Minorations de sommes d'exponentielles

Philippe MICHEL, Université d'Orsay

October 22, 2000

Bât. 425, Mathématiques,91405 Orsay
E-mail : michel@math.u-psud.fr

1 Introduction

Soit $f(X) \in \mathbf{Q}(X)$ une fraction rationnelle, on la suppose normalisée de sorte que $f = P/Q$, P et Q étant des polynômes premiers entre eux, dont les coefficients sont entiers et premiers entre eux. On considère la famille de sommes d'exponentielles S_f définie par (en notant $\mathrm{e}_n(.) = \exp(2i\pi./n)$)

$$S_f(m;n) := \sum_{\substack{x\in\mathbf{Z}/n\mathbf{Z}\\(Q(x),n)=1}} \mathrm{e}_n(mP(x)\overline{Q(x)}) := \sum_{\substack{x\in\mathbf{Z}/n\mathbf{Z}\\(Q(x),n)=1}} \mathrm{e}_n(mf(x)),\ (m,n)=1;$$

comme de coutume $\overline{m}$ (mod n) est l'inverse de m modulo n ($m\overline{m} = 1 \pmod n$). Comme on le sait, de nombreux problèmes de théorie des nombre nécessitent de savoir majorer non trivialement la somme $S_f(m;n)$. Pour ce faire, un dévissage facile nous ramène au cas crucial où $n = p$ est un nombre premier. Depuis Weil et la démontration de l'hypothèse de Riemann pour les courbes sur les corps finis, on sait que pour p assez grand, on a la majoration

$$|S_f(m;p)| \leq k_f p^{1/2},$$

avec $k_f = \max(\deg P, \deg Q) + \sharp\{$ racines distinctes de $Q\} - 1$ ([D2]). La question de savoir si cette majoration est optimale quand l'un des deux paramètres m ou p varie est donc très naturelle. Le cas où p est fixé et où m décrit $\mathbf{F}_p^*$ est assez bien compris depuis les travaux de Deligne et de Katz (voir [Ka3] pour une discussion très claire à ce propos): en effet, pour les fractions f décrites ci-dessous, on peut donner une mesure explicite μ_f sur $[-1,1]$ telle que quand $p \to +\infty$ la famille des sommes normalisées $\{\dfrac{S_f(m;p)}{k_f p^{1/2}}\}_{m=1\ldots p-1}$ devient équidistribuée relativement à μ_f. En revanche, quand m est fixé (disons $m = 1$), peu de choses sont connues sur la distribution des sommes $\{\dfrac{S_f(1;p)}{k_f p^{1/2}}\}_p$ quand p décrit l'ensemble des nombres premiers : on s'attend

cependant à ce que les sommes soient également équidistribuées relativement à μ_f. Citons deux cas connus déquirépartition : celui du monôme $f(x) = x^3$, Heath-Brown et Patterson [HB-P] ont montré que pour p décrivant l'ensemble des nombre premiers $= 1$ *mod* 3, les angles θ_p définis par $\cos\theta_p = S_{X^3}(1;p)/2p^{1/2}$ sont équirépartis relativement à la mesure uniforme sur $[-\pi,\pi]$, et plus récemment la preuve par Duke, Friedlander et Iwaniec que les rationnels $\{\pm\frac{v}{p}\}_{p\in\mathcal{P}}$ définis modulo 1 par l'équation $v^2+1 = 0(\text{mod } p)$ sont équirépartis modulo 1 [DFI]; observons que la preuve de ces deux théorèmes nécessite d'employer la pleine force de la théorie de formes modulaires... Notre but est plus modeste, puisque généralisant notre précédent travail sur les sommes de Kloosterman [Mi], nous allons donner des minorations de sommes $S_f(1;pq)$ pour un module $n = pq$ un produit de deux nombres premiers et une fraction f vérifiant des hypothèses génériques.

Commençons par introduire quelques notations:
— Dans la suite, les lettres p et q désigneront exclusivement des nombres premiers.
— Nous dirons qu'un ensemble $\mathcal{P}$ de *couples* (p,q) *de nombres premiers a une densité positive* si pour tout x suffisamment grand on a

$$\sharp\{(p,q)\in\mathcal{P},\ p,q\leq x\}\gg\frac{x^2}{\log^2 x}.$$

— Soit G un groupe algébrique complexe, fixons K un sous-groupe compact maximal de G, et notons $\mu_{H,K}$ la mesure de Haar de K et $K^\natural$ l'espace des classes de conjugaisons de K muni de la mesure $\mu_{ST,K}$ (ST comme Sato-Tate) image de $\mu_{H,K}$ par la projection canonique; pour toute représentation ρ de G, on définit la constante positive $\alpha(G,\rho)$ par l'équation

$$\mu_{H,K}(\{k\in K,\ |tr(\rho(k))|>\alpha(G,\rho)\})=1/2.$$

Nous montrons alors le Théorème suivant:

