids k pour un sous-groupe de congruence Γ (par exemple $\Gamma_0(M)$ ou $\Gamma_1(M)$) dont les coefficients de Fourier appartiennent à A. Cet espace est muni d'une norme p-adique $||_p$:

$$|h|_p = \sup_n |a_n(h)|_p \quad \text{si} \quad h = \Sigma\, a_n(h) q^n.$$

On définit alors $M_k(\Gamma,\bar{A})$ comme la complétion de $M_k(\Gamma,A)$ pour cette norme, $M_k(\Gamma_i(Mp^\infty),\bar{A})$ comme la réunion des $M_k(\Gamma_i(Mp^n),\bar{A})$ et $\bar{M}_k(\Gamma_i(Mp^\infty),\bar{A})$ comme la complétion de ce dernier espace pour la norme $||_p$ dans $\bar{A}[[q]]$ (pour $i = 0$ ou 1).

A l'opérateur de Hecke $T(p)$ défini sur les éléments de $\bar{A}[[q]]$ par

$$\Sigma\, a_n q^n | T(p) = \Sigma\, a_{np} q^n,$$

est associé un idempotent e sur $\bar{M}_k(\Gamma_0(Mp^\infty),\bar{A})$. On peut montrer que

$$e = \lim_{n\,\infty} T(p)^{tp^n}$$

où t est un entier suffisamment grand. De plus l'image de $\bar{M}_k(\Gamma_0(Mp^\infty);\bar{A})$ par e est contenue dans $M_k(\Gamma_0(Mp),\bar{A})$ (pour M premier à p).

Considérons maintenant la forme modulaire f associée à la courbe elliptique E. C'est une forme primitive pour $\Gamma_0(N)$ dans $M_2(\Gamma_0(N),\mathbb{Q})$ et ordinaire en p. L'interprétation p-adique du produit de Petterson de f avec un élément de $M_2(\Gamma_0(N'p),\bar{A})$ est alors donnée par la proposition suivante ([7]) (on rappelle que sous les hypothèses

faites, $N'p$ est égal à Np si p ne divise pas N et à N sinon).

Proposition 4. Il existe une forme linéaire continue de $M_2(\Gamma_0(N'p),\bar{A})$ dans $\bar{A}$ tel que si g est défini sur $\bar{\mathbb{Q}}$, on a

$$L_f(g) = \frac{\langle f_0^{\tau} | \begin{pmatrix} 0 & -1 \\ N'p & 0 \end{pmatrix}, g\rangle_{N'p}}{\alpha_p^{1-\gamma} H_p(f) \langle f,f\rangle_N}$$

avec

$$H_p(f) = (1 - \frac{\psi(p)}{\alpha_p^2})(1 - \frac{p\psi(p)}{\alpha_p^2}),$$

$$\langle f,f\rangle_N = \Omega_f/8\pi^2$$

et

$$f_0(z) = f(z) - \frac{p\psi(p)}{\alpha_p} f(pz).$$

On posera $L'_f = H_p(f)L_f$.

Nous allons maintenant définir successivement plusieurs mesures sur $\mathbb{Z}_p$ à valeurs dans les formes modulaires p-adiques. La première est la mesure d'Eisenstein ([7], [8]). Soit λ un entier positif impair. Notons $s(d)$ le signe de l'entier d. On note $\zeta_{Mp^r}(1-\lambda,a)$ la valeur en $s = 1-\lambda$ du prolongement analytique de la série de Hurwitz

$$\sum_{n\equiv a \bmod Mp^r} s(n)\,|n|^{-s}.$$

Posons

$$E_\lambda(a,Mp^r) = \frac{1}{2}\zeta_{Mp^r}(1-\lambda,a) + \sum_{n=1}^{\infty} \sum_{\substack{d|n \\ d\equiv a \bmod Mp^r}} s(d)\,d^{\lambda-1}\,q^n$$

et

$$E_\lambda^C(a,Mp^r) = E_\lambda(a,Mp^r) - C^\lambda E_\lambda(C^{-1}a,Mp^r)$$

où C^{-1} désigne l'inverse de C modulo Mp^r. Alors les $E_\lambda^C(a,Mp^r)$ définissent une mesure sur $\mathbb{Z}_{p,M}^{\times} = \mathbb{Z}_p^{\times} \times (\mathbb{Z}/M\mathbb{Z})^{\times}$ à valeurs dans $\bar{M}_\lambda(\Gamma_1(Mp^\infty),\mathbb{Z}_p)$.

