Séminaire Delange-Pisot-Poitou. Théorie des nombres

Marc Yor

Distributions de Frobénius

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 17, n° 2 (1975-1976), exp. n° G20, p. G1-G10

<http://www.numdam.org/item?id=SDPP_1975-1976__17_2_A22_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théorie des nombres)
17e année, 1975/76, n° G20, 10 p.

24 mai 1976

DISTRIBUTIONS DE FROBÉNIUS

par Marc YOR

(d'après S. LANG et H. TROTTER [1])

On expose ci-dessous la méthode utilisée par LANG et TROTTER dans leur livre : Frobenius distributions in GL_2-extensions [1] pour poser la première des deux conjectures qui font l'objet de ce livre. La méthode est "probabiliste" : elle consiste à considérer les traces de Frobénius t_p comme une famille de variables aléatoires, indexées par l'ensemble des nombres premiers, à valeurs dans $\underset{\sim}{Z}$, et indépendantes pour une certaine probabilité compatible avec les distributions de TCHEBOTAREV [ČEBOTAREV], SATO-TATE et HECKE ; une version de la loi forte des grands nombres permet ensuite de poser la conjecture.

0. Rappel sur les courbes elliptiques sur $\underset{\sim}{Q}$.

Si A est une courbe elliptique sur $\underset{\sim}{Q}$, donnée par exemple par l'équation homogène $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, elle est munie naturellement d'une structure de groupe, admettant $0 = (0, 1, 0)$ pour élément neutre.

Si $n \in \underset{\sim}{N}$, l'ensemble $A_n = \{x \in A ; nx = 0\}$ est un $\underset{\sim}{Z}/n\underset{\sim}{Z}$-module libre de rang 2, et on a

$$\mathrm{Aut}(A_n) \simeq GL_2(\underset{\sim}{Z}/n\underset{\sim}{Z}) .$$

Si ℓ est un nombre premier ($\ell \in P$), on note $A_{\ell^\infty} = \bigcup_{n \in \underset{\sim}{N}} A_{\ell^n}$, et on a

$$\mathrm{Aut}(A_{\ell^\infty}) \simeq GL_2(\underset{\sim}{Z}_\ell) .$$

Soit $A_\infty = \bigcup_{n \in \underset{\sim}{N}} A_n$ le sous-groupe de torsion de A. C'est un $\underset{\sim}{Z}$-module de torsion, dont la décomposition en ses composantes primaires s'écrit

$$A_\infty = \bigoplus_{\ell \in P} A_{\ell^\infty} .$$

On a donc

$$\mathrm{Aut}(A_\infty) = \prod_{\ell \in P} \mathrm{Aut}(A_{\ell^\infty}) \simeq \prod_{\ell \in P} GL_2(\underset{\sim}{Z}_\ell) .$$

Enfin, si $K = \underset{\sim}{Q}(A_\infty)$, et $G = \mathrm{Gal}(K/\underset{\sim}{Q})$, il existe un homomorphisme naturel :

$$\rho : G \to \mathrm{Aut}(A_\infty) \simeq \prod_{\ell \in P} GL_2(\underset{\sim}{Z}_\ell) .$$

1. Cadre axiomatique.

Après ce rappel, il est naturel de se placer d'emblée dans la situation suivante :

soit K extension galoisienne de degre infini de $\underset{\sim}{Q}$, et $G = \mathrm{Gal}(K/\underset{\sim}{Q})$. On suppose fixée $\rho : G \to \prod_{\ell \in P} GL_2(\underset{\sim}{Z}_\ell)$, représentation continue, G étant muni de la topologie de Krull, et $\prod_{\ell \in P} GL_2(\underset{\sim}{Z}_\ell)$ de la topologie produit (naturelle).

