Sur la conjecture d'Iwasawa-Greenberg

Yichang CAI

17 octobre 2017

Table des matières

1 Introduction

La fonction zêta est un mystère en mathématiques. Euler a calculé les valeurs de la fonction zêta de Riemann pour quelques entiers, il a déduit que $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, ..., et que (pas rigoureusement) $\zeta(-1) = -1/(2^2 \cdot 3)$, $\zeta(-3) = 1/(2^3 \cdot 3 \cdot 5)$, $\zeta(-5) = -1/(2^2 \cdot 3^2 \cdot 7)$, $\zeta(-7) = 1/(2^4 \cdot 3 \cdot 5)$, $\zeta(-9) = -1/(2^2 \cdot 3 \cdot 11)$, $\zeta(-11) = 691/(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13)$, ... (notez la présence bizarre de 691). Kummer a trouvé un lien entre les valeurs spéciales de la fonction zêta de Riemann et les groupes des classes d'idéaux. Plus précisément, il a prouvé le théorème suivant.

Théorème 1.1. *Soit p un nombre premier. Alors p divise le numérateur de $\zeta(r)$ pour un entier r impair négatif si et seulement si p divise $\#\,\mathrm{Cl}(\mathbb{Q}(\mu_p))$.*

En particulier, puisque $\zeta(-11) = 691/(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13)$, on trouve que 691 divise $\#\operatorname{Cl}(\mathbb{Q}(\mu_{691}))$. Ce théorème illustre le phénomène que les objets analytiques et les objets arithmétiques sont reliés. Kummer a aussi trouvé la propriété de congruence de la fonction zêta de Riemann, qui conduit à la définition des fonctions L p-adiques. Ces deux résultats de Kummer sont le point de départ de la théorie d'Iwasawa.

Iwasawa a trouvé sa théorie en comparant les analogues entre les corps de nombres et corps de fonctions. Il a essayé de construire un analogue du morphisme $\operatorname{Cl}^0(\mathbb{F}_q(X)) \longrightarrow \operatorname{Cl}^0(\overline{\mathbb{F}}_q(X))$, et il a observé que la limite de la p-partie de $\operatorname{Cl}(\mathbb{Q}(\mu_{p^n}))$ avait des propriétés similaires. La conjecture principale d'Iwasawa (démontrée par Mazur et Wiles dans [MW84]) indique que l'action du groupe de Galois sur le groupe des classes d'idéaux est liée à la fonction L p-adique. Pour voir la puissance de la théorie, on cite le petit corollaire suivant : la valeur $\zeta(-11) = 691/(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13)$ indique qu'il existe un élément x d'ordre 691 de $\operatorname{Cl}(\mathbb{Q}(\mu_{691}))$ tel que $\operatorname{Gal}(\mathbb{Q}(\mu_{691})/\mathbb{Q})$ agit par $\sigma(x) = x^{\omega(\sigma)}$ où $\omega : \operatorname{Gal}(\mathbb{Q}(\mu_{691})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/691\mathbb{Z})^\times$ est l'isomorphisme canonique.

Mazur a appliqué l'idée d'Iwasawa pour étudier les courbes elliptiques. Dans ce cas, l'analogue du groupe des classes d'idéaux est le groupe de Selmer, un certain sous-groupe du groupe de cohomologie galoisienne $H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})_{\mathrm{tor}})$. Il a aussi formulé la conjecture principale pour les courbes elliptiques, et maintenant on a beaucoup de résultats positifs.

Greenberg a formulé des conjectures principales pour des systèmes de représentations galoisiennes l-adiques compatibles, ou pour les motifs. Il a défini un groupe de Selmer naturel à partir de représentations galoisiennes quand un motif a bonne réduction ordinaire en p. Quand on a une forme automorphe, on peut considérer la représentation galoisienne par la correspondance de Langlands, et définir le groupe de Selmer associé.

En général, les conjectures principales d'Iwasawa postulent l'égalité de deux idéaux ; l'un est défini analytiquement — typiquement ce sera l'idéal engrendré par une fonction L p-adique dans un anneau de séries formelles — l'autre est défini arithmétiquement — typiquement il s'agira de l'idéal caractéristique d'un groupe de Selmer.

Hida a défini des idéaux de congruence et il a montré les égalités

$$\begin{aligned}(\text{fonctions } L\ p-\text{adiques}) &= (\text{idéaux de congruence}) \\ &= (\text{idéaux caractéristiques d'un groupe de Selmer})\end{aligned}$$

dans certains cas. Dans un travail récemment réalisé ([HT16]), Hida et Tilouine ont montré l'égalité

$$(\text{idéal de congruence}) = (\text{idéal caractéristique d'un groupe de Selmer})$$

pour les groupes de Selmer de certaines familles p-adiques de représentations galoisiennes obtenues par fonctorialité à partir de familles p-adiques de formes automorphes ordinaires. Le point de départ est les théorèmes du type $R = \mathbb{T}$ originellement dus à Wiles. Un but de ma thèse est de généraliser ce résultat dans le cas de pente finie.