La seconde mesure est attachée à un $\mathcal{O}_{p^n}$-idéal propre $\mathfrak{a}$ de k. Soit $Q_{\mathfrak{a}}$ la forme quadratique associée à $\mathfrak{a}$:

$$Q_{\mathfrak{a}}(x) = N_{k/\mathbb{Q}}(x)/\mathbf{N}\mathfrak{a} \quad \text{pour} \quad x \in k.$$

On pose

$$\theta_{\mathfrak{a}}(a,p^r) = \sum_{\substack{x \in \mathfrak{a} \\ Q_{\mathfrak{a}}(x) \equiv a \bmod p^r}} q^{Q_{\mathfrak{a}}(x)}$$

Les $\theta_{\mathfrak{a}}(a,p^r)$ définissent une mesure p-adique sur $\mathbb{Z}_p$ à valeurs dans $M_1(\Gamma_1(|D|p^\infty),\mathbb{Z}_p)$.

On pose maintenant

$$\psi^C_{\mathfrak{a}}(a,p^r)(z) = \sum_{\alpha \in (\mathbb{Z}/Dp^r\mathbb{Z})^\times} \theta_{\mathfrak{a}}(\alpha^2 a,p^r)(z)\tilde{E}_1(\alpha,Dp^r)(N'z).$$

On a alors la proposition.

Proposition 5. Les fonctions $\psi^C_{\mathfrak{a}}(a,p^r)$ appartiennent à $\bar{M}_2(\Gamma_0(N|D|p^\infty),\mathbb{Z}_p)$ et définissent une mesure sur $\mathbb{Z}_p^\times$.

La trace de $\bar{M}_2(\Gamma_0(N|D|p^\infty),\mathbb{Z}_p)$ à $\bar{M}_2(\Gamma_0(Np^\infty),\mathbb{Z}_p)$ est alors bien définie; on la note $tr_{ND/N}$. On pose

$$\Phi^C_{\mathfrak{a}}(a,p^r) = \frac{\varepsilon(-N)}{4u}\, tr_{ND/N}\, \psi^C_{\mathfrak{a}}(a,p^r).$$

Cela définit une mesure à valeurs dans $\bar{M}_2(\Gamma_0(Np^\infty),\mathbb{Z}_p)$. Il est facile d'en déduire une mesure sur $G(k_\infty/k)$ à l'aide de l'homomorphisme d'Artin. Si θ est un caractère diédral d'ordre fini de $G(k_\infty/k)$ (se factorisant par $G(D_n/k)$) et χ un caractère de Dirichlet, on pose

$$\int_{G(k_\infty/k)} \theta \cdot \chi \circ \mathbf{N}\, d\Phi^C = \sum_{\mathfrak{a}} \theta(\sigma_{\mathfrak{a}}) \int_{\mathbb{Z}_p^\times} \chi\, d\Phi^C_{\mathfrak{a}}$$

où $\mathfrak{a}$ parcourt un ensemble de $\mathcal{O}_{p^n}$-idéaux tel que les $\sigma_{\mathfrak{a}}$ décrivent $G(D_n/k)$. La mesure μ^C_E est alors donnée par

$$d\mu^C_E = L'_f \circ e(d\Phi^C).$$

3.2. Calcul du q-développement de la mesure $d\Phi^C_{\mathfrak{a}}$.

Nous allons maintenant donner le calcul du q-développement de la mesure $d\Phi^C_{\mathfrak{a}}$ afin d'obtenir une formule pour $D_{p,\lambda}(E/k)$. Nous ne supposerons pour l'instant aucune condition sur $\varepsilon(N)$, mais nous supposerons pour simplifier D impair.