On considère le schéma suivant (M appartient à $\underset{\sim}{N}$) :

$$G \xrightarrow{\rho} \prod_{\ell \in P} GL_2(\underset{\sim}{Z}_\ell) \xrightarrow{p_M} \prod_{\ell \mid M} GL_2(\underset{\sim}{Z}_\ell) \xrightarrow{r_M} GL_2(\underset{\sim}{Z}/M\underset{\sim}{Z}) \ ,$$

$$G \xrightarrow{\rho_M} \rho(M) \xrightarrow{\quad} GL_2(\underset{\sim}{Z}/M\underset{\sim}{Z}) \ ,$$

où p_M est la projection canonique, et r_M la réduction modulo M.

Les images respectives de G par les différentes applications sont :

$$G \to \rho(G) \to G_M \to G(M) \ .$$

On a évidemment $G_M \simeq G/\mathrm{Ker}\ \rho_M$ et $G(M) \simeq G/\mathrm{Ker}\ \rho_{(M)}$. ρ étant continue, $\mathrm{Ker}\ \rho_M$ et $\mathrm{Ker}\ \rho_{(M)}$ sont fermés dans G, et donc si K_M (resp. : $K(M)$) est le corps des invariants de $\mathrm{Ker}\ \rho_M$ (resp. : $\mathrm{Ker}\ \rho_{(M)}$), ce corps est galoisien sur $\underset{\sim}{Q}$, et on a :

$$G_M \simeq \mathrm{Gal}(K_M/\underset{\sim}{Q}) \ , \quad \text{resp. :} \quad G(M) \simeq \mathrm{Gal}(K(M)/\underset{\sim}{Q}) \ .$$

On introduit maintenant les définitions suivantes, qui seront particulièrement importantes :

<u>Définition 1.</u> - Soit $M \in \underset{\sim}{N}$. On dit que :

M <u>décompose</u> ρ si $\rho(G) \simeq \prod_{\ell \nmid M} GL_2(\underset{\sim}{Z}_\ell) \times G_M$;

M <u>stabilise</u> ρ si $G_M = r_M^{-1}(G(M))$.

D'après SERRE [5], si A est une courbe elliptique sur $\underset{\sim}{Q}$ sans multiplication complexe, alors il existe un entier $M \in \underset{\sim}{N}$ qui décompose et stabilise la représentation ρ (définie dans le § 0).

L'existence d'un tel entier M permet d'étudier $\rho(G)$, ce qui fait son importance dans l'étude des conjectures de LANG et TROTTER.

Toutes les hypothèses que l'on fait dorénavant seront vérifiées pour les courbes elliptiques sur $\underset{\sim}{Q}$, sans multiplication complexe.

On suppose toujours par la suite que ρ <u>est elliptique</u>, c'est-à-dire :

1° Il existe un entier positif Δ tel que, si p est premier, et $p \nmid \Delta\ell$, p ne se ramifie pas dans K (remarquons que, pour de tels p, la classe de Frobénius σ_p est bien définie (à une conjugaison près) dans G_ℓ).

2° Pour de tels p, $\rho_\ell(\sigma_p)$ a pour polynôme caractéristique

$$\Phi_p(X) = X^2 - t_p X + p$$

(on appelle t_p la trace de Frobénius).

3° t_p est un entier indépendant de ℓ, et les racines de Φ_p sont conjuguées

l'une de l'autre.
(On note Π_p une de ces racines.)

2. Enoncé des conjectures.

On les note C1 et C2. Bien que l'étude qui mène à C2 soit beaucoup plus compliquée que celle qui mène à C1, l'idée de base est la même (cf. l'introduction et la partie 3), et on ne s'intéressera par la suite qu'à C1.

C1 : Soit $t_0 \in Z$. On note

$$N_{t_0,\rho}(x) = \#\{p \in P ; \ p \leq x , \ t_p = t_0\} .$$

On conjecture qu'il existe une constante $C(t_0 , \rho)$, $0 \leq C(t_0 , \rho) < \infty$, telle que :

$$N_{t_0,\rho}(x) \sim C(t_0 , \rho) \sqrt{x}/\log x$$

(si $C(t_0 , \rho) = 0$, ceci signifie que $N_{t_0,\rho}(x)$ est borné uniformément en x).