Dans cet article, on va insister plus sur la partie arithmétique. Pour des raisons de simplicité, les traitements ne sont pas les plus généraux.

2 Théorie d'Iwasawa classique

Comme indiqué dans l'introduction, Iwasawa a remarqué qu'on peut faire croître le corps de base dans la tour des corps cyclotomiques pour étudier le groupe des classes d'idéaux. La limite des groupes des classes d'idéaux devient un module sur un anneau ayant une bonne structure, et son idéal caractéristique est égal à une fonction L p-adique. Par simplicité, on fixe un nombre premier $p \geq 5$.

2.1 $\mathbb{Z}_p$-extensions d'un corps de nombres

Soit μ_n l'ensemble des racines n-ièmes de l'unité ($n \geq 1$). Pour un corps de nombres K, on écrit A_K pour le p-sous-groupe de Sylow de $\mathrm{Cl}(K)$.

Définition 2.1. Soit K un corps de nombres et soit K_∞/K une extension galoisienne algébrique. On dit que K_∞/K est une $\mathbb{Z}_p$-extension lorsqu'on a $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$.

Soit maintenant K un corps de nombres contenant μ_p. On note $K_n = K(\mu_{p^n})$ pour $n \geq 1$ et $K_\infty = \bigcup_{n\geq 1} K_n$; alors on voit que K_∞/K est une $\mathbb{Z}_p$-extension. Soit L_n la plus grande p-extension abélienne non ramifiée sur K_n. On pose $L_\infty = \bigcup_{n\geq 1} L_n$.

La théorie des corps de classes nous donne un isomorphisme de groupes

$$\Phi_n : A_{K_n} \xrightarrow{\sim} \mathrm{Gal}(L_n/K_n)$$

pour chaque n. Le groupe $\mathrm{Gal}(K_n/K)$ agit naturellement sur les deux côtés, et on peut montrer que Φ_n est en fait un isomorphisme de $\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$-modules. De plus, pour $m > n$, on a le diagramme commutatif suivant

$$\begin{array}{ccc} A_{K_m} & \xrightarrow{\Phi_{K_m}} & \mathrm{Gal}(L_m/K_m) \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle i} \\ A_{K_n} & \xrightarrow{\Phi_{K_n}} & \mathrm{Gal}(L_n/K_n), \end{array}$$

où N est la norme et i est la restriction. Soit $X = \varprojlim A_{K_n}$. En prenant la limite projective, on obtient un isomorphisme de $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-modules

$$\Phi : X \xrightarrow{\sim} \mathrm{Gal}(L_\infty/K_\infty).$$

2.2 Algèbre d'Iwasawa

Pour un groupe profini G, on définit $\mathbb{Z}_p[[G]] = \varprojlim \mathbb{Z}_p[G/U]$, où U décrit l'ensemble des sous-groupes normaux ouverts de G. L'anneau $\Lambda = \mathbb{Z}_p[[G]]$ est souvent appelé l'algèbre d'Iwasawa. Si $G \simeq \mathbb{Z}_p$, l'algèbre $\mathbb{Z}_p[[G]]$ a des propriétés similaires à un anneau principal.

Théorème 2.2. *Soit R un anneau p-adiquement complet et séparé. On écrit $[\alpha]$ pour l'élément de $R[[\mathbb{Z}_p]]$ associé à $\alpha \in \mathbb{Z}_p$. Alors on a un isomorphisme d'anneaux*

$$R[[T]] \xrightarrow{\sim} R[[\mathbb{Z}_p]]$$

qui envoie T sur $[1]-1$.

On note $\Lambda_1 = \mathbb{Z}_p[[T]]$. D'après le théorème, on a un isomorphisme $\Lambda_1 \simeq \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$. Il existe une théorie pour les modules de torsion de type fini sur Λ_1, comme pour les modules de type fini sur un anneau principal.

Définition 2.3. Soient M et N des modules de torsion de type fini sur Λ_1. On dit qu'un morphisme $\varphi : M \to N$ est un pseudo-isomorphisme si le noyau et le cokernel de φ sont d'ordre fini.

Proposition 2.4. *Soit M un module de torsion de type fini sur Λ_1. Alors on a*

$$M \sim \Lambda_1/(f_1^{n_1}) \oplus \cdots \oplus \Lambda_1/(f_r^{n_r}),$$

où $\sim$ signifie pseudo-isomorphisme, les éléments $f_1, \ldots, f_r \in \Lambda_1$ sont irréductibles et $n_1, \ldots, n_r$ sont des entiers positifs. De plus, la décomposition est unique à l'ordre près et à un facteur inversible près.

