Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 347 (2009) 123–127
COMPTES RENDUS MATHEMATIQUE

Théorie des nombres

Répartition galoisienne d'une classe d'isogénie de courbes elliptiques

Rodolphe Richard [a,b]

[a] *ÉNS, 45, rue d'Ulm, 75230 Paris cedex 05, Paris, France*
[b] *IRMAR, bâtiment 22–23, université de Rennes 1, campus de Beaulieu, 35000 Rennes, France*

Reçu le 16 décembre 2007 ; accepté après révision le 26 novembre 2008

Disponible sur Internet le 5 février 2009

Présenté par Jean-Pierre Serre

Résumé

Nous montrons que dans les composantes géométriques des courbes modulaires associées aux sous-groupes de congruence de PSL(2), il y a équidistribution, vers la probabilité hyperbolique, des orbites sous Galois d'invariants modulaires formés à partir de structures de niveau sur des courbes elliptiques issues d'une même classe d'isogénie. ***Pour citer cet article : R. Richard, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Abstract

Hyperbolic Galois distribution of an isogeny class of elliptic curves. We show that, in geometrically connected modular curves associated with congruence subgroups of PSL(2), one has equidistribution, towards the hyperbolic probability, of Galois orbits of the modular invariants associated with a level structure on elliptic curves within a given isogeny class. ***To cite this article: R. Richard, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Abridged English version

We write $Y(1)(\mathbf{C})$ for the space of complex points of the modular curve of level 1. It is the usual j-line and, as such, is naturally defined over $\mathbf{Q}$. Consequently, $Y(1)(\mathbf{C})$ carries an action of $\mathrm{Aut}(\mathbf{C}/\mathbf{Q})$, namely the action on j-invariants as complex numbers. For any algebraic j-invariant one construct an atomic probability measure $\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j}$ on $Y(1)(\mathbf{C})$, adding a Dirac mass at each conjugate of j, and dividing by $\deg(\mathbf{Q}(j))$. In general, $\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j}$ has no particular property. But for families of algebraic numbers whose Weil height goes to 0, Bilu's theorem assert that $\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j}$ tends to the Haar measure on the unit circle.

Our main result here is an analogous property for families of invariants that come from elliptic curves within a single isogeny class. In this case, one knows from results of [9] that the height of involved invariants is unbounded.

Adresse e-mail : Rodolphe.Richard@Normalesup.org.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.12.008

Theorem 1. *Let E be a complex elliptic curve without complex multiplication. Let $(j_n)_{n\in\mathbf{N}}$ be a sequence of pairwise distinct algebraic j-invariants. We suppose that for every index n, there exists a complex elliptic curve whose j-invariant equals j_n and which is isogeneous to E.*

Then the sequence $(\delta_{\mathrm{Aut}(\mathbf{C}/\mathbf{Q})\cdot j})_{n\in\mathbf{N}}$ is convergent and its limit is the hyperbolic probability measure μ. Equivalently, for any bounded and continuous real valued function $f : Y(N)(\mathbf{C}) \to \mathbf{R}$,

$$\frac{1}{[\mathbf{Q}(j_n):\mathbf{Q}]} \sum_{z\in \mathcal{Gal}(\mathbf{Q}(j_n)/\mathbf{Q})\cdot j} f(z) \to \mu(f) := \int\limits_{Y(N)(\mathbf{C})} f \,\mathrm{d}\mu$$

as $n \to +\infty$.

In this statement "*hyperbolic probability measure*" means the probability measure deduced from the Poincaré measure by uniformization.

Actually, the result we get is more general, encompassing congruence subgroups of PSL(2), and any ground field of finite type over $\mathbf{Q}$. The hypothesis on complex multiplication is unnecessary, thanks to [2]. The following is immediate from the theorem and its application to the (unbounded but positive) function $f : z \mapsto \max\{0; \log|z|\}$.

Corollary 2. *For such a sequence $(j_n)_{n\in\mathbf{N}}$, the degree of $\mathbf{Q}(j(n))$ goes to ∞, and the Archimedean part of the Weil height of j_n goes to $+\infty$ as $n \to \infty$.*

Note that it is the *boundedness* of the local height that prevails at finite places.

This main ingredients of the proof are:

1. Serre's open image theorem from [5] and [6];
2. equidistribution of Hecke orbits for real homogeneous spaces;
3. an adelic variant of 2, which is deduced using finiteness of class numbers for arithmetic groups;
4. the above corollary on the degree of $\mathbf{Q}(j_n)$, which is deduced from 1 and finiteness statements from 3.

