317

ASTÉRISQUE

2008

SÉMINAIRE BOURBAKI
VOLUME 2006/2007
EXPOSÉS 967-981

La conjecture de Sato-Tate

Henri CARAYOL

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Séminaire BOURBAKI Juin 2007
59e année, 2006-2007, n° 977, p. 345 à 391

LA CONJECTURE DE SATO-TATE
[d'après Clozel, Harris, Shepherd-Barron, Taylor]

par **Henri CARAYOL**

INTRODUCTION

0.1. — Soit $\mathscr{E}$ une courbe elliptique définie sur $\mathbb{Q}$. Pour p un nombre premier de bonne réduction, autrement dit lorsque p ne divise pas le conducteur N de la courbe, écrivons comme d'habitude $1+p-a_p$ le cardinal de $\mathscr{E}(\mathbb{F}_p)$. On sait depuis Hasse que a_p est de valeur absolue inférieure où égale à $2\sqrt{p}$, de sorte que l'on peut définir un angle θ_p par :

$$a_p = 2\sqrt{p}\cos\theta_p \ \ ; \ \theta_p \in [0,\pi].$$

Les valeurs propres de l'endomorphisme de Frobenius géométrique F_p (agissant sur la cohomologie ℓ-adique de notre courbe) sont alors $\sqrt{p}\,e^{i\theta_p}$ et $\sqrt{p}\,e^{-i\theta_p}$.

La conjecture de Sato-Tate, qui remonte à la première moitié des années 60, prédit comment doivent être répartis les θ_p dans l'intervalle $[0,\pi]$, dans le cas où $\mathscr{E}$ n'a pas de « multiplication complexe » : c'est-à-dire que $\mathscr{E}$ n'a pas d'autres endomorphismes sur $\mathbb{C}$ que ceux, évidents, qui constituent un anneau isomorphe à $\mathbb{Z}$.

Conjecture 0.1. — *On suppose $\mathscr{E}$ sans multiplication complexe. Alors les θ_p sont équirépartis sur $[0,\pi]$ relativement à la mesure $\mu = \frac{2}{\pi}\sin^2\theta\, d\theta$.*

Par définition, l'équirépartition prédite par cette conjecture consiste en la propriété suivante : notant $\mathscr{P}_n$ l'ensemble des nombres premiers $\leq n$ et non diviseurs de N, la moyenne $\frac{1}{\sharp\,\mathscr{P}_n}\sum_{p\in\mathscr{P}_n}\delta_{\theta_p}$ des mesures de Dirac aux points θ_p converge vaguement vers μ, autrement dit pour chaque fonction continue f sur $[0,\pi]$, on doit avoir :

$$\lim_{n\to+\infty}\ \frac{1}{\sharp\,\mathscr{P}_n}\sum_{p\in\mathscr{P}_n} f(\theta_p) \ = \ \mu(f)\ .$$

Lorsque $\mathscr{E}$ a de la multiplication complexe, ses endomorphismes constituent un ordre dans l'anneau des entiers d'un corps quadratique imaginaire. Il n'est pas difficile

alors de voir que les θ_p sont équirépartis relativement à la mesure $\frac{1}{2}\delta_{\frac{\pi}{2}} + \frac{1}{2\pi}\,d\theta$. Plus précisément, pour les p inertes, on a $a_p = 0$ et donc $\theta_p = \pi/2$, tandis que, pour les p décomposés, les valeurs propres de Frobenius sont égales (ou conjuguées) à celles données par un Grössencharakter du corps quadratique ; or on sait depuis Hecke que les angles associés sont équirépartis sur le cercle (pour la mesure habituelle).

On formule de façon évidente une généralisation de la conjecture au cas d'une courbe elliptique (sans multiplication complexe) définie sur un quelconque corps de nombres F : en chaque place finie (idéal premier) v de bonne réduction, notant q_v le cardinal du corps résiduel correspondant, on pose :

$$a_v = 1 + q_v - \sharp\,\mathcal{E}(\mathbb{F}_{q_v}) = 2\sqrt{q}_v \cos\theta_v \quad (\theta_v \in [0,\pi])$$

et l'on définit l'équirépartition des θ_v comme ci-dessus, en considérant la moyenne des δ_{θ_v} sur l'ensemble des v de norme $\leq n$.