On appelle $\mathrm{Char}(M) = \prod_{i=1}^r (f_i^{n_i})$ l'idéal caractéristique de M.

Remarque 2.5. Pour la théorie générale des pseudo-isomorphismes et des idéaux caractéristiques sur un anneau intègre noethérien normal, on peut voir [AC], VII.4.

Théorème 2.6 (Théorème de préparation de Weierstrass)**.** *Soit R un un anneau de valuation discrète complet, soit (π) l'idéal maximal de R. Alors un élément $f \in R[[T]]$ peut être factorisé uniquement comme ci-dessous*

$$f = \pi^\mu (T^\lambda + a_1 T^{\lambda-1} + \cdots + a_\lambda) u(T),$$

où $\lambda, \mu \in \mathbb{Z}_{\geq 0}$, $a_1, \ldots, a_\lambda \in \pi R$ et $u(T) \in R[[T]]^\times$.

On écrit $\lambda(f)$ et $\mu(f)$ pour λ et μ respectivement. Ils sont appelés l'invariant λ et l'invariant μ de f.

Maintenant on peut appliquer le théorème de préparation de Weierstrass à $\mathrm{Char}(M)$ pour un module M de torsion de type fini et on obtient l'invariant $\lambda(M) := \lambda(\mathrm{Char}(M))$ et l'invariant $\mu(M) := \mu(\mathrm{Char}(M))$.

En général, il est important de montrer que les modules qui nous intéressent sont de torsion de type fini sur l'algèbre d'Iwasawa. Dans le cas classique, c'est un théorème d'Iwasawa.

Théorème 2.7. *Le module $X = \varprojlim A_{K_n}$ est de torsion de type fini sur Λ_1.*

Une étude détaillée du module X donne le théorème très connu suivant.

Théorème 2.8 (Iwasawa). *Supposons que $\#A_{K_n} = p^{e_n}$. On note $\lambda = \lambda(X)$ et $\mu = \mu(X)$. Alors il existe $\nu \in \mathbb{Z}$ tel que pour tout n suffisamment grand, on a*

$$e_n = \lambda n + \mu p^n + \nu.$$

2.3 Fonctions L p-adiques

Soit $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ un caractère de Dirichlet primitif. Rappelons que la fonction L associeé est définie par $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. Elle admet un prolongement analytique sur $\mathbb{C}$. Rappelons aussi le caractère de Teichmüller $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ qui identifie $(\mathbb{Z}/p\mathbb{Z})^\times$ avec les racines $(p-1)$-ièmes de l'unité de $\mathbb{Z}_p^\times$.

Kubota et Leopoldt ont montré qu'il existe une unique fonction L p-adique $L_p(s,\chi)$ telle que

$$L_p(1-r,\chi) = (1-\chi\omega^{-r}(p)p^{r-1})L(1-r,\chi\omega^{-r})$$

pour $r \in \mathbb{Z}_{\geq 1}$. La fonction $L_p(s,\chi)$ est analytique. Elle est définie sur $\mathbb{Z}_p$ si χ n'est pas trivial, et sur $\mathbb{Z}_p \smallsetminus \{1\}$ si non. On remarque que si le caractère est impair (c'est-à-dire, $\chi(-1) = -1$), alors $L_p(s,\chi)$ est identiquement nulle, donc il suffit de considérer les caractères pairs.

Iwasawa a prouvé que la fonction L_p réside en fait dans $\mathcal{O}_\chi[[T]]$ (ici $\mathcal{O}_\chi = \mathbb{Z}_p[\mathrm{Im}\chi]$ est un anneau de valuation discrète complet).

Théorème 2.9 (Iwasawa). *On fixe un générateur topologique u de $1 + p\mathbb{Z}_p$.*

(1) Pour un caractère de Dirichlet primitif χ, il existe un élément $G_\chi(T)$ de $\mathrm{Frac}(\mathcal{O}_\chi[[T]])$ tel que

$$L_p(s,\chi) = G_\chi(u^s - 1).$$

(2) Si le conducteur de χ n'est ni 1 ni $p^n (n \geq 2)$, alors $G_\chi(T)$ est un élément de $\mathcal{O}_\chi[[T]]$.