Rappelons que si l'on note

$$\Pi_{1/2}(x) = \sum_{p\in P, p\leq x} 1/2\sqrt{p} ,$$

on a

$$\Pi_{1/2}(x) \sim \sqrt{x}/\log x .$$

On peut donc poser la conjecture sous la forme :

$$N_{t_0,\rho}(x) \sim C(t_0 , \rho) \ \Pi_{1/2}(x)$$

forme qui se présente plus naturellement dans les calculs théoriques (voir la suite) ou numériques.

C2 : Soit k un corps imaginaire quadratique. On note

$$N_{k,\rho}(x) = \#\{p \in P ; \ p \leq x ; \ Q(\Pi_p) = k\} .$$

On conjecture qu'il existe une constante $C(k , \rho)$, $0 < C(k , \rho) < \infty$ telle que

$$N_{k,\rho}(x) \sim C(k , \rho) \sqrt{x}/\log x \sim C(k , \rho) \ \Pi_{1/2}(x) .$$

Tout en posant ces conjectures, les auteurs obtiennent des expressions explicites des constantes $C(t_0 , \rho)$ et $C(k , \rho)$.

Remarques.

1° Il existe d'autres résultats ou conjectures sur les courbes ou fonctions elliptiques (voir les références en [1]) dont la formulation est voisine de C1 ou C2. En particulier, dans le cas où A admet des multiplications complexes, une conjecture de HARDY-LITTLEWOOD suppose que

$$N_{1,\rho}(x) \sim C \sqrt{x}/\log x$$

(mais, la situation n'est pas du tout comparable).

2° Les entiers p tels que $t_p = 0$ (p est dit supersingulier), ou $t_p = 1$ (p est dit anormal) jouent un rôle important dans l'arithmétique des courbes elliptiques (cf. [3], propositions 8.5 et 8.14).

3° On connaît, indépendamment du travail de LANG et TROTTER des formules théoriques explicites pour les traces de Frobénius t_p des courbes elliptiques sans multiplication complexe. Ces formules sont précieuses pour calculer effectivement les traces de Frobénius t_p, pour p "petit" nombre premier, ce qui permet souvent de déterminer un entier M qui décompose et stabilise ρ.

Signalons en particulier la formule $t_p = 1 + p - N_p$, où N_p est le nombre de points rationnels de la courbe sur $\underset{\sim}{F}_p$. De cette formule, on déduit (pour g_2 et g_3 entiers)

$$t_p = - \sum_{i=1}^{p} \left(\frac{4i^3 - g_2 i - g_3}{p}\right),$$

où $\left(\frac{a}{p}\right)$ est le symbole de Legendre.

D'autre part, en [2], LIGOZAT a explicité, pour une courbe modulaire elliptique, la fonction L associée : t_p est alors le coefficient de q^p dans le développement en série de L.

3. Modèle probabiliste et résultats principaux.

3.1 : Le résultat de calcul des probabilités qui sera utile par la suite est une version améliorée de la loi forte des grands nombres, version due à KOLMOGOROV. LANG et TROTTER en donnent une démonstration dans leur livre. On trouvera par ailleurs ce résultat et de nombreuses conséquences en [4] (IV, 6 et IV, 7).

THÉORÈME 1. - *Soit* $(\Omega, \mathfrak{F}, P)$ *espace de probabilité, et* $Y_n : (\Omega, \mathfrak{F}) \to \underset{\sim}{R}$ *une suite de variables aléatoires P-indépendantes, centrées. Alors, si* (μ_n) *est une suite de nombres positifs croissant vers* $+\infty$, *la convergence de la série* $\sum_{n \geqslant 1} \frac{1}{\mu_n^2} E[Y_n^2]$ *entraîne*

$$\lim_{n \to \infty} \frac{1}{\mu_n} \sum_{m=1}^{n} Y_m = 0 \quad P \text{ presque sûrement (p. s.)}.$$

On prend maintenant pour espace de probabilité un produit infini de tels espaces $\prod_{n \in \underset{\sim}{N}} (\Omega_n, \mathfrak{F}_n, \mu_n)$. On note $\omega = (\omega_n, n \in \underset{\sim}{N})$ l'élément générique de $\Omega = \prod_n \Omega_n$, et $\mu = \bigotimes_n \mu_n$.

