Fonctions L p-adiques - mémoire de magistère

Li Ma.

9 juillet 2009

Introduction

Cet article est une introduction aux fonctions L p-adiques.

La première partie introduira les courbes elliptiques sur $\mathbb{Q}$, les formes modulaires, et leurs fonctions L (classiques) associées. Le théorème de modularité établit un lien entre ces deux objets.

La deuxième partie rappellera brièvement la définition du corps p-adique et la construction de la fonction zeta p-adique. C'est aussi une inspiration pour la définition d'une fonction L p-adique.

Dans la troisième partie on verra deux constructions de fonctions L p-adiques associées à une courbe elliptique sur $\mathbb{Q}$. On présentera à la fin le cadre anticyclotomique et l'intervention des représentations p-adiques.

Pour des raisons de simplifications, quelques définitions et résultats ne sont pas les plus généraux possibles.

Table des matières

Introduction **1**

1 Fonctions L **2**
1.1 Courbes elliptiques sur $\mathbb{Q}$ 3
1.2 Formes modulaires 5

2 p-adique **6**
2.1 Nombres p-adiques 7
2.2 Conguence de Kummer et fonction zeta p-adique 7

3 Fonctions L p-adiques **9**
3.1 Construction de Mazur-Swinnerton-Dyer 9
3.2 Construction de Schneider 10
3.3 Le cadre anticyclotomique 11
3.4 L'approche d'Emerton 11

Références **12**

1 Fonctions L

Dans l'histoire, les fonctions L (complexes) ont été inventées par Dirichlet pour démontrer son théorème sur l'infinité des nombres premiers dans une progression arithmétique. On appelle une "série formelle de Dirichlet" une série de la forme :

$$f(s) = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \cdots + \frac{a_n}{n^s} + \cdots = \sum_{n \geq 1} \frac{a_n}{n^s},$$

où s est une variable formelle et les a_n sont dans un corps (par exemple, un corps de nombres). Habituellement, si cette série provient d'un objet arithmétique, alors elle converge pour s dans un demi-plan à droite du plan complexe, et la fonction qu'elle définit s'étend à une fonction méromorphe (ou même holomorphe) sur $\mathbb{C}$, que l'on appelle la "fonction L". Cette fonction va concentrer beaucoup d'information arithmétique de l'objet original.

Exemple 1. La fonction zeta de Riemann est définie par la série : $\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s}$. Cette fonction s'étend en une fonction méromorphe sur $\mathbb{C}$, avec un seul pôle en $z = 1$. L'hypothèse de Riemann prédit que tous les zéros non-triviaux de cette fonction sont sur la droite $\Im(s) = \frac{1}{2}$.

2. Si $p \equiv 3 (\text{mod } 4)$ est un nombre premier, il y a une fonction L associée au corps de nombres $K = \mathbb{Q}(\sqrt{-p})$, définie par : $L_K(s) := \sum_{n\geq 1} \frac{\chi(n)}{n^s}$, où χ est le symbol de Legendre modulo p. Cette fonction s'étend à une fonction entière sur $\mathbb{C}$, et la formule de nombre de classes relie la valeur $L_K(1)$ au nombre de classes de l'anneau $\mathcal{O}_K$ des entiers de K.

Dans la suite, on va introduire les fonctions L associées aux courbes elliptiques sur $\mathbb{Q}$ et aux formes modulaires, qui sont des objets arithmétiques intéressants. On va voir comment ces fonctions sont liées aux propriétés arithmétiques des objets.

1.1 Courbes elliptiques sur $\mathbb{Q}$

On commence par la définition d'une courbe elliptique.