On peut en déduire la conguence de Kummer : si r_1 et r_2 sont des entiers positifs non divisés par $p-1$, et $r_1 \equiv r_2 \mod (p-1)p^{n-1}$ avec $n \geq 1$, alors

$$(1-p^{r_1-1})\zeta(1-r_1) \equiv (1-p^{r_2-1})\zeta(1-r_2) \mod p^n.$$

Supposons que le conducteur de χ n'est ni 1 ni $p^n (n \geq 2)$. Le théorème de Ferrero-Washington nous dit qu'au moins un coefficient de $G_\chi(T)$ est inversible dans $\mathcal{O}_\chi$. Cela implique que l'invariant $\mu(X)$ est nul.

2.4 La conjecture principale

Supposons que χ est un caractère de Dirichlet primitif de conducteur $N = N_0 p$ où N_0 est non divisible par p. On suppose de plus que $\chi \neq \omega$. On définit

$$K_n = \mathbb{Q}(\mu_{N_0 p^n}),$$
$$K_\infty = \mathbb{Q}(\mu_{N_0 p^\infty}) = \bigcup_{n \geq 1} K_n,$$

et on écrit $K = K_1$. Alors $\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \Delta \times \Gamma$, où $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ et $\Gamma = \mathrm{Gal}(K_\infty/K)$. On peut regarder χ comme un caractère de Δ.

On définit

$$\Lambda_{N_0} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] = \mathbb{Z}_p[[\Delta \times \Gamma]],$$
$$\Lambda_\chi = \mathcal{O}_\chi[[\mathrm{Gal}(K_\infty/K)]] = \mathcal{O}_\chi[[\Gamma]].$$

Notons que $\Lambda_\chi \simeq \mathcal{O}_\chi[[T]]$ par le théorème 2.2, et on a un morphisme naturel d'anneaux $\varphi_\chi : \Lambda_{N_0} \to \Lambda_\chi$.

Rappelons que $X_{K_\infty} = \varprojlim A_{K_n}$ est un module de torsion de type fini sur $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$, c'est bien sûr aussi un module de torsion de type fini sur $\Lambda_{N_0} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$. On définit

$$X_\chi = X_{K_\infty} \otimes_{\Lambda_{N_0}} \Lambda_\chi,$$

alors X_χ est un module de torsion de type fini sur Λ_χ. Donc l'idéal principal $\mathrm{Char}(X_\chi) \subset \Lambda_\chi$ est bien défini. D'autre part, il existe un élément $G_{\chi^{-1}\omega}(T) \in \mathcal{O}_\chi[[T]]$ par le théorème 2.9. Maintenant, on peut formuler la conjecture principale.

Théorème 2.10 (La conjecture principale)**.** *Soit χ comme ci-dessus. Alors on a l'égalité*

$$\mathrm{Char}(X_\chi) = (G_{\chi^{-1}\omega}(T)).$$

Remarque 2.11. La conjecture principale a été prouvée par deux méthodes différentes. L'une due à Mazur et Wiles ([MW84]) en utilisant des formes modulaires, l'autre à Rubin (chapitre 15 de [ICF]) en utilisant la méthode de Kolyvagin. La première méthode démontre la divisibilité $(G_{\chi^{-1}\omega}(T)) \mid \mathrm{Char}(X_\chi)$; par contre, la seconde méthode démontre la divisibilité inverse. Grâce à la formule du nombre de classes, chaque divisibilité implique l'égalité.

3 Théorie d'Iwasawa pour les courbes elliptiques

On fixe toujours un nombre premier $p \geq 5$. On rappelle quelques faits sur les courbes elliptiques. Dans le texte qui suit, on suppose que $E/\mathbb{Q}$ est une courbe elliptique définie

sur $\mathbb{Q}$, c'est-à-dire, E est une courbe algébrique projective non singulière de genre 1 sur $\mathbb{Q}$. Alors E peut être réalisée par une équation de Weierstrass

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

Pour un corps $K \supset \mathbb{Q}$, on note $E(K)$ l'ensemble des K-points de E. On rappelle le célèbre théorème de Mordell et Weil.

Théorème 3.1 (Mordell-Weil)**.** *Pour un corps de nombres K, le groupe $E(K)$ a la forme*

$$E(K) \simeq E(K)_{\text{tor}} \oplus \mathbb{Z}^r, \quad r \in \mathbb{Z}_{\geq 0}.$$

Mais pour une extension infinie $K/\mathbb{Q}$, le théorème ne marche plus. On veut étudier la structure des groupes $E(K_n)$ pour une tour (K_n).

Dorénavant, on suppose que E a bonne réduction ordinaire en p, c'est-à-dire, la réduction $\widetilde{E} := E \mod p$ est une courbe elliptique sur $\mathbb{F}_p$, et $\widetilde{E}$ a des points de p-torsion.

3.1 Groupe de Selmer

Une méthode pour étudier le groupe $E(K)$ est via la cohomologie galoisienne.