COROLLAIRE 1. - *Soient* $S_n \in \mathfrak{F}_n$ *tels que* $\mu_n(S_n) \xrightarrow[(n \to \infty)]{} \ell$. *Alors*,

$$d\mu(\omega) \text{ p. s.}, \quad \frac{1}{n} \sum_{m=1}^{n} 1_{S_m}(\omega_m) \xrightarrow[(n \to \infty)]{} \ell.$$

Démonstration. - On applique le théorème 1 à

$$Y_m(\omega) = 1_{S_m}(\omega_m) - \mu_m(S_m) \quad \text{et} \quad u_m = m ,$$

puis on utilise le lemme de Césaro.

COROLLAIRE 2. - Soient $S_n \in \mathfrak{S}_n$, tels que $\sum_n \frac{1}{u_n^2} \mu_n(S_n) < \infty$. Alors,

$$d\mu(\omega) \text{ p. s.}, \qquad \#\{n \leq N ; \omega_n \in S_n\} = \sum_{n=1}^{N} \mu_n(S_n) + o(u_N) .$$

Démonstration. - Prendre $Y_n(\omega) = 1_{S_n}(\omega_n) - \mu_n(S_n)$.

COROLLAIRE 3. - Soit p_n le n-ième nombre premier. On suppose qu'il existe $C > 0$, tel que $\mu_n(S_n) \sim C \frac{1}{2\sqrt{p_n}}$. Alors,

$$d\mu(\omega) \text{ p. s.}, \qquad \#\{n \leq N , \omega_n \in S_n\} \sim C \sum_{n \leq N} \frac{1}{2\sqrt{p_n}}$$

Démonstration. - Appliquer le corollaire 2 avec $u_n = \sum_{m \leq n} \frac{1}{2\sqrt{p_n}}$

3.2. Modèle probabiliste. - On se place sur l'espace $\Omega = \underset{\sim}{Z}^P$, muni de sa tribu produit (naturelle) $\mathfrak{A}$; si $p \in P$, on note $Y_p(\omega) = \omega(p)$. On va munir l'espace mesurable $(\Omega , \mathfrak{A})$ de probabilités $(\underset{\sim}{P}_M , M \in \underset{\sim}{N})$ telles que certains résultats ou conjectures déjà obtenus (ou faits) sur les traces de Frobénius t_p d'une courbe elliptique sans multiplication complexe soient vérifiés $\underset{\sim}{P}_M(d\omega)$ p. s. pour la suite $(Y_p , p \in P)$.

Enonçons donc les propriétés en question :

(a) Soit $M \in \underset{\sim}{N}$; on note, pour $t \in \underset{\sim}{Z}$,

$$S_t = \{u \in \underset{\sim}{Z} ; u \equiv t \pmod M\} \quad \text{et} \quad G(M)_t = \{\sigma \in G(M) ; \operatorname{tr} \sigma \in S_t\} .$$

Alors, d'après la condition 1° de la définition : ρ est elliptique, et le théorème de Tchebotarev ([6] , I-8) , on a :

$$(1) \qquad d\{p \in P ; t_p \in S_t\} = \frac{|G(M)_t|}{|G(M)|} ,$$

où, si $A \subset P$, $d(A)$ désigne la densité naturelle de A si elle existe, et, par ailleurs $|F| = \#(F)$.

(b) Si A est une courbe elliptique sans multiplication complexe, une conjecture de Sato-Tate consiste en l'égalité suivante :

$$(2) \qquad d\{p \in P ; \frac{t_p}{2\sqrt{p}} \in (\xi_1 , \xi_2)\} = \int_{\xi_1}^{\xi_2} g(\xi)\, d\xi ,$$

où $(\xi_1 , \xi_2) \subset (-1 , +1)$, et $g(\xi) = \frac{2}{\pi} \sqrt{1 - \xi^2}$.

