Séminaire BOURBAKI Janvier 2018
70e année, 2017–2018, no 1141, p. 205 à 250
doi:10.24033/ast.1085

ÉQUIRÉPARTITION DE SOMMES EXPONENTIELLES

[Travaux de Katz]

par **Javier FRESÁN**

1. INTRODUCTION

Cent ans se sont écoulés depuis la parution de l'article de Weyl [**48**] sans que les résultats d'équirépartition en théorie des nombres cessent de faire florès, révélant des liens profonds avec la géométrie algébrique et la théorie des représentations. L'interaction de ces domaines est particulièrement riche dans les travaux de Katz dont il sera question ici. Ce sont des théorèmes, anciens et récents, d'équirépartition de sommes exponentielles sur les corps finis, le plus souvent à caractéristique fixée. Les sommes concernées s'obtiennent par transformation de Fourier, relative à un caractère, de la fonction trace d'un faisceau ℓ-adique sur un groupe algébrique commutatif, et il s'agit de comprendre leur répartition lorsque le faisceau est fixe mais que l'on fait varier le caractère.

1.1. L'exemple des sommes de Gauss et des sommes de Kloosterman

Soient p un nombre premier, q une puissance de p et $\mathbf{F}_q$ un corps fini à q éléments. Étant donnés un caractère additif non trivial $\psi\colon \mathbf{F}_q \to \mathbf{C}^\times$ et un caractère multiplicatif $\chi\colon \mathbf{F}_q^\times \to \mathbf{C}^\times$, on définit la *somme de Gauss* $g(\psi,\chi)$ comme l'entier algébrique

$$g(\psi,\chi) = \sum_{x\in\mathbf{F}_q^\times} \psi(x)\chi(x).$$

Par exemple, si $q = p$ et si l'on prend pour ψ le caractère $x \mapsto \exp(2\pi i x/p)$ et pour χ le symbole de Legendre, il s'agit de la somme considérée par Gauss dans sa quatrième preuve de la loi de réciprocité quadratique [**12**].

Si χ est trivial, la somme de Gauss vaut -1 ; sinon, sa valeur absolue est égale à $\sqrt{q}$. Choisissons, pour chaque p, un caractère non trivial ψ_p de $\mathbf{F}_p$ et notons ψ_q le caractère de $\mathbf{F}_q$ obtenu par composition avec la trace. Gardant ψ_q fixe et faisant varier χ parmi les caractères multiplicatifs non triviaux, on obtient $q-2$ points

$$\theta_{q,\chi} = \frac{g(\psi_q, \chi)}{\sqrt{q}}$$

dans le cercle unité S^1. Comment ces points se répartissent-ils quand q tend vers l'infini ?

Soient (X, μ) un espace topologique compact muni d'une mesure de probabilité μ et (S_N) une suite [(1)] d'ensembles finis non vides avec des applications $\theta_N \colon S_N \to X$. Rappelons que les (S_N, θ_N) sont dits *équirépartis selon* μ si la suite de mesures $|S_N|^{-1} \sum_{x \in S_N} \delta_{\theta_N(x)}$ converge vaguement vers μ lorsque N tend vers l'infini, c'est-à-dire si, pour toute fonction continue $f \colon X \to \mathbf{C}$, on a l'égalité

$$\int_X f(x)\mu(x) = \lim_{N \to \infty} \frac{1}{|S_N|} \sum_{x \in S_N} f(\theta_N(x)).$$

Il suffit en fait de la vérifier pour une classe de fonctions test dont les combinaisons linéaires finies sont denses dans l'espace $\mathscr{C}(X)$ des fonctions continues à valeurs complexes muni de la topologie de la convergence uniforme.