Soit L un corps de caractéristique 0. On rappelle le morphisme de Kummer

$$\kappa : E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to H^1(L, E(\overline{L})_{\text{tor}})$$

défini comme ci-dessous : pour $\alpha = P \otimes r$ où $P \in E(L)$ et $r = \frac{m}{n} + \mathbb{Z}$, on choisit $Q \in E(\overline{L})$ tel que $nQ = mP$, et on définit un 1-cocycle

$$\begin{aligned} \varphi_\alpha : G_L &\to E(\overline{L}) \\ g &\mapsto g(Q) - Q. \end{aligned}$$

Ensuite, on pose $\kappa(\alpha) = [\varphi_\alpha]$. C'est la contrepartie, dans le cas des courbes eliptiques, de la version limite inductive du morphisme de Kummer $L^\times/(L^\times)^n \xrightarrow{\sim} H^1(L, \mu)$ dans le cas classique.

Supposons que K est un corps de nombres. On note κ_v (v une place de K) pour le morphisme de Kummer de K_v. Le groupe de Selmer est défini par

$$\text{Sel}(E/K) = \ker(H^1(K, E(\overline{K})_{\text{tor}}) \to \prod_{v \text{ place de } K} (H^1(K_v, E(\overline{K}_v)_{\text{tor}})/\text{im}(\kappa_v))).$$

Rappelons aussi le groupe de Tate-Shafarevich

$$Ш(E/K) = \ker(H^1(K, E(\overline{K})) \to \prod_{v \text{ place de } K} H^1(K_v.E(\overline{K}_v))).$$

C'est une conjecture fondamentale que $Ш(E/K)$ est toujours fini.

On a une suite exacte qui fait le lien entre les groupes $E(K)$, $\mathrm{Sel}(E/K)$ et $Ш(E/K)$:

$$0 \to E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}(E/K) \to Ш(E/K) \to 0.$$

Donc les groupes $\mathrm{Sel}(E/K)$ et $Ш(E/K)$ portent des informations significatives de E.

Nous focaliserons notre attention sur la p-partie du groupe de Selmer

$$\mathrm{Sel}(E/K)_p = \ker(H^1(K, E[p^\infty]) \to \prod_{v \text{ place de } K} (H^1(K_v, E[p^\infty])/\mathrm{im}(\kappa_v))).$$

On note $X(E/K) = \mathrm{Hom}(\mathrm{Sel}(E/K)_p, \mathbb{Q}_p/\mathbb{Z}_p)$ pour le dual de Pontryagin.

On peut définir une tour de corps $K_\infty = \bigcup_n K_n$ pour la courbe elliptique E, où K_n est le corps fixé par le noyau de $\rho_{p^n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p^n])$, et on note $G = \mathrm{Gal}(K_\infty/\mathbb{Q})$. Alors la limite $X = \varprojlim X(E/K_n)$ est le Λ-module que on souhaite étudier (ici $\Lambda = \mathbb{Z}_p[[G]]$). On sait que c'est de type fini, et la question est de déterminer si X est de torsion. Quand E est à multiplication complexe, l'algèbre Λ est commutative et similaire à $\Lambda_1 = \mathbb{Z}_p[[T]]$, et la théorie est assez connue (voir [Rub91]). Mais si E n'est pas à multiplication complexe, alors l'algèbre Λ n'est pas commutative. Le cas non commutatif a été développé par Coates, Fukaya, Kato and Sujatha et Venjakob dans [CFKSV].

3.2 La conjecture principale

La fonction L complexe d'une courbe elliptique $E/\mathbb{Q}$ est définie par

$$L(E, s) = \prod_l P_l(l^{-s})^{-1} \text{ pour } \Re(s) > 3/2,$$

où $P_l(T) = 1 - a_l T + lT^2$ avec $a_l = l + 1 - E(\mathbb{F}_l)$ quand E a bonne réduction en l, et $P_l(T) = 1 - T$, ou $1 + T$, ou 1 quand E a réduction multiplicative déployée, ou réduction multiplicative non déployée, ou réduction additive en l respectivement. Elle admet un prolongement analytique sur $\mathbb{C}$. On mentionne la célèbre conjecture de Birch et Swinnerton-Dyer.

Conjecture 3.2 (BSD)**.** *Soit $E/\mathbb{Q}$ une courbe elliptique. Alors*

(1) L'ordre de $L(E, s)$ en $s = 1$ est égal au rang de E.

(2) Le groupe de Tate-Shafarevich $Ш(E/\mathbb{Q})$ est toujours fini.

(3) Soit r l'ordre de $L(E, s)$ en $s = 1$. Alors

$$\lim_{s \to 1} (s-1)^{-r} L(E, s) = \frac{h_E R_E \Omega_E \tau(E)}{\omega_E}.$$

La partie (3) est la version courbe elliptique de la formule du nombre de classes. On mentionne aussi que le premier résultat important démontré par Coates et Wiles (qui dit $L(E,1) \neq 0 \Rightarrow E(\mathbb{Q})$ est fini dans certaines conditions) est inspiré par la théorie d'Iwasawa.