Dans la situation axiomatique où l'on se trouve, on supposera que l'égalité (2) est vérifiée avec une fonction $g : \underset{\sim}{R} \to \underset{\sim}{R}$, continue, nulle hors de $(-1 , +1)$.

Ces deux propriétés énoncées, on fixe $M \in \underset{\sim}{N}$.

Posons $F_M(t) = M \frac{|G(M)_t|}{|G(M)|}$, et remarquons que $\sum_{t \bmod M} \frac{1}{M} F_M(t) = 1$.

On définit la probabilité $\underset{\sim}{P}_M$ sur $(\Omega , \mathfrak{A})$ par $\underset{\sim}{P}_M = \otimes_{p \in P} \mu_{p,M}$,

où $\mu_{p,M}\{t\} = c_{p,M}\, g(\frac{t}{2\sqrt{p}})\, F_M(t)$ ($c_{p,M}$ est une constante de normalisation qui fait de $\mu_{p,M}$ une probabilité sur $\underset{\sim}{Z}$) .

PROPOSITION 1. - Les propriétés (1) et (2) sont vraies $\underset{\sim}{P}_M(d\omega)$ p. s: lorsque l'on remplace (t_p) par la suite $(Y_p(\omega) , p \in P)$.

De plus, lorsque $p \to \infty$, on a $c_{p,M} \sim \frac{1}{2\sqrt{p}}$.

Indiquons très succintement le déroulement de la démonstration : l'approximation de l'intégrale $\int_{-1}^{+1} g(\xi)d\xi = 1$ par les sommes de Riemann

$$\frac{1}{2\sqrt{p}} \sum_{-2\sqrt{p}<t<2\sqrt{p}} g(\frac{t}{2\sqrt{p}})$$

conduit à $c_{p,M} \sim \frac{1}{2\sqrt{p}}$ (lorsque $p \to \infty$) et d'autre part, si $t_0 \in \underset{\sim}{Z}$, à

$$\lim_{p\to\infty} \mu_{p,M}(S_{t_0}) = \frac{1}{M} F_M(t_0) .$$

On déduit alors du corollaire 1 :

$$d\{p \in P ; Y_p(\omega) \equiv t_0 \pmod M\} = \frac{1}{M} F_M(t_0)\ \underset{\sim}{P}_M(d\omega) \text{ p. s. .}$$

On démontre la propriété (2) avec un raisonnement très analogue.

Soulignons encore que, pour $M \in \underset{\sim}{N}$, et $t_0 \in \underset{\sim}{Z}$, on a

$$(3) \qquad P_M[Y_p = t_0] = c_{p,M}\, g(\frac{t_0}{2\sqrt{p}})\, F_M(t_0) \quad (\simeq_{p\to\infty}) \quad \frac{1}{2\sqrt{p}}\, g(0)\, F_M(t_0) .$$

On veut définir une probabilité $\underset{\sim}{P}$ sur $(\Omega , \mathfrak{A})$ qui soit la limite (en un certain sens) des probabilités $\underset{\sim}{P}_M$ lorsque $M \to \infty$,. Pour cela, il faut, d'après la formule (3), étudier la variation de $F_M(t)$ en M .

3.3. - Comportement de $F_M(t)$ lorsque $M \to \infty$. Contrairement au reste de l'étude, les résultats suivants, résumés dans le théorème 2, ne sont pas "conjecturels".