Définition 1.1. *Une "courbe elliptique" E sur $\mathbb{Q}$ est une courbe projective lisse de genre 1 définie sur $\mathbb{Q}$. Dans une carte affine, elle admet une équation de la forme $y^2 = f(x)$ avec $f \in \mathbb{Q}[x]$ un polynôme unitaire de degré 3 n'ayant pas de zéro multiple. Si K est une extension de $\mathbb{Q}$ (par exemple, $\mathbb{Q}(i)$, $\mathbb{R}$ ou $\mathbb{C}$), alors les solutions $(x, y) \in K^2$ de cette équation sont appelées les "K-points" de E. Le point (∞, ∞) est considéré comme un K-point pour tout K, et c'est le seul point à l'infini.*

Exemple 1. Soit $n > 0$ un entier. L'équation $y^2 = x^3 - n^2x$ définit une courbe elliptique E_n sur $\mathbb{Q}$. Les 4 points $(0, 0)$, $(n, 0)$, $(-n, 0)$, (∞, ∞) sont des $\mathbb{Q}$-points de E. Cette courbe est reliée au problème de nombres congruents. Un nombre entier est appelé un "nombre congruent" s'il est égal à l'aire d'un triangle pythagorien. Par des arguments élémentaires ([6] Chapitre I), on sait que n est un nombre congruent si et seulement si E_n possède un $\mathbb{Q}$-point hors des 4 points ci-dessus.

2. Soient A, B, C trois entiers strictement positifs tels que $A + B = C$. L'équation $y^2 = x(x - A)(x + B)$ définit une courbe elliptique, appelée la

"courbe de Frey" associée à l'égalité $A + B = C$. Cette courbe joue un rôle crucial dans la preuve du théorème de Fermat (voir ci-dessous).

Soit $E : y^2 = f(x)$ une courbe elliptique sur $\mathbb{Q}$. On va définir une fonction L associée à E. Quitte à faire des changements de variables linéaires, on suppose que $f(x)$ est à coefficients entiers et "les plus petits possibles" (c'est-à-dire les valeurs absolue des coefficients sont les plus petites possibles). Pour chaque nombre premier p, on note

$$\begin{aligned} N_p &:= \#\{(x,y) \in \mathbb{F}_p^2 : y^2 = f(x) \text{ dans } \mathbb{F}_p\}, \\ a_p &:= p - N_p, \end{aligned}$$

et on définit la fonction L associée à E par :

$$L_E(s) := \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Remarque Ce n'est pas la définition habituelle de la fonction L, mais leur quotient est juste un produit fini des facteurs de la forme $1/(1-a_p p^{-s}+p^{1-2s})$ ou $(1 \pm p^{-s})/(1 - a_p p^{-s} + p^{1-2s})$, donc en particulier n'a pas d'influence sur la conjecture de Birch-Swinnerton-Dyer ci-dessous.

Par l'inégalité de Hasse, on sait que L_E converge sur le demi-plan $\Re(s) > 3/2$ ([10] Chapitre V).

Il est bien connu que les K-points d'une courbe elliptique forment un groupe abélien ([10] Chapitre III). Quand on considère les $\mathbb{Q}$-points d'une courbe elliptique sur $\mathbb{Q}$, la situation est encore meilleure :

Théorème 1.2. *(Mordell-Weil) Le groupe abélien des $\mathbb{Q}$-points d'une courbe elliptique sur $\mathbb{Q}$ est de type fini, donc isomorphe à $T \oplus \mathbb{Z}^r$, où T est un groupe fini et $r \geq 0$ est un entier. L'entier r s'appelle le "rang" de la courbe elliptique.*

Le groupe de torsion T est facile à déterminer, mais le rang r est en général difficile à calculer. La conjecture de Birch-Swinnerton-Dyer relie le rang r au comportement de la fonction L_E au voisinage du point $s = 1$:

Conjecture 1.3. *(Birch-Swinnerton-Dyer) Le rang r d'une courbe elliptique E sur $\mathbb{Q}$ est égal à $\mathrm{ord}_{s=1} L_E(s)$, l'ordre du zéro de la fonction L_E en $s = 1$.*

Notons que l'on ne sait pas encore que L_E est défini en $s = 1$.