L'objet de cet exposé est d'expliquer comment cette conjecture est maintenant démontrée sous certaines hypothèses additionnelles :

THÉORÈME 0.2. — *Soit $\mathcal{E}$ une courbe elliptique définie sur un corps totalement réel F. On suppose que $\mathcal{E}$ admet une réduction multiplicative en au moins une place finie. Alors les nombres θ_v sont équirépartis sur $[0,\pi]$ relativement à la mesure μ définie ci-dessus (dite « de Sato-Tate »).*

Remarque 0.3. — L'hypothèse que $\mathcal{E}$ admette quelque part une réduction multiplicative équivaut à dire que son invariant $j(\mathcal{E})$ n'est pas un entier de F, et elle entraîne que $\mathcal{E}$ ne possède pas de multiplication complexe. C'est une hypothèse qui pourra être levée le jour où l'on disposera de résultats suffisants sur la stabilisation de la formule des traces d'Arthur-Selberg, résultats qui semblent accessibles dans l'état d'avancement actuel de la théorie automorphe. Mentionnons également que Harris ([**14**]) a récemment prouvé, en admettant de telles avancées, des résultats conditionnels : en particulier un analogue de la conjecture de Sato-Tate pour le produit de deux courbes elliptiques (non isogènes).

0.2. — L'application de SU(2) dans $[0,\pi]$ qui, à une matrice unitaire u, associe $\arccos\left(\frac{1}{2}\mathrm{tr(u)}\right)$ est surjective $\left(\text{de section } \theta \to \begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix}\right)$ et elle identifie l'intervalle $[0,\pi]$ à l'ensemble des classes de conjugaison de SU(2). Il est facile de voir que la mesure de Sato-Tate n'est autre que l'image directe par cette application de la mesure de Haar normalisée de SU(2). Par suite la conjecture revient à prédire que les classes de conjugaison des $\begin{pmatrix} e^{i\theta_p} & \\ & e^{-i\theta_p} \end{pmatrix}$ sont équiréparties dans SU(2).

Dès la fin des années 60, Serre savait ramener cette conjecture à une question sur les fonctions L, ainsi qu'il l'a expliqué précisément dans son livre [**26**]. Noter que vers la même époque Tate avait également conscience de cette relation. Serre généralise

la méthode de Hadamard–de la Vallée Poussin afin d'énoncer un résultat qui couvre de nombreux cas connus ou conjecturaux d'équirépartition, et dont le prototype est l'équirépartition des nombres premiers dans les différentes classes de congruence de $(\mathbb{Z}/N\mathbb{Z})^*$:

Soient K un groupe compact, F un corps de nombres et supposons donnée, pour chaque place finie v (à l'exception d'un nombre fini) de F, une classe de conjugaison Θ_v dans K. Notant q_v le cardinal du corps résiduel correspondant, on forme, pour chaque représentation irréductible (unitaire) non triviale r de K, la fonction L suivante, qui converge pour $\Re s > 1$:

$$L^*(r,s) = \prod_v \det(1 - q_v^{-s} r(\Theta_v))^{-1}.$$

PROPOSITION 0.4 ([**26**]). — *On suppose que, pour chaque r irréductible non triviale, cette fonction se prolonge analytiquement à un ouvert contenant le demi-plan fermé $\Re s \geq 1$ et que le prolongement ne s'annule pas sur la droite $\Re s = 1$. Alors les classes de conjugaison Θ_v sont équiréparties dans K.*

Revenons au cas, qui nous intéresse ici, d'une courbe elliptique $\mathscr{E}/F$, et notons $\beta_v = e^{i\theta_v}$ et $\beta_v^{-1} = e^{-i\theta_v}$ les valeurs propres de Frobenius divisées par $\sqrt{q}_v$. Les représentations irréductibles non triviales de $\mathrm{SU}(2)$ sont les puissances symétriques $\mathrm{Sym}^{\mathrm{n}}\mathrm{r}_1$ ($n > 0$) de la représentation naturelle de dimension 2. La fonction L correspondante écrit alors

$$L^*(\mathrm{Sym}^{\mathrm{n}}\mathscr{E}, \mathrm{s}) = \prod_{\mathrm{v}} (1-\beta_{\mathrm{v}}^{-\mathrm{n}}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}(1-\beta_{\mathrm{v}}^{-\mathrm{n}+2}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}\cdots(1-\beta_{\mathrm{v}}^{\mathrm{n}-2}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}(1-\beta_{\mathrm{v}}^{\mathrm{n}}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}\,.$$

On prendra garde au fait qu'il s'agit d'une fonction L incomplète (manquent les facteurs aux mauvaises places et en l'infini) et qu'elle est normalisée de façon inhabituelle (à la manière automorphe, ce qui se traduit par un décalage de $n/2$ par rapport à la normalisation habituelle). Pour prouver la conjecture de Sato-Tate, il « suffit » donc de montrer que ces fonctions se prolongent analytiquement et n'ont pas de zéro sur la droite $\Re s = 1$.