Théorème 1.1 . — *Soit $f(X)\in\mathbf{Q}(X)$ une fraction qui n'est pas un polynôme de degré ≤ 2 et qui vérifie les trois conditions suivantes:*

- *H.1.— Les zéros de $f'(X)$ dans $\mathbf{P}^1(\mathbf{C})$ sont simples; on note Z_f l'ensemble de ces zéros de f' (donc $\sharp Z_f = k_f$).*
- *H.2.— f sépare les zéros de $f'(X)$: si z, z' sont deux zéros de f', $f(z)=f(z')\Longrightarrow z=z'$: soit $C_f := f(Z_f)$ alors $\sharp C_f = \sharp Z_f$.*
- *H.3.— Soient $s_1,s_2,s_4,s_4\in C_f$, il n'y a pas de relations de la forme $s_1-s_2=s_3-s_4$, exceptées les relations triviales $s_1=s_3$ et $s_2=s_4$ (resp. $s_1=s_2$ et $s_3=s_4$).*

Alors, pour tout $\epsilon>0$ l'ensemble des couples de nombres premiers (p,q) vérifiant l'inégalité

$$|\frac{S_f(1;pq)}{(pq)^{1/2}}|\geq\alpha(SL_{k_f},std)^2-\epsilon \tag{1}$$

a une densité positive (std désigne la représentation standard de SL_{k_f}). D'autre part, pour tout $\epsilon > 0$, l'ensemble des couples de nombres premiers (p, q) vérifiant

$$|\frac{S_f(1; pq)}{(pq)^{1/2}}| \leq \epsilon, \tag{2}$$

a une densité positive.

Remarque. — Notons que si $\deg P \leq \deg Q$, la condition H.1. n'est jamais vérifiée (∞ est un zéro d'ordre au moins deux de $f'(X)$). Remarquons encore que si $\deg P > \deg Q$ sont fixés, les trois conditions H.1, H.2., H.3. sont vérifiées génériquement.

Remarque. — Il semble que dans ce théorème, les conditions les plus importantes soient H.1. et H.2. (elles assurent en effet qu'un faisceau associé à la somme S_f est irréductible). Par exemple, si k_f est premier, un résultat analogue est valable sans l'hypothèse H.3, quitte à changer de constante $\alpha(G, \rho)$. Il nous parait donc raisonnable de conjecturer une minoration similaire des sommes $S_f(1; pq)$ sous les seules hypothèses H.1. et H.2. En revanche, comme le montre l'exemple des sommes de Gauss ($f(X) = X^k$) qui est le cas extrême de réductibilité, se passer des hypothèses H.1 et H.2 ne paraît pas raisonnable sans poser de conditions de congruences supplémentaires sur p et q.

Les conditions H.1. H.2., H.3. sont vérifiées quand f a la forme suivante ([Ka2], 7.10.5,7.10.6).

- $$f(X) = aX^{k+1} + bX$$
  avec $a, b \neq 0$, et k un entier impair vérifiant $k \geq 2$ ou $k \leq -2$ est un entier pair.
- $f(x)$ est un polynôme non nul dont le polynôme dérivé est proportionnel à un polynôme unitaire de degré $k+1 \geq 6$, irréductible ayant pour groupe de *Galois* le groupe des permutations de k éléments, $\mathcal{S}_k$ (rappelons ([G]), que presque tout polynôme g de $\mathbf{Z}[X]$ est irréductible de groupe de Galois $\mathcal{S}_{\deg q}$).

Ce théorème admet une variante qui permet de traiter des cas non couverts par le Théorème précédent, par exemple le cas où $f(X) = aX^{k+1} + bX$ avec k pair $\neq 0$.