THÉORÈME 2. - Soit M entier qui décompose et stabilise ρ . Alors, pour tout $t \in \underset{\sim}{Z}$, la suite $F_N(t)$ converge, lorsque N croît vers $+\infty$, pour l'ordre partiel de la divisibilité (on note : $N \uparrow_d \infty$) , vers le produit infini :

$$F(t) = F_M(t) \prod_{\ell \in P, \ell \nmid M} F_\ell(t)$$

De plus, pour $\ell \in P$, $\ell \nmid M$, on a, en posant $r = 1/\ell$:

$$F_\ell(t) = \begin{cases} \dfrac{1}{1 - r^2} & \text{si } t \equiv 0 \pmod \ell \\ (1 - \dfrac{r^3}{1 - r - r^2})^{-1} & \text{sinon .} \end{cases}$$

Nous donnons encore une idée succinte de la démonstration. Elle découle principalement des trois propriétés suivantes :

(p 1) : Si M_1 , $M_2 \in \underset{\sim}{N}$ sont tels que

$$(M_1 , M_2) = 1 \quad \text{et} \quad G(M_1 M_2) = G(M_1) \times G(M_2) ,$$

alors $F_{M_1 M_2}(t) = F_{M_1}(t) \, F_{M_2}(t)$.

(p 2) Si M stabilise ρ , et si M' est un multiple de M , admettant les mêmes diviseurs premiers, alors $F_{M'}(t) = F_M(t)$.

(p 3) : Si pour u entier (mod M) , $uI \in G(M)$, alors $F_M(ut) = F_M(t)$.

De (p 3), on déduit facilement la forme explicite de $F_\ell(t)$ pour $\ell \in P$, $\ell \nmid M$.

D'autre part, si $N = M' \prod_{i=1}^{k} \ell_i^{\beta_i}$, avec $\ell_i \in P$, $\ell_i \nmid M$, et M' multiple de M , admettant les mêmes diviseurs premiers que M , on a, d'après (p 1)

$$F_N(t) = F_{M'}(t) \prod_{i=1}^{k} F_{\ell_i^{\beta_i}}(t) ,$$

et d'après (p 2);

$$F_N(t) = F_M(t) \prod_{i=1}^{k} F_{\ell_i}(t) .$$

Du calcul explicite de $F_\ell(t)$, découle en particulier la convergence du produit infini $\prod_{\ell \in P, \ell \nmid M} F_\ell(t)$ d'où finalement le théorème.

3.4. - Conséquence : la conjecture C 1. - Soit $N \in \underset{\sim}{N}$, $\mu_{p,N}$ étant une probabilité (sur $\underset{\sim}{Z}$), on a :

$$c_{p,N} \sum_{-2\sqrt{p}<t<2\sqrt{p}} g\left(\frac{t}{2\sqrt{p}}\right) F_N(t) = 1 .$$

On vient d'établir la convergence de $F_N(t)$ vers $F(t)$ lorsque $N \uparrow_d \infty$, et donc d'après l'égalité précédente, $c_{p,N}$ converge (vers c_p) lorsque $N \uparrow_d \infty$. Ceci entraîne l'existence d'une probabilité $\underset{\sim}{P}$ sur $(\Omega , \mathfrak{A})$ telle que :

$$\underset{\sim}{P}_N(A) \xrightarrow[N \uparrow_d]{} \underset{\sim}{P}(A) \quad \text{pour tout pavé} \quad A = \prod_{p \in P} A_p \in \mathfrak{A}$$

($A_p = \underset{\sim}{Z}$ sauf pour un nombre fini de p).

Pour $\underset{\sim}{P}$, les variables $(Y_p , p \in P)$ sont indépendantes et si $t_0 \in \underset{\sim}{Z}$, on a :

$$\underset{\sim}{P}[Y_p = t_0] = c_p \, g\left(\frac{t_0}{2\sqrt{p}}\right) F(t_0) . \tag{4}$$

La question est maintenant de savoir si, comme pour la suite $(c_{p,N} , p \in \underset{\sim}{N})$ lorsque N est fixé, on a l'équivalence :

$$c_p \sim \frac{1}{2\sqrt{p}} \quad \text{lorsque} \quad p \longrightarrow \infty . \tag{5}$$

D'après S. LANG (communication personnelle), la démonstration de ce résultat est suffisamment longue et compliquée pour avoir été omise dans la rédaction de [1] où (5) est en fait jugée "raisonnable" et admise.