Exemple On considère la courbe $E_n : y^2 = x^3 - n^2x$ dans l'exemple ci-dessus. On sait que ([6] Chapitre I Proposition 17) les quatre points triviaux sont exactement les points de torsion, donc n est un nombre congruent si et seulement si le rang r est non nul. Par la conjecture de Birch-Swinnerton-Dyer, ceci est encore équivalent à $L_E(1) = 0$.

En regardant les "points de Heegner" sur une courbe elliptique, B. H. Gross et D. B. Zagier ont obtenu un résultat partiel pour la conjecture de Birch-Swinnerton-Dyer. En combinant avec les travaux de V. Kolyvagin, on a le théorème suivant :

Théorème 1.4. *(Gross-Zagier-Kolyvagin) Soit E une courbe elliptique "modulaire" (voir le chapitre ci-dessous). Si $\mathrm{ord}_{s=1}L_E(s) \leq 1$, alors on a : $\mathrm{ord}_{s=1}L_E(s) = r$.*

1.2 Formes modulaires

Soit $N > 0$ un entier. On note

$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 (\mathrm{mod} N)\}.$$

On note aussi $\mathcal{H}$ le demi-plan de Poincaré, i.e. l'ensemble des nombres complexes dont la partie imaginaire est strictement positive.

Définition 1.5. *Soit k un entier. Une forme modulaire de poids k et de niveau N est une fonction holomorphe sur $\mathcal{H}$ telle que*

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$$

et qui est de plus "holomorphe à l'infini" (aux pointes) au sens ci-dessous.

Comme la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est dans $\Gamma_0(N)$, une forme modulaire vérifie $f(z+1) = f(z)$, et donc a un développement en série de Fourier :

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n,$$

où $q = e^{2i\pi z}$ pour tout $z \in \mathcal{H}$. Dire que f est holomorphe à l'infini signifie que $a_n = 0$ pour tout $n < 0$.

Si on a de plus $a_0 = 0$, alors la forme f est dite "parabolique".

Définition 1.6. *Soit f une forme modulaire parabolique. On définit la fonction L associée à f par*

$$L_f := \sum_{n \geq 1} \frac{a_n}{n^s},$$

où $\sum a_n q^n$ est le développement de Fourier de f.

On a le résultat suivant :

Proposition 1.7. *Si f est une forme modulaire parabolique, alors la fonction L_f s'étend à une fonction holomorphe sur $\mathbb{C}$.*

Rappelons que la fonction L d'une courbe elliptique n'est pas encore définie en $s = 1$. Le théorème suivant était connu comme la "conjecture de Taniyama-Shimura-Weil", et maintenant un théorème de Wiles (et d'autres personnes) :

Théorème 1.8. *(Théorème de modularité) Pour toute courbe elliptique E sur $\mathbb{Q}$, il existe une forme modulaire parabolique f de poids 2, telle que l'on a $L_f = L_E$ (sur le demi-plan $\Re(s) > 3/2$).*

Corollaire 1.9. *La fonction L d'une courbe elliptique sur $\mathbb{Q}$ s'étend à une fonction holomorphe sur $\mathbb{C}$.*

Ce théorème, appliqué à la courbe de Frey, implique le théorème de Fermat.

2 p-adique

Les nombres p-adiques ont été décrits par Kurt Hensel en 1897. Le corps p-adique est obtenu en complétant le corps des nombres rationnels par rapport à une métrique différente de la métrique usuelle.

Dans cette partie, p est toujours un nombre premier fixé.

2.1 Nombres p-adiques

Sur le corps $\mathbb{Q}$, on définit la norme p-adique, notée $|\cdot|_p$, par les formules suivantes :

$$\begin{aligned} |0|_p &:= 0; \\ \left|p^\alpha \frac{a}{b}\right|_p &:= p^{-\alpha}, \alpha \in \mathbb{Z}, a, b \in \mathbb{Z}, p \nmid ab. \end{aligned}$$

Il est facile de voir que $|\cdot|_p$ est bien une norme, et on note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour cette norme. $|\cdot|_p$ s'étend naturellement à une norme sur $\mathbb{Q}_p$, qui fait de $\mathbb{Q}_p$ un corps normé complèt.