Commençons par quelques notations. Si $\mathfrak{a}$ est un idéal de k, soit $r_{\mathfrak{a}}(n)$ le cardinal de l'ensemble des idéaux entiers de k équivalents à $\mathfrak{a}$ et de norme n. On a alors

$$\Theta_{\mathfrak{a}}(z) = \sum_{x \in \mathfrak{a}} q^{Q_{\mathfrak{a}}(x)} = 2u \sum_{n} r_{\mathfrak{a}}(n)\, q^{n}.$$

Si D_1 et D_2 dont deux discriminants de corps quadratiques de caractères associés ε_{D_1} et ε_{D_2} tels que $D_1 D_2 = D$, soit $\chi_{D_1 \cdot D_2}$ le caractère de genre associé défini par

$$\chi_{D_1 \cdot D_2}(\mathfrak{a}) = \varepsilon_{D_1}(\mathbf{N}\mathfrak{a}) = \varepsilon_{D_2}(\mathbf{N}\mathfrak{a})$$

si $\mathfrak{a}$ est un idéal de k. Finalement, on pose comme dans [4]

$$\varepsilon_{\mathfrak{a}}(n,d) = \begin{cases} 0 & \text{si} \quad (d, \frac{n}{d}, D) \neq 1 \\ \varepsilon_{D_1}(d)\varepsilon_{D_2}(-N'\frac{n}{d})\chi_{D_1 \cdot D_2}(\mathfrak{a}) & \text{si} \quad (d, \frac{n}{d}, D) = 1 \\ & \qquad (d, D) = D_2,\ D_1 D_2 = D. \end{cases}$$

Si $\nu_{\mathbb{Q}}$ est un caractère de $G(\overline{\mathbb{Q}}/\mathbb{Q})$ à valeurs dans $\mathbb{Z}_p^{\times}$, on note ν sa restriction à $G(k_\infty/k)$ et ℓ_ν le composé de l'homomorphisme qu'il induit sur $\mathbb{Q}_p^{\times}$ avec le logarithme.

Proposition 6. *Posons pour* m *divisible par* p

$$A_m^{\mathfrak{a}} = \sum_{\substack{n=1 \\ p \nmid n}}^{m|D|/N'} r_{\mathfrak{a}}(m|D| - nN') \sum_{\substack{d|n \\ d>0}} \varepsilon_{\mathfrak{a}}(n,d)$$

et

$$B_m^{\mathfrak{a}} = -\sum_{\substack{n=1 \\ p \nmid n}}^{m|D|/N'} r_{\mathfrak{a}}(m|D| - nN') \sum_{\substack{d|n \\ d>0}} \varepsilon_{\mathfrak{a}}(n,d)\, \ell_\nu(n/d^2).$$

Alors, on a les formules

$$L_p(E/k)(\Pi) = \alpha_p^{-1} \sum_{\mathfrak{a}} L_f' \circ e\Big(\sum_m A_{mp}^{\mathfrak{a}} q^m\Big)$$

$$D_{p,\nu}(E/k) = \alpha_p^{-1} \sum_{\mathfrak{a}} L_f' \circ e\Big(\sum_m B_{mp}^{\mathfrak{a}} q^m\Big) \qquad \text{si} \quad \varepsilon(N') = 1$$

où $\mathfrak{a}$ *parcourt un système de représentants des classes d'idéaux de* k.

Donnons une esquisse de la démonstration de cette proposition. Si φ est une fonction continue sur $\mathbb{Z}_p^\times$, posons

$$\int_{\mathbb{Z}_p^\times} \varphi \, d\Phi_{\mathfrak{a}}^C = \sum_m A_m^{\mathfrak{a},C}(\varphi) q^m$$

et

$$\int_{\mathbb{Z}_p^\times} \varphi \, d\Phi_{\mathfrak{a}} = \sum_m A_m^{\mathfrak{a}}(\varphi) q^m$$

(lorsque cela est défini) où $d\Phi_{\mathfrak{a}}$ est la distribution construite en remplaçant $E_1^C(\alpha, Dp^r)$ par $E_1(\alpha, Dp^r)$ dans la définition de $d\Phi_{\mathfrak{a}}^C$. On a alors le lemme suivant.