De (4) et(5), on déduit

$$\underset{\sim}{P}[Y_p = t_0] \underset{(p \to \infty)}{\simeq} \frac{1}{2\sqrt{p}}\, g(0)\, F(t_0) ,$$

et, d'après le corollaire 3,

$$\underset{\sim}{P}(d\omega) \text{ p. s. }, \qquad \#\{p \leq x ; Y_p(\omega) = t_0\} \simeq g(0)\, F(t_0)\, \Pi_{1/2}(x) .$$

On est donc parvenu à la conjecture $\underset{\sim}{C}$, et on a même obtenu pour $C(t_0 , \rho)$ l'expression :

$$C(t_0 , \rho) = g(0)\, F(t_0) .$$

Signalons en particulier, à cause de son importance, que si $t_0 = 0$, on déduit de cette formule et de $F_\ell(0) = \dfrac{1}{1 - 1/\ell^2}$ si $\ell \in P$, $\ell \nmid M$ (voir le théorème 2), la formule suivante :

$$C(0 , \rho) = g(0)\, \frac{\Pi^2}{6}\, F_M(0) \prod_{\ell \mid M} \left(1 - \frac{1}{\ell^2}\right) .$$

Remarque : On a montré précédemment que pour tout pavé $A \in \mathfrak{A}$, $\underset{\sim}{P}_N(A) \to \underset{\sim}{P}(A)$ lorsque $N \uparrow_d \infty$. Ceci n'entraîne évidemment pas que cette convergence ait lieu pour tout $A \in \mathfrak{A}$, comme le montre le contre-exemple suivant.

On a obtenu (essentiellement comme conséquence du corollaire 3),

$$\underset{\sim}{P}(d\omega) \text{ p. s. }, \qquad \#\{p \leq x ; Y_p(\omega) = t_0\} \simeq g(0)\, F(t_0)\, \Pi_{1/2}(x) .$$

La même démonstration donne, pour $N \in \underset{\sim}{N}$,

$$\underset{\sim}{P}_N(d\omega) \text{ p. s. }, \qquad \#\{p \leq x ; Y_p(\omega) = t_0\} \simeq g(0)\, F_N(t_0)\, \Pi_{1/2}(x) ,$$

et donc si $F_N(t_0) \neq F(t_0)$, on a $\underset{\sim}{P}_N(A_0) = 0$, où

$$A_0 = \{\omega ; \#\{p \leq x ; Y_p(\omega) = t_0\} \simeq g(0)\, F(t_0)\, \Pi_{1/2}(x)\}$$

est un ensemble $\mathfrak{A}$-mesurable qui porte la probabilité $\underset{\sim}{P}$.

4. Exemples.

Ils portent sur des courbes elliptiques particulières. D'après ce qui précède, il s'agit, pour chaque exemple, de déterminer un entier $M \in \underset{\sim}{N}$ qui décompose et stabilise ρ, et de calculer explicitement $F_M(t)$.

4.1. Les courbes de Serre. - On a besoin des notations suivantes :

Si $q \in P$ (q impair), $GL_2(\underset{\sim}{Z}_q)$ a un unique sous-groupe d'indice 2, noté E_q, constitué des matrices $\sigma \in GL_2(\underset{\sim}{Z}_q)$ telles que $\det \sigma$ soit un carré mod q.

Si $q = 2$, on considère la restriction modulo 2

$$r_2 : GL_2(\underset{\sim}{Z}_2) \to GL_2(\underset{\sim}{Z}/2\underset{\sim}{Z}) \simeq S_3$$

$$\sigma \to \bar{\sigma}$$

et on définit $E_2 = \{\sigma \in GL_2(\underset{\sim}{Z}_2) ; \bar{\sigma}$ est une permutation paire$\}$.

Si $q \in P$, O_q est le complémentaire de E_q dans $GL_2(\underset{\sim}{Z}_q)$, et on note, pour $q \in P$ $(q \neq 2)$,

$$S_{2q} = (E_2 \times E_q) \cup (O_2 \times O_q) ,$$

sous-groupe de $GL_2(\underset{\sim}{Z}_2) \times GL_2(\underset{\sim}{Z}_q)$.