La norme $|\cdot|_p$ est "ultramétrique", c'est-à-dire pour $x, y \in \mathbb{Q}_p$, on a :

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

Grâce à cette inégalité, on voit que les éléments de $\mathbb{Q}_p$ de norme ≤ 1 forment un sous-anneau de $\mathbb{Q}_p$, appelé l'anneau des entiers de $\mathbb{Q}_p$, et noté $\mathbb{Z}_p$.

L'anneau $\mathbb{Z}_p$ apparaît comme les groupes de Galois de certaines extensions de corps. Par exemple, si on note $K_n := \mathbb{Q}(\zeta_n)$ où ζ_n est une p^n-ième racine de l'unité primitive, et $K_\infty := \cup_n K_n$, alors l'extension K_∞/K_1 est galoisienne de groupe de Galois isomorphe à $\mathbb{Z}_p$.

2.2 Conguence de Kummer et fonction zeta p-adique

Comme dans les autres corps complèts ($\mathbb{R}$ ou $\mathbb{C}$), on peut faire de l'analyse et de la géométrie sur le corps $\mathbb{Q}_p$. Or, le plus grand problème dans le monde p-adique est la manque d'une "mesure de Haar p-adique", qui nous impose de considérer différentes sortes de "distributions" (i.e. fonctionnelles linéaires continues sur un espace de fonctions (continues, tempérées, localement constantes, etc.)).

En étudiant des distributions localement constantes et leurs liens avec les nombres de Bernouli, N. Koblitz a présenté ([7] Chapitre II) une démonstration du théorème classique de congruence de Kummer. Rappelons que les nombres de Bernouli sont "presque" les coefficients du développement en série

entière de la fonction $t/(e^t-1)$ en $t=0$:

$$\frac{t}{e^t-1} =: \sum_{k=0}^{\infty} B_k t^k/k!.$$

Les premières valeurs des B_k sont les suivantes :

$$B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_3 = 0, B_4 = -1/30, B_5 = 0, B_6 = 1/42, \cdots$$

Rappelons aussi que les méthodes analytiques classiques (e.g. transformation de Fourier) donne la formule suivante :

$$\zeta(2k) = (-1)^{k+1}\frac{2^{2k-1}\pi^{2k}}{(2k)!}B_{2k}, \forall k \geq 1,$$

où ζ est la fonction zeta de Riemann. Combinée avec l'équation fonctionnelle de la fonction zeta, on obtient :

$$\zeta(1-k) = -\frac{B_k}{k}, \forall k > 1,$$

i.e. les nombres de Bernouli sont les "valeurs spéciales" de la fonction zeta.

Théorème 2.1. *(Conguence de Kummer) 1) Si on a $p-1 \nmid k$, alors on a $|B_k/k|_p \leq 1$.*
2) Si on a $p-1 \nmid k$ et $k \equiv k'(mod\ (p-1)p^N)$, alors on a $(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'}(mod\ p^{N+1})$.

Grâce à ce théorème, on voit que les valeurs $(1-p^{k-1})\frac{B_k}{k}$ s'interpolent p-adiquement en une "fonction zeta p-adique". Plus précisément, si on note $Z := \{k > 1 : p-1 \nmid k\} \subseteq \mathbb{Z}_p$, alors Z est un sous-ensemble dense de $\mathbb{Z}_p$, et la fonction $Z \to \mathbb{Z}_p$ donnée par $k \mapsto (1-p^{k-1})\frac{B_k}{k}$ est continue, à cause du théorème. Elle se prolonge donc à une fonction continue $\zeta_p : \mathbb{Z}_p \to \mathbb{Z}_p$, vérifiant :

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k).$$

En général, il existe aussi des congruences pour les valeurs spéciales des fonction L, et on peut construire les fonctions L p-adiques en les interpolant.

3 Fonctions L p-adiques

Dans cette partie, on va voir deux constructions de fonctions L p-adiques associées à certaines courbes elliptiques sur $\mathbb{Q}$. On note p un nombre premier (impair) fixé.