Lemme 7. On a

$$L_p(E/k)(1\!\!1) = \sum_{\mathfrak{a}} L'_f \circ e\Big(\sum_m A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times}) q^m\Big)$$

et

$$D_{p,\nu}(E/k) = \sum_{\mathfrak{a}} L'_f \circ e\Big(\sum_m (A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times} \cdot \ell_\nu) - 2\ell_\nu(N) A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times})) q^m\Big)$$

où $1_{\mathbb{Z}_p^\times}$ est la fonction caractéristique de $\mathbb{Z}_p^\times$.

Démonstration. Posons

$$F_{\mathfrak{a}}(s) = \nu_{\mathbb{Q}}(N')^{-2s}(1 - C\varepsilon(C)\nu_{\mathbb{Q}}(C)^{-2s})^{-1} \int_{\mathbb{Z}_p^\times} \nu_{\mathbb{Q}}^s \, d\Phi_{\mathfrak{a}}^C$$

On a alors

$$L_p(E/k)(\nu^s) = \sum_{\mathfrak{a}} L'_f \circ e(F_{\mathfrak{a}}(s)).$$

D'où

$$D_{p,\nu}(E/k) = \sum_{\mathfrak{a}} L'_f \circ e(F'_{\mathfrak{a}}(0)).$$

En remarquant que

$$A_m^{\mathfrak{a},C}(\varphi) = A_m^{\mathfrak{a}}(\varphi) - C\varepsilon(C) A_m^{\mathfrak{a}}(\varphi_C)$$

avec $\varphi_C(x) = \varphi(C^{-2}x)$, on vérifie facilement que le développement de Fourier de $F'_{\mathfrak{a}}(0)$ est

$$\sum_m A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times} \cdot \ell_\nu) q^m - 2\ell_\nu(N') \sum_m A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times}) q^m.$$

Donnons maintenant le lemme essentiel suivant.

Lemme 8. On a

$$A_m^{\mathfrak{a}}(\varphi) = \sum_{\substack{n>0 \\ p\nmid m|D|-nN'}} r_{\mathfrak{a}}(m|D|-nN') \sum_{\substack{0<d|n \\ p\nmid \frac{n}{d}}} \varepsilon_{\mathfrak{a}}(n,d)\, \varphi\left(\frac{m|D|-nN'}{|D|} \cdot \frac{d^2}{n^2}\right)$$

$$+ \frac{1}{4} r_{\mathfrak{a}}(m) \int_{\mathbb{Z}_{p,D}^\times} \varepsilon(x) \varphi\left(\frac{m}{x^2}\right) d\zeta_{D,1}(x)$$

où $d\zeta_{D,\lambda}$ est la distribution associée à

$$(\zeta_{Dp^r}(1-\lambda,a))$$

Remarquons que si χ est un caractère de conducteur p^r, on a

$$\frac{1}{2} \int_{\mathbb{Z}_{p,D}^\times} \varepsilon(x)\chi(x)\, d\zeta_{D,\lambda}(x) = \left(1 - \frac{\varepsilon(p)\chi(p)}{p^{\lambda-1}}\right) L(\varepsilon\chi, 1-\lambda).$$

Soit $d\zeta_{D,\lambda}^C$ la mesure associée à la distribution $d\zeta_{D,\lambda}$ par

$$\zeta_{D,\lambda}^C(a,Dp^r) = \zeta_{Dp^r}(1-\lambda,a) - C^\lambda\, \zeta_{Dp^r}(1-\lambda,C^{-1}a)$$

La fonction de Kubota-Leopoldt est alors définie à l'aide de la mesure $d\zeta_{D,\lambda}^C$ par

$$L_p(s,\varepsilon) = \frac{1}{2} \int_{\mathbb{Z}_p^\times} \omega^{-1}(x)\varepsilon(x) \langle x \rangle^{-s} d\zeta_{D,1}^C / (1 - \langle C \rangle \varepsilon(C))$$

où ω est le caractère de Teichmüller sur $\mathbb{Z}_p^\times$ et où

$$\langle x \rangle = x\,\omega(x)^{-1} \quad \text{pour} \quad x \in \mathbb{Z}_p^\times.$$

D'autre part, remarquons que le coefficient de $r_{\mathfrak{a}}(m)$ est nul dans la formule du lemme 8 dès que p divise m puisque φ est à support dans $\mathbb{Z}_p^\times$.