Définition 2. - On dit que A est une courbe de Serre pour $M = 2q$ si

1° $M = 2q$ décompose et stabilise ρ, avec $G_M \subset S_{2q}$

2° $G(M) = r_{2q}(S_{2q})$.

Si A est une courbe de Serre pour $M = 2q$, on peut donner une formule explicite pour $F_{2q}(t)$ (voir [1], page 43).

Précisons seulement

$$F_{2q}(t) = \frac{2q\,|G(2q)_t|}{3q(q-1)(q^2-1)} ,$$

formule qui découle de la propriété : $G(2q) = S_{2q}(2q)$ est d'indice 2 dans $GL_2(\underset{\sim}{Z}/2\underset{\sim}{Z}) \times GL_2(\underset{\sim}{Z}/q\underset{\sim}{Z})$.

Par exemple, la courbe d'équation $y^2 = x^3 + 6x - 2$ est une courbe de Serre pour $M = 2 \times 3$.

4.2. La courbe de Shimura. - C'est une des douze courbes elliptiques modulaires étudiées par LIGOZAT [2]. Elle a pour équation $y^2 + y = x^3 - x^2 - 10x - 20$.

Ce n'est pas une courbe de Serre, et la détermination d'un entier M qui décompose et stabilise ρ est plus compliquée que pour ces courbes.

Les résultats essentiels sont les suivants :

(a) t_p est le coefficient de q^p dans le développement en série de

$$q \prod_{n=1}^{\infty} (1 - q^n)^2 \, (1 - q^{11n})^2 .$$

(b) $M = 2 \times 11 \times 25$ décompose et stabilise ρ.

(c) 5 est stable ; d'après (p 2), on a donc $F_{25}(t) = F_5(t)$; de plus,

$$G(5) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} , \; u \in \underset{\sim}{F}_5^* \right\} ,$$

dont on déduit facilement :

$$F_5(t) = \begin{cases} 5/4 & \text{si } t \not\equiv 1 \pmod 5 \\ 0 & \text{si } t \equiv 1 \pmod 5 \end{cases} .$$

(d) $\rho_{2\times 11}(G) = S_{2\times 11}$, et $F_{2\times 11}(t)$ est donné par la formule générale valable pour une courbe de Serre pour $q = 11$.

(e) $F_M(t) = F_{2\times 11}(t)\, F_{25}(t) = F_{2\times 11}(t)\, F_5(t)$. En particulier, si $t \equiv 1 \pmod 5$, cette courbe fournit donc un exemple pour lequel $C(t, \rho) = 0$.

BIBLIOGRAPHIE

[1] LANG (S.) et TROTTER (H.). - Frobenius distributions in GL_2 extensions. - Berlin, Springer-Verlag, 1976 (Lecture Notes in Mathematics, 504).

[2] LIGOZAT (G.). - Courbes modulaires de genre 1, Bull. Soc. math. France, Mémoire 43, 1975, 80 p.

[3] MAZUR (B.). - Rational points of abelian varieties with values in towers of number fields, Invent. Math., t. 18, 1972, p. 183-266.

[4] NEVEU (J.). - Bases mathématiques du calcul des probabilités. - Paris, Masson, 1964.

[5] SERRE (J.-P.). - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., t. 15, 1972, p. 259-331.

[6] SERRE (J.-P.). — Abelian ℓ-adic representations and elliptic curves. - New York, Benjamin, 1968.

[7] SERRE (J.-P.). - Groupes de Lie ℓ-adiques attachés aux courbes elliptiques, Colloques internationaux du C. N. R. S., 143 : Les tendances géométriques en algèbre et théorie des nombres [1964. Clermont-Ferrand], p. 239-256. - Paris, Centre national de la Recherche scientifique, 1966.

(Texte reçu le 6 juillet 1976)

Marc YOR
212 avenue Aristide Briand
92220 BAGNEUX