The author recently remarked that the proof applies to quaternionic Fuchsian groups, replacing Serre's theorem by its extension by Ohta in [4].

1. Énoncé

Soit N un entier naturel non nul. Fixons le choix, dans $\mathbf{C}$, d'une racine de l'unité, disons $\zeta := \exp(2\pi i/N)$. On considère la courbe modulaire $Y(N)$. C'est une courbe algébrique *affine* et *géométriquement connexe* définie sur $\mathbf{Q}(\zeta)$. L'espace $Y(N)(\mathbf{C})$ de ses points complexes s'identifie au quotient du demi-plan de Poincaré $\mathfrak{H} := \{\tau \in \mathbf{C} \mid \Im(\tau) > 0\}$ par l'action à gauche du groupe $\Gamma(N)$. La mesure de Poincaré sur $\mathfrak{H}$ détermine une mesure de probabilité μ, que l'on qualifiera d'*hyperbolique*, sur $Y(N)(\mathbf{C})$.

Le schéma $Y(N)$ est l'espace de modules (fin pour $N \geqslant 3$, grossier pour $N = 1$ ou 2) des courbes elliptiques munies d'une *structure complète de niveau N de racine associée ζ*, c'est-à-dire de deux points rationnels de N-torsion P et Q dont l'accouplement de Weil $e(P, Q)$ (normalisé comme en [8] III.§8) vaut ζ.

Soit E une courbe elliptique complexe. Considérons une suite $(E_n)_{n\in\mathbf{N}}$ de courbes elliptiques complexes toutes isogènes à E. On choisit, pour chaque n, une structure complète de niveau N et de racine ζ sur E_n, que l'on notera β_n. À chaque couple (E_n, β_n) correspond un point de $Y(N)(\mathbf{C})$. Notons-le z_n.

Soit L un corps de type fini sur $\mathbf{Q}$ sur lequel E admet un modèle. Alors, pour chaque n, l'orbite de z_n sous $\mathrm{Aut}(\mathbf{C}/L)$ est finie. On notera $\delta_L(z_n)$ la probabilité sur $Y(N)(\mathbf{C})$ supportée par cette orbite et affectant du même poids chacun des conjugués de z_n. Notre résultat décrit le comportement asymptotique de $\delta_L(z_n)$.

Théorème 1. *On suppose E sans multiplication complexe. Supposons aussi que l'on ne puisse pas extraire de $(z_n)_{n\in\mathbf{N}}$ une suite constante.*

Alors la probabilité $\delta_L(z_n)$ converge vers la probabilité hyperbolique μ lorsque n tend vers $+\infty$.

Autrement dit, pour toute fonction continue bornée $f : Y(N)(\mathbf{C}) \to \mathbf{R}$,

$$\delta_L(z_n)(f) := \frac{1}{\#\operatorname{Aut}(\mathbf{C}/L)\cdot z_n} \sum_{z\in \operatorname{Aut}(\mathbf{C}/L)\cdot z_n} f(z) \to \mu(f) := \int\limits_{Y(N)(\mathbf{C})} f\,\mathrm{d}\mu$$

lorsque $n \to +\infty$.

Ce résultat ne rentre pas *a priori* dans le cadre de l'équidistribution des points de petite hauteur. En effet la hauteur de Faltings d'une suite de courbes elliptiques dans une même classe d'isogénie n'est en général pas bornée [9]. L'énoncé analogue, dans le cas où E admet de la multiplication complexe, est lui aussi valide ; dans ce cas, l'hypothèse que les courbes soient isogènes est superflue, d'après un théorème de William Duke [2].

Notre méthode combine une forme adélique l'*équidistribution des points de Hecke* et les propriétés d'*image ouverte* d'un groupe de Galois agissant sur la torsion de courbes elliptiques.

2. Classe d'isogénie, action galoisienne et uniformisation

Pour toute courbe elliptique complexe E, on notera $\hat{T}(E)$ son module de Tate profini, et $\hat{V}(E)$ son module de Tate adélique. Ce sont des modules libres de rang 2 sur $\hat{\mathbf{Z}}$ et $\mathbf{A}_f$ respectivement, et ils dépendent fonctoriellement de E. On notera K_N le sous-groupe principal de congruence modulo N de $\mathrm{GL}(2,\hat{\mathbf{Z}})$, et on notera $\operatorname{Aut}(E\otimes\mathbf{Q})$ le groupe des inversibles de l'algèbre $\operatorname{End}(E/\mathbf{C})\otimes\mathbf{Q}$.