Montrons comment l'on déduit la proposition 6 du lemme 8. Supposons donc que p divise m. Alors la condition $p\nmid m|D|-nN'$ devient $p\nmid n$ et celle sur d disparaît. On obtient donc

$$A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times}) = A_m^{\mathfrak{a}}.$$

Si maintenant φ est la fonction $\ell_\nu \cdot 1_{\mathbb{Z}_p^\times}$, on voit que

$$A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times}\cdot\ell_\nu) = B_m^{\mathfrak{a}} + \sum_{p\nmid n} r_{\mathfrak{a}}(m|D|-nN') \sum_{d|n} \varepsilon_{\mathfrak{a}}(n,d)\ell_\nu\left(\frac{m|D|-nN'}{n|D|}\right).$$

Supposons que n est tel que $r_{\mathfrak{a}}(m|D|-nN')$ est non nul; il existe alors un idéal $\mathfrak{h}$ équivalent à $\mathfrak{a}$ tel que

$$-nN' \equiv \mathbf{N}\mathfrak{h} \bmod D.$$

On a dans ce cas l'équation fonctionnelle ([3], IV (4.2))

$$\varepsilon_{\mathfrak{a}}(n,d) = -\varepsilon(N')\varepsilon_{\mathfrak{a}}(n,n/d).$$

Lorsque $\varepsilon(N) = 1$, on en déduit que $\sum_{d|n} \varepsilon_{\mathfrak{a}}(n,d)$ est nul. D'où

$$A_m^{\mathfrak{a}}(1_{\mathbb{Z}_p^\times}\cdot\ell_\nu) = B_m^{\mathfrak{a}}.$$

Le même calcul montre que $A_m^{\mathfrak{a}}$ est nul lorsque p divise m et que $\varepsilon(N') = 1$. Pour obtenir la proposition 6, il suffit de remarquer encore que

$$L'_f \circ e \circ T(p)(h) = \alpha_p L'_f \circ e(h).$$

Le lemme 8 se montre à partir de trois lemmes que nous allons énoncer maintenant. Le premier concerne le calcul de la trace de $N|D|$ à N d'une forme modulaire. Les deux suivants donnent les formules de transformation de séries d'Eisenstein et de fonctions Θ sous certaines matrices. Nous n'en donnerons pas ici la démonstration. On choisit pour tout discriminant D_1 une matrice $W_{D_1}^{(\mu)}$ de déterminant δ_1 de la forme

$$W_{D_1}^{(\mu)} = \begin{pmatrix} \delta_1 x & y \\ N\delta p^\mu t & \delta_1 w \end{pmatrix}$$

avec $\delta = |D|$, $\delta_1 = |D_1|$. Si h est une forme modulaire, on note $\sum_n a_n(h)q^n$ son développement de Fourier.

Lemme 9. Si h appartient à $M_k(\Gamma_0(N|D|p^\mu)$, on a

$$a_m(tr_{N|D|/N}(h)) = \sum_{D_1D_2=D} \delta_1^{1-k/2}\, a_{m\delta_1}(h|W_{D_1}^{(\mu)})$$

où D_1 parcourt les discriminants divisant D.