3.1 Construction de Mazur-Swinnerton-Dyer

L'idée de la construction de la fonction L p-adique de Mazur-Swinnerton-Dyer est d'interpoler les valeurs spéciales de la fonction L classique (complexe).

Soient E une courbe elliptique sur $\mathbb{Q}$ et f la forme modulaire lui associée par le théorème de modularité, avec $L(s) = \sum_n a_n/n^s$ la fonction L correspondante. Soit N le niveau de f. Si ψ est un caractère de Dirichlet, on note

$$L_\psi(s) := \sum_n \frac{a_n \psi(n)}{n^s}.$$

Un théorème de Drinfeld-Manin montre que les valeurs spéciales $L_\psi(1)$ sont prèsque "rationnels" - en effet, il existe deux nombres complexe non nul Ω^+ et Ω^- (les "périodes"), tels que les quotients $L_\psi(1)/\Omega^{\mathrm{sign}(\psi)}$ sont rationnels, où $\mathrm{sign}(\psi)$ est le sign du caractère ψ.

On suppose que p ne divise pas N (le cas "bonne réduction") ou que p divise N exactement (le cas "réduction multiplicative"). Une fonction L p-adique L_p est alors construite dans [8] Chapitre I, qui à chaque caractère p-adique continu χ de $\mathbb{Z}_p^*$ associe un nombre p-adique $L_p(\chi)$, et qui vérifie la condition d'interpolation : pour tout caractère de Dirichlet ψ, on a

$$L_p(\psi) = e_p(\psi) L_{\overline{\psi}}(1)/\Omega^{\mathrm{sign}(\psi)},$$

où $e_p(\psi)$ est un "facteur simple" dépendant de ψ.

Remarque À cause de ce "facteur simple", il existe un phénomène de "zéro exceptionnel" dans cette histoire de fonction L p-adique. Par exemple, quand e_p est nul, L_p est toujours nul, mais la fonction L classique peut ne pas

s'annuler. Dans l'article [8] les auteurs ont proposé des conjectures sur cette phénomène, mais on n'en discute pas ici.

Soit $\langle\cdot\rangle$ le caractère p-adique défini par $x \mapsto \lim_n x^{1-p^n}$, alors la fonction L p-adique à une variable, notée encore L_p, est définie par :

$$L_p(s) := L_p(\langle\cdot\rangle^s).$$

Cette fonction est localement analytique. Elle est l'analogue p-adique de la fonction L classique.

Dans [8], les auteurs ont aussi proposé quelques conjectures arithmétiques, en particulier l'analogue p-adique de la conjecture BSD :

Conjecture 3.1. *(BSD p-adique) Soient E une courbe elliptique sur $\mathbb{Q}$ de rang r et L_p la fonction L p-adique associée.*

1. Si L_p n'a pas de zéro exceptionnel (voir la remarque ci-dessus), alors on a $\mathrm{ord}_{s=1} L_p(s) = r$.

2. Si L_p a un zéro exceptionnel, alors on a $\mathrm{ord}_{s=1} L_p(s) = r + 1$.

3.2 Construction de Schneider

Dans [9], Schneider a proposé une autre construction de la fonction L p-adique associée à une courbe elliptique. La construction de Schneider se fait en 2 étapes :

1. Utiliser la correspondance de Jacquet-Langlands pour obtenir une "forme modulaire p-adique" associée à la courble elliptique E ;

2. Définir une fonction L p-adique pour chaque forme modulaire p-adique.

Plus précisément, soit $\mathbb{C}_p$ la clôture topologique de la clôture algébrique de $\mathbb{Q}_p$ (le corps des "nombres complexes p-adiques") et $\mathbb{H}_p := \mathbb{C}_p \backslash \mathbb{Q}_p$ le "demi-plan p-adique". Soit $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Q}_p)$ un sous-groupe discrèt, on définit une "forme modulaire p-adique de poids k et de niveau Γ" comme une fonction ϕ globalement analytique sur $\mathbb{H}_p$ vérifiant