Soit E une courbe elliptique complexe et soit $\varphi : {\mathbf{A}_f}^2 \to \hat{V}(E)$ un isomorphisme $\mathbf{A}_f$-linéaire. Il existe un entier n_φ, une courbe elliptique complexe E_φ, et une isogénie $\pi_\varphi : E_\varphi \to E$ tels que les images de $\hat{T}(\pi_\varphi) : \hat{T}(E_\varphi) \to \hat{T}(E)$ et de $n_\varphi\cdot\varphi$ coïncident dans $\hat{T}(E)$. Il s'ensuit que la correspondance

$$\gamma_\varphi : \hat{\mathbf{Z}}^2 \xrightarrow{n_\varphi\cdot\varphi} \hat{T}(E) \xleftarrow{\hat{T}(\pi_\varphi)} \hat{T}(E_\varphi)$$

est un isomorphisme de $\hat{\mathbf{Z}}^2$ sur $\hat{T}(E_\varphi)$. Cela définit, par passage au quotient, une structure de niveau N sur E_φ, disons

$$\beta_\phi : \big(\mathbf{Z}/(N)\big)^2 \to E_\varphi[N].$$

La classe d'isomorphisme de $(E_\varphi,\beta_\varphi)$ ne dépend que de φ. On notera ζ_φ la racine de l'unité associée à β_φ, et lorsque $\zeta_\varphi = \zeta$, on notera z_φ le point de $Y(N)(\mathbf{C})$ qui représente $(E_\varphi,\beta_\varphi)$.

Soit $\operatorname{Isom}_\zeta({\mathbf{A}_f}^2,\hat{V}(E))$ l'ensemble des isomorphismes $\mathbf{A}_f$-linéaires φ de ${\mathbf{A}_f}^2$ sur $\hat{V}(E)$ tels que $\zeta_\varphi = \zeta$. Soit aussi $\operatorname{Isog}_\zeta(E)$ le sous-ensemble de $Y(N)(\mathbf{C})$ des invariants modulaires provenant de courbes isogènes à E (munies de structures de racine ζ). Alors l'application $\varphi \mapsto z_\varphi$ de $\operatorname{Isom}_\zeta({\mathbf{A}_f}^2,\hat{V}(E))$ vers $Y(N)(\mathbf{C})$ est bien définie et son image est $\operatorname{Isog}_\zeta(E)$. Cette application est en outre invariante à gauche sous $\operatorname{Aut}(E\otimes\mathbf{Q})$, à droite sous K_N et elle induit une bijection

$$\operatorname{Aut}(E\otimes\mathbf{Q})\backslash \operatorname{Isom}_\zeta\big({\mathbf{A}_f}^2,\hat{V}(E)\big)\big/K_N \to \operatorname{Isog}_\zeta(E).$$

Fixons un modèle de E sur un sous-corps de $\mathbf{C}$ contenant $\mathbf{Q}(\zeta)$. On en déduit une représentation de $\operatorname{Aut}(\mathbf{C}/L)$ sur $\hat{T}(E)$, puis, par composition, une action à gauche sur $\operatorname{Isom}_\zeta({\mathbf{A}_f}^2,\hat{V}(E))$. Cette action est compatible, via la flèche $\varphi\mapsto z_\varphi$ à l'action à gauche de $\operatorname{Aut}(\mathbf{C}/L)$ sur les $\mathbf{C}$-points de $Y(N)$.

Enfin cette application est « compatible à l'uniformisation » de $Y(N)(\mathbf{C})$, au sens où elle s'inscrit dans un carré commutatif

$$\begin{array}{ccc}
\operatorname{Isom}_\zeta\big({\mathbf{A}_f}^2,\hat{V}(E)\big) & \longrightarrow & \operatorname{PGL}(2,\mathbf{Q})\backslash\operatorname{PGL}(2,\mathbf{A}) \\
\downarrow & & \downarrow \\
\operatorname{Aut}(E\otimes\mathbf{Q})\backslash\operatorname{Isom}_\zeta\big({\mathbf{A}_f}^2,\hat{V}(E)\big)\big/K_N & \longrightarrow & Y(N)(\mathbf{C}).
\end{array}$$