Posons $$K(D_1) = \begin{cases} 1 & \text{si } D_1 > 0 \\ i & \text{si } D_1 < 0. \end{cases}$$

Lemme 10. On a pour $\mu \geq 2r$

$$\Theta_{\mathfrak{a}}(a,p^r)|W_{D_1}^{(\mu)} = \varepsilon_{D_1}(Ntp^\mu)\varepsilon_{D_2}(\delta_1 w)\chi_{D_1\cdot D_2}(\mathfrak{a})K(D_1)^{-1}\Theta_{\mathfrak{D}_1^{-1}\mathfrak{a}}(\delta_1 x^2 a, p^r)$$

où $\mathfrak{D}_1$ est un idéal de k de carré (D_1).

Lemme 11. On a pour $D_1 \neq 1$ et $\mu \geq r$

$$\sum_{\alpha \bmod \delta_1} \varepsilon_{D_1}(\alpha)\, \tilde{E}_\lambda((\alpha,\beta),\delta p^r)\Big|\begin{pmatrix} \delta_1 x & yN' \\ \delta p^{\mu+\gamma} t & \delta_1 w \end{pmatrix}$$

$$= \delta_1^{(\lambda-1)/2}\varepsilon_{D_1}(yN')K(D_1) \sum_{m>0} \sum_{\substack{d|m \\ d\equiv x\beta \bmod \delta_2 p^r}} s(d)\varepsilon_{D_1}(\tfrac{m}{d})d^{\lambda-1}q^m .$$

Ici, le couple (α,β) représente un entier modulo δp^r congru à α modulo δ_1 et à β modulo $\delta_2 p^r$.

Soit φ une fonction sur $\mathbb{Z}_p^\times$ localement constante modulo p^r. Montrons d'abord pour $\delta_1 \neq 1$ la formule suivante

$$(2) \qquad a_{m\delta_1}\Big(\int_{\mathbb{Z}_p^\times} \varphi\, d\Phi_{\mathfrak{a}}|W_{D_1}^{(\mu)}\Big) =$$

$$\chi_{D_1\cdot D_2}(\mathfrak{a})\varepsilon_{D_1}(\delta_2) \sum_{\substack{nN'+t=m\delta_1 \\ p\nmid t}} \mathfrak{D}_1^{-1}\mathfrak{a}(t) \sum_{\substack{d|n \\ p\nmid d \\ d>0}} \varepsilon_{D_2}(-N'd)\varepsilon_{D_1}(\tfrac{n}{d})\varphi\Big(\frac{t}{\delta_1 d^2}\Big).$$

En effet en utilisant les lemmes 10 et 11 et en effectuant la sommation modulo δ, on a

$$\Phi_{\mathfrak{a}}^{C}(a,p^r)\,|\,W_{D_1} = \frac{1}{2}\,\chi_{D_1\cdot D_2}(\mathfrak{a})\,\varepsilon(-N')\,\varepsilon_{D_1}(-N'\delta_2)\,\varepsilon_{D_2}(\delta_1 w)\,\varepsilon_{D_2}(x)$$

$$\times \sum_{\beta\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \sum_{\substack{u\in\mathfrak{D}_1^{-1}\mathfrak{a} \\ Q_{\mathfrak{D}_1^{-1}\mathfrak{a}}(u)\equiv\delta_1\beta^2x^2a \bmod p^r}} q^{Q_{\mathfrak{D}_1^{-1}\mathfrak{a}}(u)} \sum_{n>0} q^{nN'} \sum_{\substack{d\mid n \\ d\equiv x\beta \bmod p^r}} \varepsilon_{D_1}\left(\frac{n}{d}\right) s(d)\,\varepsilon_{D_2}(d)$$

La première ligne vaut :

$$\frac{1}{2}\,\chi_{D_1\cdot D_2}(\mathfrak{a})\,\varepsilon_{D_2}(-N')\,\varepsilon_{D_1}(\delta_2).$$

D'autre part, le membre de gauche de (2) vaut

$$\sum_{a\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \varphi(a)\; a_{m\delta_1}(\Phi_{\mathfrak{a}}^{C}(a,p^r)\,|\,W_{D_1}^{(\mu)})$$

On en déduit (2) en invertissant les signes Σ et en remarquant que lorsque $t = Q_{\mathfrak{D}_1^{-1}\mathfrak{a}}(u)$ et d sont donnés, β et a sont déterminés par

$$\begin{aligned}\beta &\equiv x^{-1}d \bmod p^r\\ a &\equiv \delta_1^{-1}x^{-2}\beta^{-2}t \bmod p^r\\ &\equiv \delta_1^{-1}d^{-2}t \bmod p^r\end{aligned}$$

à condition que d et t soient premiers à p (on rappelle aussi que $\varepsilon(d)s(d) = \varepsilon(-d)s(-d)$ ce qui permet de remplacer la sommation sur d par une sommation sur $d>0$).