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, f(\frac{az+b}{cz+d}) = (cz+d)^k f(z).$$

La correspondance de Jacquet-Langlands établit une correspondance entre les formes modulaires complexes de poids k et les formes modulaires p-adiques de poids k (pour un niveau Γ, qui est obtenu du groupe des unités d'un $\mathbb{Z}[1/p]$-ordre d'une algèbre de quaternion sur $\mathbb{Q}$), ainsi associer une forme modulaire p-adique de poids 2 à une courbe elliptique sur $\mathbb{Q}$.

Pour le deuxième étape, soit ϕ une forme modulaire p-adique de poids 2. En utilisant les cocycles harmoniques, Schneider a définit une distribution μ_ϕ sur $\mathbb{P}_1(\mathbb{Q}_p)$, qui est le bord de $\mathbb{H}_p$. Par restriction, μ_ϕ induit une distribution sur $\mathbb{Z}_p^*$. La fonction L p-adique est alors définie par

$$L_p(s) := \int_{\mathbb{Z}_p^*} \langle x \rangle^s d\mu_\phi$$

Remarque Le lien entre les deux fonctions L p-adiques (i.e. de Mazur-Swinnerton-Dyer et de Schneider) n'est pas encore clair.

3.3 Le cadre anticyclotomique

La méthode de Schneider n'est pas aussi satisfaisante que l'on espère. Motivés par les conjectures de [8], H. Darmon et M. Bertolini ([1]) ont commencé une étude parallèle dans le cas anticyclotomique. Ils ont trouvé des nouveaux phénomènes de zéros exceptionnels.

Une construction de fonction L p-adique dans ce cadre ([3]) est inspirée par l'idée de Schneider, mais il s'avère que cette théorie est plus satisfaisante que celle de Schneider. Les travaux sur ce sujet donnent aussi un aperçu de l'obstruction dans la situation originale de Schneider.

3.4 L'approche d'Emerton

Emerton ([5]) a expliqué le phénomène de zéro exceptionnel de [8] d'un point de vu de la théorie des représentations p-adiques. En regardant les complétés unitaires universels de certaines représentations p-adiques du groupe $\mathrm{GL}_2(\mathbb{Q}_p)$, on peut étendre une distribution sur les fonctions localement algébriques à une distribution sur les fonctions localement analytiques, qui est juste la distribution dans [8] pour définir la fonction L p-adique. On en déduit

alors (combinant avec une description de "l'invariant $\mathcal{L}$" dans [4]) formellement des formules pour la fonction L p-adique.

La théorie des représentations p-adiques a été bien développée pendant ces dernières années. Il est donc probable de suivre l'idée d'Emerton, de reformuler les travaux sur les fonctions L p-adiques et de généraliser les résultats.

Références

[1] M. Bertolini, H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. 126 (1996), 413-456.

[2] M. Bertolini, H. Darmon, *Hida families and rational points on elliptic curves*, Invent. Math. 168 (2007), no. 2, 371-431.

[3] M. Bertolini, H. Darmon, A. Iovita, M. Spiess, *Teitelbaum's exceptional zero conjecture in the anticyclotomic setting*, American Journal of Math. 124 (2002) 411-449.

[4] C. Breuil, *Série spéciale p-adique et cohomologie étale complété*, preprint (2003).

[5] M. Emerton, *p-adic L-functions and unitary completions of representations of p-adic reductive groups*, Duke Math. J. 130 (2005), no. 2, 353-392.

[6] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Second Edition, Springer-Verlag, 1984.

[7] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Second Edition, Springer-Verlag, 1984.

[8] B. Mazur, J. Tate, J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. 84 (1986), no. 1, 1-48.

[9] P. Schneider, *Rigid-analytic L-transforms*, Number Theory Noordwijkherhout 1983, 216-230, Lecture Notes in Math., 1068, Springer, Berlin-New York, 1984.

[10] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.