Il est souvent important de regarder la version p-adique de la fonction $L(E,s)$. On peut définir la fonction L p-adique $L_p(E)$ comme un élément de $\Lambda[1/p]$. L'idée est que les valeurs spéciales de la famille $L_R(E,s)$ en $s=1$ peuvent être interpolées p-adiquement (R est un ensemble fini de nombres premiers de $\mathbb{Q}$). Pour plus de détails, on peut voir [MTT86].

La conjecture principale dans ce cas est formulée comme suit.

Conjecture 3.3 (La conjecture principale)**.** *On a l'égalité suivante.*

$$(L_p(E)) = \mathrm{Char}(X).$$

Remarque 3.4. (1) Dans le cas où E est à multiplication complexe, la conjecture a été démontrée par Rubin dans [Rub91].

(2) Dans le cas où E n'est pas à multiplication complexe, il existe $n \geq 0$ tel que $\mathrm{Char}(X)$ divise $(p^n L_p(E))$.

(3) Skinner et Urban ont démontré que $L_p(E)$ divise $\mathrm{Char}(X)$ sous certaines hypothèses.

Les résultats (1) et (2) sont démontrés en utilisant le système d'Euler, et le résultat (3) est démontré en utilisant des formes modulaires.

4 Formalisme de Greenberg

Dans l'article [Gre91], Greenberg a formulé la conjecture principale d'Iwasawa pour une famille analytique $\{V_p \otimes \varphi\}$, où V_p est une $G_{\mathbb{Q}}$-représentation p-adique et φ décrit un sous-ensemble de $\mathrm{Hom}(\mathbb{Z}_p, \mathbb{C}_p^{\times})$.

On peut définir les groupes de Selmer pour une représentation p-adique (voir par exemple le chapitre 1 de [Rub00]). En général, on a besoin de l'anneau de Fontaine $\mathbb{B}_{\mathrm{cris}}$, mais la condition devient facile si on suppose que la représentation V_p est ordinaire, c'est-à-dire qu'il existe une $G_{\mathbb{Q}_p}$-filtration F^i de V_p telle que

(1) $F^{i+1} \subset F^i$. $F^i = V_p$ pour $i << 0$, et $F^i = 0$ pour $i >> 0$.

(2) le groupe d'inertie $I_{\mathbb{Q}_p}$ agit sur $\mathrm{gr}^i = F^i/F^{i+1}$ par $\mathcal{N}^i$ où $\mathcal{N}$ est le p-adique caractère cyclotomique.

Remarque 4.1. (1) Un exemple de base est la représentation $V_p = \mathbb{Q}_p(n)$ où $G_{\mathbb{Q}}$ agit par $\mathcal{N}^n$, $n \in \mathbb{Z}$.

(2) Soit $E/\mathbb{Q}$ une courbe elliptique qui a bonne réduction ordinaire en p. Soit $T_p^1(E)$ le noyau du morphisme de Tate $T_p(E) \to T_p(\widetilde{E})$. On peut mettre $V_p = F^0 = T_p(E) \otimes \mathbb{Q}_p$, $F^1 = T_p^1(E) \otimes \mathbb{Q}_p$, et $F^2 = 0$. Alors le groupe d'inertie $I_{\mathbb{Q}_p}$ agit trivialement sur gr^0 et agit par $\mathcal{N}^1$ sur gr^1.

Soit T_p un réseau $G_{\mathbb{Q}_p}$-invariant de V_p et soit $A = V_p/T_p$. On écrit $F^+(A)$ pour l'image de F^1 dans A. Le groupe de Selmer est défini par

$$S_A(\mathbb{Q}_\infty) = \ker(H^1(\overline{\mathbb{Q}}/\mathbb{Q}_\infty, A) \to H^1(I_\pi, A/F^+(A)) \times \prod_{\lambda \neq \pi} H^1(I_{\lambda,A})),$$

où π est la place de $\mathbb{Q}_\infty$ au-dessus de p.

Remarque 4.2. (1) Pour la famille des représentations $\{\mathbb{Q}_l(n)\}$, le groupe de Selmer $S_A(\mathbb{Q}_\infty)$ est le dual Pontryagin de $X = \varprojlim A_{\mathbb{Q}_n}$.

(2) Dans le cas de courbes elliptiques, ça correspond au groupe de Selmer pour des courbes elliptiques sur $\mathbb{Q}_\infty$.