Théorème 1.2 *Soit f une fraction rationnelle impaire qui n'est pas un polynôme de degré 1 et qui vérifie les hypothèses H.1. et H.2. du Théorème 1.1 ainsi que l'hypothèse*

- *H.3'.— Soient $s_1, s_2, s_4, s_4 \in C_f$, il n'y a pas de relations de la forme $s_1 - s_2 = s_3 - s_4$, exceptées les relations triviales $s_1 = s_3$ et $s_2 = s_4$ ou bien $s_1 = s_2$ et $s_3 = s_4$ ou bien $s_1 = -s_4$ et $s_2 = -s_3$.*

Alors k_f est pair et pour tout $\epsilon > 0$ l'ensemble des couples de nombres premiers (p,q) vérifiant l'équation

$$|\frac{S_f(1;pq)}{(pq)^{1/2}}| \geq \alpha(Sp_{k_f}, std)^2 - \epsilon \tag{3}$$

a une densité positive. D'autre part, pour tout $\epsilon > 0$ l'ensemble des couples de nombres premiers (p,q) vérifiant

$$|\frac{S_f(1;pq)}{(pq)^{1/2}}| \leq \epsilon, \tag{4}$$

a une densité positive.

De même nous généralisons le Théorème 1 de [Mi] aux sommes de Kloosterman à plusieurs variables:

Théorème 1.3 . — *Soit $k \geq 2$; pour m et n des entiers premiers entre eux, on pose $Kl_k(m;n)$ la somme de Kloosterman en k variables:*

$$Kl_k(m;n) = \sum_{\substack{x_1,\ldots,x_k \in \mathbf{Z}/n\mathbf{Z}^* \\ x_1 x_2 \ldots x_k = m (\mathrm{mod}\ n)}} \mathrm{e}_n(x_1 + \ldots + x_k).$$

Soit $\alpha_k = \alpha(SL_k, std)$ (resp. $= \alpha(Sp_k, std)$) si k est impair (resp. pair). Alors, pour tout $\epsilon > 0$, l'ensemble des couples de nombres premiers vérifiant l'équation ci-dessous a une densité positive

$$|\frac{Kl_k(1;pq)}{(pq)^{(k-1)/2}}| \geq \alpha_k - \epsilon.$$

D'autre part, pour tout $\epsilon > 0$ l'ensemble des couples de nombres premiers (p,q) vérifiant

$$|\frac{Kl_k(1;pq)}{(pq)^{(k-1)/2}}| \leq \epsilon$$

a une densité positive.

Enfin il n'est pas beaucoup plus difficile d'obtenir des minorations *simultanée* de plusieurs sommes d'exponentielles des différents types rencontrées précédemment; à titre d'exemple nous donnons le théorème assez frappant suivant pour plusieurs sommes "conjuguées" par Galois:

Théorème 1.4 . — *Soit $a_1, \ldots, a_n$, n entiers positifs distincts; soit f une fraction rationnelle vérifiant les hypothèses du Théorème 1.1, et notons $\alpha(SL_{k_f}, std, n)$ la constante positive définie par l'équation*

$$\mu_{H,K_{SL_{k_f}}}(\{k \in K_{SL_{k_f}},\ |tr(k)| > \alpha(SL_{k_f}, std, n)\}) = 1/2^{1/n};$$

alors, pour tout $\epsilon > 0$ l'ensemble des couples de nombres premiers (p, q), vérifiant le système d'inégalités

$$|\frac{S_f(a_i; pq)}{(pq)^{1/2}}| \geq \alpha(SL_{k_f}, std, n)^2 - \epsilon, \tag{5}$$

pour tout $i = 1 \ldots n$, a une densité positive.

Ce dernier résultat suggère que les sommes $S_f(m; p)$ pour des m distincts devraient se comporter indépendamment les unes des autres quand p décrit l'ensemble des nombres premiers.

Remerciements

Ce travail est une généralisation d'une partie de ma thèse à Orsay et je tiens à remercier E. Fouvry mon directeur, N.M. Katz dont le travail sous-tend tout cet article ainsi que Gérard Laumon de l'aide qu'ils m'ont apportée.

2 $\overline{\mathbf{Q}}_\ell$-faisceaux sur $\mathbf{G}_m \otimes \mathbf{F}_p$

Notations

On fixe $\ell \neq p$ un nombre premier; une clôture algébrique $\overline{\mathbf{Q}}_\ell$ de $\mathbf{Q}_\ell$ et un plongement de $\overline{\mathbf{Q}}_\ell$ dans $\mathbf{C}$.

Soit ψ (resp. χ) un caractère additif (resp. multiplicatif) de $\mathbf{F}_{p^n}$ (resp. de $\mathbf{F}_{p^n}^*$), on note $\mathcal{L}_\psi$ (resp. $\mathcal{L}_\chi$) le $\overline{\mathbf{Q}}_\ell$-faisceaux de rang 1 qui lui correspond.