En remplaçant n par $\delta_2 n$ et en faisant le changement de variables $d \to n/d$, on obtient

$$a_{m\delta_1}\left(\int_{\mathbb{Z}_p^\times} \varphi\, d\Phi_{\mathfrak{a}}\,|\,W_{D_1}^{(\mu)}\right) =$$

$$\chi_{D_1\cdot D_2}(\mathfrak{a}) \sum_{\substack{\delta_2\mid n \\ p\nmid m\delta-nN'}} r_{\mathfrak{D}_1^{-1}\mathfrak{a}}(m\delta-nN') \sum_{\substack{d\mid n \\ p\nmid \frac{n}{d} \\ \delta_2\mid d}} \varepsilon_{D_1}(d)\,\varepsilon_{D_2}(-N'\tfrac{n}{d})\,\varphi\left(\frac{m\delta-nN'}{\delta}\cdot\frac{d^2}{n^2}\right)$$

Si $D_1 = 1$, il faut rajouter un terme correspondant au terme constant de la série d'Eisenstein, c'est-à-dire

$$\frac{1}{4}\, r_{\mathfrak{a}}(m) \sum_{\alpha \in (\mathbb{Z}/p^r\delta\mathbb{Z})^\times} \varepsilon(\alpha)\varphi(m/\alpha^2)\zeta_{\delta p^r}(0,\alpha) = \frac{1}{4}\, r_{\mathfrak{a}}(m) \int_{\mathbb{Z}_{p,\delta}^\times} \varepsilon(\alpha)\varphi\left(\frac{m}{\alpha^2}\right) d\zeta_{D,1}(\alpha).$$

On remarque alors que

$$\varepsilon_{D_1}(d)\varepsilon_{D_2}\left(\frac{n}{d}\right)$$

est nul si D_2 n'est pas le p.g.c.d. de d et de D (sous la condition que δ_2 divise n). Dans le cas contraire, on a

$$\chi_{D_1 \cdot D_2}(\mathfrak{a})\varepsilon_{D_1}(d)\varepsilon_{D_2}\left(-N'\frac{n}{d}\right) = \varepsilon_{\mathfrak{a}}(n,d).$$

De plus, $\mathfrak{D}$ étant principal, les fonctions $r_{\mathfrak{a}}$ et $r_{\mathfrak{D}^{-1}\mathfrak{a}}$, sont égales. En utilisant alors le lemme 9, on en déduit le lemme 8.

Pour conclure cette partie encore inachevée, nous allons voir comment le calcul précédent permet de donner une autre formulation de la conjecture B lorsque p ne divise pas N.

Notons $F_m^{\mathfrak{a}}$ la "partie finie" de la hauteur p-adique sur $J_0(N)$ des diviseurs de Heegner $(x)-(i\infty)$ et $T_N(m)((x)-(0))^{\sigma_{\mathfrak{a}}}$ où $T_N(m)$ est l'opérateur de Hecke de niveau N. Les calculs de symboles locaux faits dans [4] (formule finale dans V.1) impliquent que pour $(m,N) = 1$

$$F_m^{\mathfrak{a}} = -u^2 \sum_{n=1}^{m|D|/N} r_{\mathfrak{a}}(m|D|-nN) \sum_{d|n} \varepsilon_{\mathfrak{a}}(n,d)\ell_v(n/d^2) + h\, u\, r_{\mathfrak{a}}(m)\ell_v(N/m).$$

Si χ est un caractère de $G(H/k)$, posons

$$F_\chi = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \sum_m F_m^{\mathfrak{a}} q^m$$

et

$$B_\chi = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \sum_m B_m^{\mathfrak{a}} q^m.$$

On a alors la relation suivante entre F_χ et B_χ.