Soit $\Sigma = \{p, \infty\} \cup \{\text{places ramifiées}\}$. Soit Σ_∞ les places de $\mathbb{Q}_\infty$ au-dessus de Σ. On peut montrer que pour $\lambda \notin \Sigma_\infty$, le groupe d'inertie I_λ agit trivialement sur A. Donc on dérive la description alternative

$$S_A(\mathbb{Q}_\infty) = \ker(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A) \to H^1(I_\pi, A/F^+(A)) \times \prod_{\pi \neq \lambda \in \Sigma_\infty} H^1(I_\lambda, A)).$$

Maintenant $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ agit naturellement sur $S_A(\mathbb{Q}_\infty)$ et on voit que $S_A(\mathbb{Q}_\infty)$ est un Λ_1-module et le dual de Pontryagin $X = S_A(\mathbb{Q}_\infty)\hat{}$ est de type fini sur Λ_1. La conjecture suivante est essentielle.

Conjecture 4.3. *Le dual de Pontryagin X est de torsion sur Λ_1.*

Si la conjecture est vérifiée, alors on peut définir un élément $\theta_A \in \mathrm{Frac}(\Lambda_1)$ en utilisant l'idéal caractéristique $\mathrm{Char}(X)$. C'est l'objet du côté arithmétique.

Dans le côté analytique, la fonction L p-adique $L_p(\varphi, V)$ (φ un caractère) est supposée avoir certaines propriétés (voir [Gre91] pour les détails), mais l'existence est conjecturale en général. Elle est supposée habiter dans le corps des fraction de l'algèbre d'Iwasawa : il existe $\theta_V \in \mathrm{Frac}(\Lambda_1)$ tel que $L_p(\varphi, V) = \varphi(\theta_V)$ sauf un nombre fini de φ.

Exemple 4.4. Si $V = \{\mathbb{Q}_l(n)\}$, alors $L_V(s) = \zeta(s-n)$, et $L_V(1, \varphi) = L(1-n, \varphi)$ (la fonction L de Dirichlet). La fonction $L_p(\varphi, V)$ est caractérisée par $L_V(1, \varphi)$, donc c'est essentiellement la fonction L de Kubota et Leopoldt.

Maintenant, on présente la conjecture principale.

Conjecture 4.5 (La conjecture principale)**.** *Les deux idéaux sont égaux :* $(\theta_V) = (\theta_A)$.

5 Idéaux de congruence

Au lieu d'établir la relation entre l'idéal caractéristique et la fonction L p-adique, on peut introduire un objet du milieu, qui s'appelle l'idéaux de congruence.

Supposons que R est une A-algèbre de rang fini réduite sur un anneau réduit A avec un morphisme de A-algèbres $\lambda : R \to A$. On peut définir l'idéal de congruence $\mathfrak{c}_\lambda$ qui est en fait un idéal de A. On a aussi le module différentiel $C_1(\lambda, A) = \Omega_{R/A} \otimes_R A$ (qui sera le dual du groupe de Selmer), où $\Omega_{R/A}$ est le R-module qui représente le foncteur

$$M \to \mathrm{Der}_A(R, M) = \{\delta : R \to M \in \mathrm{Hom}_A(R, M) \mid \delta(ab) = a\delta(b) + b\delta(a)\}.$$

Il existe une décomposition $Q(R) = Q(A) \oplus X$ comme A-algèbres, où $Q(\bullet)$ signifie l'anneau total des fractions. Soit R_A l'image de $R \to X$ et soit $\mathfrak{b}$ le noyau de $R \to A$, alors on a les isomorphismes $A/\mathfrak{c}_\lambda \simeq R_A/\mathfrak{b}$ et $C_1(\lambda, A) \simeq \mathfrak{b}/\mathfrak{b}^2$. De plus, on peut définir $C_n(\lambda, A) = \mathfrak{b}^n/\mathfrak{b}^{n+1}$ pour $n \in \mathbb{N}$. Quand R est un anneau de déformation universel, la connaissance de $\bigoplus_n C_n(\lambda, A)$ est presque équivalente à la connaissance de R.

Les idéaux de congruence satisfont la propriété du transfert suivante.

Proposition 5.1. *Soit A un anneau intègre noethérien local. Soient R et S des A-algèbres plates de rang fini réduites, de Gorenstein sur A. Si on a des morphismes de A-algèbres*

$$\begin{array}{ccccc} & & \overset{\lambda}{\frown} & & \\ R & \xrightarrow{\theta} & S & \xrightarrow{\mu} & A\,, \end{array}$$

avec $\lambda = \mu \circ \theta$, alors $\mathfrak{c}_\mu$ et $\mathfrak{c}_\lambda$ sont des idéaux principaux de A, et $\mathfrak{c}_\theta$ est un idéal principal de S. De plus, on a $\lambda(\mathfrak{c}_\theta) \cdot \mathfrak{c}_\mu = \mathfrak{c}_\lambda$.