Dans le cas qui nous occupe, Katz remarqua dans [**17**, §1.3.3] que la majoration des sommes de Kloosterman obtenue par Deligne comme conséquence de ses travaux sur la conjecture de Weil entraînait le résultat d'équirépartition suivant :

THÉORÈME 1.1 (Deligne). — *Lorsque q tend vers l'infini, les points $\{\theta_{q,\chi}\}_{\chi \neq 1}$ s'équirépartissent selon la mesure de Haar normalisée sur le cercle unité. Autrement dit, pour toute fonction continue $f \colon S^1 \to \mathbf{C}$ on a l'égalité*

$$\frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta})\, d\theta = \lim_{q \to \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}). \tag{1}$$

Comme les polynômes de Laurent sont denses dans $\mathscr{C}(S^1)$, il suffit de considérer les fonctions $f(z) = z^n$ avec n entier. Le cas $n = 0$ est évident. Le membre gauche de (1) étant nul pour $n \neq 0$, il faut démontrer que la suite

$$\frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}) = \frac{1}{q^{\frac{n}{2}}(q-2)} \sum_{\chi \neq 1} g(\psi_q, \chi)^n$$

(1) Bien que l'on utilise N comme paramètre, dans les énoncés qui suivent la suite n'est pas forcément indexée par des entiers mais par des caractères, des points d'une variété algébrique, etc.

converge vers zéro lorsque q tend vers l'infini (c'est le *critère d'équirépartition de Weyl*). Grâce à la relation $g(\psi_q,\chi)^{-1} = g(\bar{\psi}_q,\bar{\chi})q^{-1}$, on peut se ramener à $n \geqslant 1$, auquel cas les puissances des sommes de Gauss sont égales à

$$\begin{aligned} g(\psi_q,\chi)^n &= \sum_{x_1,\dots,x_n\in\mathbf{F}_q^\times} \psi_q(x_1+\cdots+x_n)\chi(x_1\cdots x_n) \\ &= \sum_{a\in\mathbf{F}_q^\times}\chi(a) \sum_{\substack{x_1,\dots,x_n\in\mathbf{F}_q^\times \\ x_1\cdots x_n=a}} \psi_q(x_1+\cdots+x_n). \end{aligned} \tag{2}$$

Il s'ensuit que $\chi \mapsto g(\psi_q,\chi)^n$ est la transformée de Fourier, au sens du groupe abélien fini $\mathbf{F}_q^\times$, de la fonction qui à un élément $a \in \mathbf{F}_q^\times$ associe la *somme de Kloosterman*

$$\mathrm{Kl}_n(a,q) = \sum_{\substack{x_1,\dots,x_n\in\mathbf{F}_q^\times \\ x_1\cdots x_n=a}} \psi_q(x_1+\ldots+x_n).$$

Pour $n = 2$, ces sommes font un caméo dans l'article posthume de Poincaré sur les formes modulaires, où il « se borne à constater » qu'elles ne sont pas nulles en général [(2)] [**39**, p. 148]. Kloosterman les introduisit de manière indépendante en 1926, en raffinant la méthode du cercle pour étudier l'asymptotique du nombre de représentations d'un entier par une forme quadratique définie positive en quatre variables [**29**]. Un point clé de son travail est la majoration $|\mathrm{Kl}_2(a,q)| < 2q^{3/4}$, qu'il obtint en calculant le quatrième moment

$$\sum_{a\in\mathbf{F}_q^\times} \mathrm{Kl}_2(a,q)^4 = 2q^3 - 3q^2 - 3q - 1. \tag{3}$$

Quelques années plus tard, Salié [**43**] et Davenport [**7**] purent améliorer l'exposant de $3/4$ à $2/3$ en estimant le sixième moment. Puis en 1934 Hasse observa, en comparant la somme de Kloosterman au nombre de solutions de l'équation $y^q - y = x + ax^{-1}$, que la borne optimale $2\sqrt{q}$ découlait de l'hypothèse de Riemann pour les courbes sur les corps finis [**15**] ; avec la preuve de Weil entre 1940 et 1948, elle fut enfin établie [**46**].