Dans ce diagramme, la flèche supérieure est équivariante *à droite* sous le stabilisateur de $\operatorname{Isom}_\zeta({\mathbf{A}_f}^2,\hat{V}(E))$ dans $\mathrm{GL}(2,\mathbf{A}_f)$. Il est formé des g pour lesquels $\mathbf{dét}(g)\in\mathbf{Q}^\times\cdot(N\hat{\mathbf{Z}})^\times$. La flèche de droite est un quotient par un sous-groupe compact maximal de $\mathrm{PGL}(2,\mathbf{A})$, de la forme $K'\times\mathrm{PSO}(2,\mathbf{R})$. On choisira pour K' le sous-groupe de $\mathrm{PGL}(2,\hat{\mathbf{Z}})$ engendré par le sous-groupe principal de congruence modulo N *et par le tore diagonal*. Dès que $N\geqslant 3$, ce groupe K' contient *strictement* l'image de K_N dans $\mathrm{PGL}(2,\hat{\mathbf{Z}})$.

3. Démonstration du théorème, image ouverte

On se place dans la situation de l'introduction et sous les hypothèses du théorème. Pour chaque n, on choisit un isomorphisme $\varphi_n \in \mathrm{Isom}_\zeta(\mathbf{A}_f{}^2, \hat{V}(E))$ tel que $z_{\varphi_n} = z_n$. On déduit de ce qui précède que l'orbite $\mathrm{Aut}(\mathbf{C}/L)\cdot z_n$ dans $Y(N)(\mathbf{C})$ est l'image de $\mathrm{Aut}(\mathbf{C}/L)\cdot\varphi_n$. Soit $\mathrm{PGL}(2,\mathbf{Q})\cdot g_n$ l'image de φ_n dans $\mathrm{PGL}(2,\mathbf{Q})\backslash\mathrm{PGL}(2,\mathbf{A})$. D'après la commutativité du diagramme ci-dessus, $\mathrm{Aut}(\mathbf{C}/L)\cdot z_n$ est l'image dans $Y(N)(\mathbf{C})$ d'un ensemble de la forme $\mathrm{PGL}(2,\mathbf{Q})\cdot K\cdot g_n$ où K est un sous-groupe de $\mathrm{PGL}(2,\hat{\mathbf{Z}})$ déterminé par l'action de $\mathrm{Aut}(\mathbf{C}/L)$ sur $\hat{T}(E)$.

Après avoir déduit du fait suivant que K est ouvert, on montre la propriété d'équidistribution annoncée en appliquant la Proposition 2 pour $G = \mathrm{PGL}(2)$.

Proposition 1. *Soit E une courbe elliptique sans multiplication complexe géométrique définie sur un corps L de type fini sur $\mathbf{Q}$ et contenu dans $\mathbf{C}$. Considérons la représentation ρ de $\mathrm{Aut}(\mathbf{C}/L)$ sur $\hat{T}(E)$.*

Alors l'image de ρ est un sous-groupe d'indice fini du groupe, isomorphe à $\mathrm{GL}(2,\hat{\mathbf{Z}})$, des automorphismes continus du groupe abélien profini $\hat{T}(E)$.

Cela se déduit du théorème de l'image ouverte de Serre ([5] et [6]) dans le cas où $j(E)$ est algébrique sur $\mathbf{Q}$, et des travaux de Shimura dans le cas où $j(E)$ est transcendant [7].

4. Équidistribution adélique et points de Hecke

Soit G un groupe algébrique sur $\mathbf{Q}$. On désigne par $G(\mathbf{R})^+$ la composante neutre du groupe de Lie réel associé, et on identifie $G(\mathbf{Q})$ à son image dans $G(\mathbf{A})$ par le plongement diagonal. Soit $G(\mathbf{Q})^+$ l'image inverse de $G(\mathbf{R})^+$ par le morphisme $G(\mathbf{Q})\to G(\mathbf{R})$ et soit $\iota_f(\mathbf{Q})$ l'image de $\mathbf{Q}$ dans l'anneau $\mathbf{A}_f$. Alors $G(\iota_f(\mathbf{Q}))^+$ désignera l'image de $G(\mathbf{Q})^+$ dans $G(\mathbf{A}_f)$ et $\overline{G(\iota_f(\mathbf{Q}))^+}$ son adhérence dans $G(\mathbf{A}_f)$. Le résultat suivant utilise la propriété d'équidistribution des points de Hecke (voir [1] ou [3]).