Lemme 12. On a la formule

$$B_\chi | T(p)^4 - T(p)^2 = \frac{1}{u^2} F_\chi | \prod_{\mathfrak{p}|p} (T(N\mathfrak{p}) - \chi(\mathfrak{p}))^2.$$

Faisons maintenant l'hypothèse que $F_\chi|e$ est une forme modulaire de niveau N (et non seulement de niveau Np). Notons $\mathbb{I}_f$ le projecteur sur $M_2(\Gamma_0(N),\bar{A})$ associé à f (si g appartient à $M_2(\Gamma_0(N),\bar{\mathbb{Q}})$, on a $\mathbb{I}_f(g) = \frac{<f,g>_N}{<f,f>_N}$).

Donnons alors le corollaire frappant suivant :

Corollaire. On a

$$\frac{d}{ds} L_p(E/k)(\chi\nu^s)|_{s=0} = \prod_{\mathfrak{p}|p} (1 - \frac{\chi(\mathfrak{p})}{\alpha_{\mathbf{N}\mathfrak{p}}})^2 \frac{\mathbb{I}_f(F_\chi|e)}{u^2} .$$

En particulier,

$$D_{p,\nu}(E/k) = \prod_{\mathfrak{p}|p} (1 - \frac{1}{\alpha_{\mathbf{N}\mathfrak{p}}})^2 \frac{\mathbb{I}_f(F|e)}{u^2} .$$

Montrer la conjecture B revient maintenant à lier $F|e$ avec la hauteur p-adique des points de Heegner sur la partie ordinaire de $J_0(N)$.

Note ajoutée en avril 1986 : j'ai maintenant démontré la conjecture B lorsque p se décompose dans k.

BIBLIOGRAPHIE

[1] D. Bernardi, C. Goldstein.- A p-adic analogue of the Birch and Swinnerton-Dyer conjecture, C.R. Acad. Sci. Paris 301 (1985), 455-458.

[2] D. Bertrand.- Propriétés arithmétiques de fonctions thêta à plusieurs variables, Journées arithmétiques de Leiden (1983).

[3] B. Gross.- Heegner points on $X_0(N)$, In Modular forms (ed. R.A. Rankin), Chichester : Ellis Horwood (1984), 87-106

[4] B.H. Gross et D.B. Zagier.- Heegner points and derivatives of L-series, à paraître dans Inv. Math.

[5] S. Haran.- p-adic L functions for elliptic curves over CM fields, Ph D. M.I.T. (1983).

[6] H. Hida.- Congruences of cusp forms and special values of their Zeta functions, Invent. Math. 63 (1981), 225-261.

[7] H. Hida.- A p-adic measure attached to the zeta functions associated with two elliptic modular forms, I. Invent. Math. 79 (1985), 159-195.

[8] N. Katz.- The Eisenstein measure and p-adic interpolation, Amer. J. Math. 99 (1977), 238-311.

[9] B. Mazur et P. Swinnerton-Dyer.- Arithmetic of Weil curves, Invent. Math. 25 (1974), 1-61.

[10] B. Mazur et J. Tate.- Canonical height pairings via biextensions, vol. dédié à Shafarevich, Progress in Math. 35-36 (1983), 195-237.

[11] B. Mazur, J. Tate et J. Teitelbaum.- On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer.

[12] B. Perrin-Riou.- Fonctions L p-adiques attachée à une courbe elliptique modulaire et à un corps quadratique imaginaire.

[13] B. Perrin-Riou.- Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner.

[14] G. Shimura.- Introduction to the arithmetic theory of automorphic functions, Tokyo-Princeton : Iwanami Shoten et Princeton University Press (1971).

Bernadette PERRIN-RIOU
L.M.F. U.E.R. 48
45-46 3ème étage
Université P. et M. Curie
2, place Jussieu
75230 PARIS CEDEX 05