Trouver la majoration optimale pour les sommes de Kloosterman en plusieurs variables est une tâche significativement plus compliquée qui requiert l'analogue de l'hypothèse de Riemann pour la cohomologie à coefficients dans un faisceau ℓ-adique. En la démontrant dans l'article [**9**], auquel on se référera comme « Weil II » par la suite, Deligne ouvrit la voie à de nombreuses applications à l'étude des sommes

(2) Les sommes de Poincaré portent sur $(\mathbf{Z}/q\mathbf{Z})^\times$ et peuvent être nulles. Celles que l'on considère ici ne le sont *jamais*, car $\mathrm{Kl}_2(a,q)$ appartient au sous-anneau de $\mathbf{C}$ engendré par une racine primitive p-ème de l'unité ζ_p et l'on a $\mathrm{Kl}_2(a,q) \equiv -1$ modulo l'idéal premier $1-\zeta_p$.

exponentielles que nous sommes encore loin d'avoir épuisées. Lui-même exposa le principe de la méthode dans **[8]**, où il montre comment en déduire l'estimée

$$|\mathrm{Kl}_n(a,q)| \leqslant nq^{\frac{n-1}{2}}$$

pour n'importe quels $n \geqslant 2$ et $a \in \mathbf{F}_q^\times$. C'est ce qu'il fallait pour conclure la preuve.

Fin de la démonstration. — En sommant la formule (2) sur les caractères multiplicatifs non triviaux, il vient

$$\sum_{\chi \neq 1} g(\psi_q, \chi)^n = -g(\psi,1)^n + \sum_{a \in \mathbf{F}_q^\times} \mathrm{Kl}_n(a,q) \sum_{\chi} \chi(a) = (-1)^{n+1} + (q-1)\mathrm{Kl}_n(1,q)$$

par orthogonalité des caractères. D'après la majoration de Deligne, nous avons donc

$$\left| \frac{1}{q^{\frac{n}{2}}(q-2)} \sum_{\chi \neq 1} g(\psi_q, \chi)^n \right| \leqslant \frac{2n+1}{\sqrt{q}}$$

pour tout $q > 2$ et la limite du membre gauche est bien zéro lorsque $q \to \infty$. □

Remarque 1.2. — Le théorème s'applique tant à la situation où p est fixe et l'on fait tendre q vers l'infini parmi les puissances de p qu'à la situation où p varie aussi, ce qui est possible car la constante dans la majoration des moments (en l'occurrence $2n+1$) est indépendante de p. En théorie analytique des nombres, on parle souvent d'équirépartition *verticale* ou *horizontale* pour distinguer ces deux cas.

Revenons maintenant aux sommes de Kloosterman. Comme appliquer la conjugaison complexe revient à échanger x_i et $-x_i$ dans l'expression de $\mathrm{Kl}_2(a,q)$, ce sont des nombre réels (il en va de même pour tout n pair). Au vu de la borne de Weil, pour chaque $a \in \mathbf{F}_q^\times$, il existe un unique angle $\theta_{q,a} \in [0,\pi]$ tel que

$$\mathrm{Kl}_2(a,q) = 2\sqrt{q}\cos\theta_{q,a}.$$

Comment ces $q-1$ angles varient-ils avec q ? En s'appuyant sur l'interprétation de la somme $\mathrm{Kl}_2(a,q)$ comme la trace de Frobenius en $a \in \mathbb{G}_m(\mathbf{F}_q)$ d'un système local ℓ-adique sur $\mathbb{G}_m$ et sur un théorème de Deligne affirmant que la répartition de telles traces est gouvernée par le groupe de monodromie, Katz démontra dans **[18]** que les angles $\{\theta_{q,a}\}_{a \in \mathbf{F}_q^\times}$ se répartissent comme les classes de conjugaison de matrices aléatoires dans le groupe spécial unitaire $\mathrm{SU}(2)$. Plus précisément, si l'on identifie l'intervalle $[0,\pi]$ à l'espace de ces classes par l'application qui envoie θ sur la classe de conjugaison de $\left(\begin{smallmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{smallmatrix}\right)$, l'image directe de la mesure de Haar normalisée sur $\mathrm{SU}(2)$ par la projection canonique est la mesure $(2/\pi)\sin^2\theta\, d\theta$ sur $[0,\pi]$. Elle porte en théorie des nombres le nom de *mesure de Sato-Tate*, d'après leur célèbre conjecture sur la répartition du terme d'erreur dans l'approximation par $p+1$ du nombre de points de la réduction modulo p d'une courbe elliptique sur $\mathbf{Q}$ sans multiplication complexe.