Proposition 2. *Soit G un groupe algébrique linéaire $\mathbf{Q}$-simple connexe de type non compact. Soient K et K' deux sous-groupes compacts et ouverts de $G(\mathbf{A}_f)$. On désigne par μ la probabilité $G(\mathbf{R})^+$-invariante sur le $G(\mathbf{R})^+$-espace homogène à droite connexe $\mathbf{X} := G(\mathbf{Q})\backslash G(\mathbf{Q})\cdot G(\mathbf{R})^+\cdot K'/K'$.*

Soit $(g_n)_{n\in\mathbf{N}}$ une suite de $\overline{G(\iota_f(\mathbf{Q}))^+}$ sans valeur d'adhérence dans $G(\mathbf{A}_f)$. Considérons les sous-ensembles de $G(\mathbf{A}_f)$ suivants.

$$E_n = (K\cdot g_n)\cap\Big(\overline{G\big(\iota_f(\mathbf{Q})\big)^+}\cdot K'\Big).$$

Alors, pour toute fonction continue et bornée $f:\mathbf{X}\to\mathbf{R}$,

$$\frac{\sum_{x\in G(\mathbf{Q})\backslash G(\mathbf{Q})\cdot E_n\cdot K'/K'} f(x)}{\#G(\mathbf{Q})\backslash G(\mathbf{Q})\cdot E_n\cdot K'/K'} \text{ tend vers } \int_{\mathbf{X}} f\,\mathrm{d}\mu \text{ lorsque } n\to+\infty.$$

5. Dernières remarques

1. L'énoncé de [3] utilise comme hypothèse que les orbites considérées doivent avoir un cardinal (le « degré » des points considérés) de plus en plus grand. Pour des réseaux arithmétiques, cette hypothèse est automatiquement vérifiée. Ce sont des propriétés de finitude que nous déduisons des résultats généraux d'A. Borel sur l'arithmétique des groupes semi-simples de type non-compact. Dans le cas qui nous intéresse, celui des courbes modulaires $Y(N)(\mathbf{C})$, cela se traduit, par l'énoncé suivant. On notera que cet énoncé, qui n'est pas sans rappeler le théorème de Shafarevich [5], est un corollaire du Théorème 1.

Proposition 3. *Soit E une courbe elliptique définie sur un corps L de type fini et contenu dans $\mathbf{C}$. Alors il n'existe, à $\mathbf{C}$-isomorphisme près qu'un nombre fini de courbes elliptiques complexes définissables sur L et $\mathbf{C}$-isogènes à E.*

2. Nous avons restreint l'énoncé du théorème aux courbes modulaires $Y(N)$. Mais notre résultat s'étend tel quel aux courbes modulaires géométriquement connexes associées aux sous-groupes de congruence de $\Gamma(1)$, vu que ces

dernières sont recouvertes par les courbes $Y(N)$. On peut également adapter l'énoncé au cas non connexe. Les mesures limites seront alors les moyennes arithmétiques de probabilités associées aux composantes géométriquement connexes issues d'une même composante connexe.

3. Plus récement, l'auteur a remarqué que ce résultat s'étend aux courbes de Shimura associées à des algèbres de quaternions non déployées. Les courbes elliptiques sont alors remplacées par des surfaces abéliennes à multiplication quaternionique, auxquelles M. Ohta [4] a étendu la Proposition 1.

Références

[1] L. Clozel, H. Oh, E. Ullmo, Hecke operators and equidistribution of Hecke points, Invent. Math. 144 (2001) 327–351.
[2] W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, Invent. Math. 92 (1988).
[3] A. Eskin, H. Oh, Ergodic theoretic proof of equidistribution of Hecke points, Ergodic Theory Dynam. Systems 26 (1) (2006) 163–167.
[4] M. Ohta, On ℓ-adic representations of Galois groups obtained from certain two-dimensional abelian varieties, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 21 (1974).
[5] J.-P. Serre, Abelian ℓ-Adic Representations and Elliptic Curves, W.A. Benjamin, Inc., 1968.
[6] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 258–331.
[7] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Kanô Memorial Lectures, no. 1 Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, 1971.
[8] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106, Springer, 1986.
[9] L. Szpiro, E. Ullmo, Variation de la hauteur de Faltings dans une classe de $\overline{\mathbb{Q}}$-isogénie de courbe elliptique, Duke Math. J. 97 (1) (1999) 81–97.