On a un théorème de Tate qui relie l'idéal de congruence et le module différentiel quand R est d'intersection complète sur A.

Théorème 5.2 (Tate)**.** *Soit A un anneau intègre noethérien local complet normal. Supposons que R est réduite et d'intersection complète sur A avec un morphisme de A-algèbres $\lambda : R \to A$. Alors $C_1(\lambda, A)$ est un A-module de torsion de type fini, et on a :*

$$\mathrm{Char}(C_1(\lambda, A)) = \mathfrak{c}_\lambda.$$

Dans l'article [HT16], en utilisant le théorème de Tate ci-dessus, les auteurs démontrent les théorèmes du type : l'idéal caractéristique d'un groupe de Selmer est un générateur de l'idéal de congruence entre certaines familles de formes automorphes. La fonction L p-adique n'a pas encore été construite dans ce cas, et on peut considérer l'idéal de congruences comme la fonction L p-adique du pauvre.

On considère plus généralement un L-homomorphisme $\varphi : {}^L H \to {}^L G$. On suppose que les représentations galoisiennes dans ${}^L H$ et dans ${}^L G$ ont été construites ainsi que les variétés de Hecke pour H et G. Un point clé dans la démonstration est de montrer des théorèmes $R_H = \mathbb{T}_H$ et $R_G = \mathbb{T}_G$ concernant les déformations de représentations galoisiennes. Ces conditions sont remplies dans plusieurs situations, par exemple carré extérieur de GL_4,

transfert à GL_n puis à des groupes unitaires, transfert de GSp(4) à $U(4)$. Des d'égalités $\lambda(\mathfrak{c}_\theta) = \mathrm{Char}(\mathrm{Sel})$ sont démontrables.

La question du lien entre les idéaux de congruences et les fonctions L p-adiques peut probablement être abordée dans le cas par exemple du changement de base d'une forme classique à un corps quadratique réel. Dans ce cas, on pense pouvoir montrer que la divisibilité de la valeur spéciale en 1 de la fonction L adjointe tordue entraîne l'existence d'une classe non triviale dans le groupe de Selmer de l'adjoint de l'induite de la représentation galoisienne associée à une forme classique.

Références

[AC] N. Bourbaki. *Algèbre Commutative*. Hermann, Paris, 1961-1998.

[CFKSV] J. Coates, T. Fukaya, K. Kato, R.Sujatha et O. Venjakob. *The GL2 main conjecture for elliptic curves without complex multiplication*. Publications Mathématiques de l'IHÉS, 101, 163–208, 2005.

[Gre91] R. Greenberg. *Iwasawa theory for motives*. LMS Lecture Note Series 153, 211–234, 1991.

[Gre94] R. Greenberg. *Iwasawa theory and p-adic deformations of motives*. Proceedings of Symposia in Pure Math. 55 II, 193–223, 1994.

[Gre01] R. Greenberg. *Introduction to Iwasawa theory for elliptic curves*. IAS/Park City Mathematics Series 9, 407–464, 2001.

[Hid00] H. Hida. *Adjoint Selmer groups as Iwasawa modules*. Israel J. Math. 120, 361–427, 2000.

[Hid16] H. Hida. *Arithmetic of adjoint L-values*. Chapter 6 of p-Adic Aspects of Modular Forms, pp.185–236, World Scientific, 2016.

[HT16] H. Hida et J. Tilouine. *Symmetric power congruence ideals and Selmer groups*. preprint, 2016.

[ICF] L. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[Kat06] K. Kato. *Iwasawa theory and generalizations*. Proceedings of the International Congress of Mathematicians, Madrid, Spain, 2006.

[MTT86] B. Mazur, J. Tate et J. Teitelbaum. *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Inventiones Mathematicae, 84, 1–48, 1986.

[MT90] B. Mazur et J. Tilouine. *Représentations galoisiennes, différentielles de Kaehler et "Conjectures Principales"*. Publ. Math. de l'Inst. des Hautes Etudes Sci. No.71, 65–103, 1990.

[MW84] B. Mazur et A. Wiles. *Class fields of abelian extensions of* $\mathbb{Q}$. Invent. Math. 76 , 179–330, 1984.

[NT3] N. Kurokawa, M. Kurihara et T. Saito. *Number Theory 3 : Iwasawa Theory and Modular Forms*. Translations of Mathematical Monographs Iwanami Series in Modern Mathematics, 2012.

[Rub91] K. Rubin. *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*. Invent. Math. 103, 25–68, 1991.

[Rub00] K. Rubin. *Euler systems*. Annals of Mathematics Studies, 147, Princeton University Press, 2000.