0.3. — Du moins lorsque le corps de base est $\mathbb{Q}$, on sait depuis les travaux de Wiles et Taylor-Wiles, complétés par ceux de Diamond, Breuil, Conrad et Taylor (cf. [**10**]), que notre courbe elliptique est associée à une forme modulaire parabolique (ou, dans un langage un peu différent, à une représentation automorphe parabolique du groupe $\mathrm{GL}_2(\mathbb{A})$), pour laquelle on sait par ailleurs que la fonction L admet un prolongement qui ne s'annule pas sur $\Re s = 1$. Les conjectures générales de Langlands prédisent d'autre part que doit exister une « fonctorialité puissance symétrique », qui à une représentation automorphe de $\mathrm{GL}_2(\mathbb{A})$ en associe une autre, cette fois-ci du groupe $\mathrm{GL}_{n+1}(\mathbb{A})$. Or on sait que les fonctions L associées aux représentations

automorphes paraboliques du groupe linéaire GL_n ($n > 1$) vérifient les propriétés voulues de prolongement (holomorphe) et de non-annulation sur la droite $\Re s = 1$. Si on savait prouver l'existence de ces fonctorialités, a priori de nature « analytique », la conjecture en découlerait donc aussitôt. Malheureusement, on ne sait faire cela à l'heure actuelle que pour des petites valeurs de n (Shahidi). La stratégie utilisée par Clozel, Harris, Shepherd–Barron, Taylor met en jeu plus d'arithmétique. L'idée est en gros de généraliser aux groupes de dimension supérieure la méthode de Taylor-Wiles afin de prouver directement la « modularité » des puissances symétriques, c'est-à-dire le fait qu'elles correspondent à des représentations automorphes des groupes linéaires. Formulé ainsi, il s'agit encore d'un résultat inaccessible à l'heure actuelle, mais les auteurs en prouvent une version affaiblie dans laquelle on doit se restreindre au groupe de Galois absolu d'une extension assez grande F'/F (ce que Taylor nomme l'automorphie « potentielle ») et supposer n *impair*. Cette dernière restriction est d'ailleurs conditionnellement levée dans le récent article de Harris [**14**] mentionné plus haut, qui établit un résultat analogue pour n pair.

THÉORÈME 0.5. — *Soit $\mathcal{E}$ une courbe elliptique comme ci-dessus (admettant quelque part une réduction multiplicative) ; supposons n impair. Il existe alors une extension galoisienne totalement réelle F'/F sur laquelle $\mathrm{Sym}^n \mathcal{E}$ devient automorphe (parabolique) : cela signifie que la puissance symétrique n-ième de la représentation ℓ-adique associée à $\mathcal{E}$, restreinte au groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/F')$, a même fonction L (convenablement normalisée) qu'une représentation automorphe parabolique de $\mathrm{GL}_{n+1}(\mathbb{A}_{F'})$.*

Remarque 0.6. — À vrai dire, on a besoin d'une version légèrement plus forte de ce théorème qui assure que l'on peut choisir, lorsque n varie dans un ensemble fini $\mathcal{N}$ de nombres impairs, F' fixe ; utilisant les propriétés du changement de base construit par Arthur et Clozel [**1**], on peut contrôler la « descente » (idée due originellement à Harris) et voir aussi que l'automorphie est alors assurée pour toute extension intermédiaire $F \subset F'' \subset F'$ avec F'/F'' résoluble.

Le théorème (0.2) résulte alors de ce qui précède par des arguments assez simples qui seront expliqués au paragraphe suivant.

0.4. — Le principe de la méthode utilisée avec succès depuis les travaux fondateurs de Wiles pour établir la modularité (nous parlerons plutôt ici d'automorphie) d'une représentation ℓ–adique ρ consiste à partir de la modularité de sa réduction $\overline{\rho}$ et d'un résultat de « relèvement de la modularité » affirmant que tout relèvement convenable de $\overline{\rho}$ est encore modulaire. Ici « convenable » est une abréviation imprécise pour un ensemble d'hypothèses, dont certaines sont naturelles (en particulier la nature de ρ aux places divisant ℓ, qui doit être au minimum « potentiellement semi-stable », mais pour lesquelles on demande en général plus) et dont d'autres sont beaucoup