THÉORÈME 1.3 (Katz). — *Lorsque q tend vers l'infini, les angles $\{\theta_{q,a}\}_{a\in\mathbf{F}_q^\times}$ s'équirépartissent selon la mesure de Sato-Tate, c'est-à-dire pour toute fonction continue $f\colon[0,\pi]\to\mathbf{C}$ on a l'égalité*

$$\frac{2}{\pi}\int_0^\pi f(\theta)\sin^2\theta\,d\theta=\lim_{q\to\infty}\frac{1}{q-1}\sum_{a\in\mathbf{F}_q^\times}f(\theta_{q,a}).$$

À nouveau, ce résultat est valable pour n'importe quelle suite de corps finis de cardinaux croissants. On conjecture également que, pour un entier *fixe* a, les angles $\{\theta_{p,a}\}_{p\leqslant N}$ s'équirépartissent selon la mesure de Sato-Tate lorsque p tend vers l'infini parmi les nombres premiers ne divisant pas a, mais même des conséquences faibles de cet énoncé paraissent hors de portée à l'heure actuelle [(3)].

1.2. Les sommes d'Evans et de Rudnick

Autour de 2003, Evans et Rudnick trouvèrent d'autres exemples de sommes exponentielles dépendant d'un caractère multiplicatif qui, d'après leurs expériences numériques, semblaient s'équirépartir selon la mesure de Sato-Tate. D'un côté, Evans étudia les sommes

$$S(\chi)=-\frac{1}{\sqrt{q}}\sum_{x\in\mathbf{F}_q^\times}\chi(x)\psi_q\big(x-x^{-1}\big),$$

qui sont des nombres réels de valeur absolue au plus 2 par l'hypothèse de Riemann sur les courbes. Ils s'écrivent donc $S(\chi)=2\cos\theta_{q,\chi}$ pour un unique $\theta_{q,\chi}\in[0,\pi]$. Est-il vrai que les angles $\{\theta_{q,\chi}\}_\chi$ s'équirépartissent selon la mesure de Sato-Tate quand q tend vers l'infini ? Ou, ce qui revient au même, les sommes $S(\chi)$ s'équirépartissent-elles selon la *mesure du demi-cercle* $(1/2\pi)\sqrt{4-x^2}\,dx$ sur l'intervalle $[-2,2]$?

À la même époque, Rudnick rencontra des sommes semblables dans ses travaux sur le chaos quantique. Décrivons brièvement le contexte, en nous référant à **[32]**, **[33]** et **[42]** pour plus de détails. Il s'agit de quantifier le système dynamique obtenu en itérant la transformation du tore $T^2=\mathbf{R}^2/\mathbf{Z}^2$ définie par une matrice hyperbolique $A\in\mathrm{SL}(2,\mathbf{Z})$, des applications connues comme « cat maps » dans la littérature. Soient $N\geqslant 1$ un entier et $\mathcal{H}_N$ l'espace de Hilbert $L^2(\mathbf{Z}/N\mathbf{Z})$. On pense à N comme à l'inverse de la constante de Planck $\hbar$, de sorte que la limite semi-classique $\hbar\to 0$ devienne $N\to\infty$. Après avoir associé à chaque observable classique

(3) Mentionnons, à titre d'exemple, la *conjecture du changement de signe* : puisque $\sin^2\theta$ est symétrique par rapport à $\theta=\pi/2$ et que les $\mathrm{Kl}_2(a,p)$ sont tous non nuls, il devrait y avoir asymptotiquement autant de premiers p pour lesquels la somme de Kloosterman est positive que négative. On n'en sait rien ! Dans **[10]**, Fouvry et Michel démontrent des résultats dans cette direction quand la suite des p est remplacée par une suite de nombres « presque premiers », c'est-à-dire non premiers, sans facteur carré et ayant un nombre de facteurs premiers borné uniformément.