$\mathcal{G}^\vee$ désigne le *dual* du faisceau $\mathcal{G}$, $G_{geom}(\mathcal{G})$ et $G_{arith}(\mathcal{G})$ désignent respectivement ses groupes de monodromie géométrique et arithmétique ; pour tout faisceau $\mathcal{G}$ sur $\mathbf{G}_m$ et $a \in \overline{\mathbf{F}}_p^*$, on note $a^*\mathcal{G}$ le pull-back de $\mathcal{G}$ par le morphisme de translation $\mathbf{G}_m : x \to ax$; pour tout entier $k \in \mathbf{Z} - \{0\}$, on note $[k]^*\mathcal{G}$ le pull-back de $\mathcal{G}$ par le morphisme de $\mathbf{G}_m : x \to x^k$.

2.1 Fonctions supermorses

On rappelle ici la construction due à Katz [Ka2] 7.10.2, du faisceau attaché aux sommes $S_f(m; p)$.

Soit $f(X)$ une fraction rationnelle vérifiant H.1. et H.2. alors pour tout p assez grand $f(X)$ mod p vérifie encore H.1. et H.2. dans $\mathbf{F}_p$; on suppose p est fixé assez grand et on note f pour f modulo p. Soit D_f le diviseur des pôles de f (on a vu que $\infty \in D_f$), Z_f l'ensemble des zéros de f' et $C_f = f(Z_f)$ (par H.2. $\sharp Z_f = \sharp C_f = k_f$), si $p > \deg f$, f défini un revêtement fini étale

$$\mathbf{P}^1 - D_f - Z_f \to \mathbf{A}^1 - C_f$$

de degré $\deg f$, et on dit que f est une fonction *supermorse*; on dispose alors d'une application trace: $tr_f : f_*\overline{\mathbf{Q}}_\ell \to \overline{\mathbf{Q}}_\ell$ dont on note $\mathcal{F}_f$ le noyau. On note $\mathcal{G}_f := NFT_\psi\mathcal{F}_f$ son transformé de Fourier : c'est un faisceau lisse sur $\mathbf{G}_{m,\mathbf{F}_p}$, pur de poids 1, de rang $k_f = \sharp Z_f$, Lie-irréductible modérément ramifié en 0 et sauvagement ramifié en ∞ ([Ka2] 7.9, 7.10) on a:

$$\forall t \in \mathbf{F}_p^*,\ tr(Frob_t, \mathcal{G}_f) = S_f(t;p);$$

$$\mathcal{G}_f(0)/\mathcal{G}_{f,0} \simeq \bigoplus_{\substack{y\in D_f\\ y\neq\infty}} \bigoplus_{\chi^{ord_y(f)}=1} \mathcal{L}_{\chi(x)} \oplus \bigoplus_{\substack{\chi^{ord_\infty(f)}=1\\ \chi\neq 1}} \mathcal{L}_{\chi(x)};$$

($\mathcal{G}_f(0)$ est la restriction au groupe d'inertie I_0 de $\mathcal{G}_f$, alors que $\mathcal{G}_{f,0}$ est la fibre de $\mathcal{G}_f$ en 0 vue comme I_0-représentation triviale). D'autre part, en ∞, on a la décomposition

$$\mathcal{G}_f(\infty) \simeq \bigoplus_{z\in Z_f} \mathcal{L}_{\psi(f(z)x)} \otimes \mathcal{L}_{\chi_2(x)}, \tag{6}$$

de sorte que

$$\det(\mathcal{G}_f)(\infty) \simeq \mathcal{L}_{\psi(k_f\beta x)} \otimes \mathcal{L}_{\chi_2^{k_f}(x)},$$

avec $\beta = \frac{1}{k_f}\sum_{z\in Z_f} f(z) \in \mathbf{F}_p$. Ainsi le faisceau

$$\det(\mathcal{G}_f(1/2) \otimes \mathcal{L}_{\psi(-\beta x)} \otimes \mathcal{L}_{\chi_2^{k_f}(x)})$$

($\mathcal{G}_f(1/2)$ désigne le twist de Tate de $\mathcal{G}_f$ qui est pur de poids 0 et non pas une représentation de l'inertie en 1/2!) est lisse sur $\mathbf{G}_m \cup \{\infty\}$, modérément ramifié en 0 et pur de poids 0; il est donc géométriquement constant et de la forme $\alpha := t \in \mathbf{G}_m \to tr(Frob_t, \alpha) = \alpha^{\deg t}$, où $\alpha \in \overline{\mathbf{Q}}_\ell$ vérifie $|\alpha| = 1$ pour tout plongement de $\overline{\mathbf{Q}}_\ell$ dans $\mathbf{C}$. Notant $\mathcal{L}$ le faisceau pur de poids 0, $\mathcal{L} := \alpha^{-1/k_f} \otimes \mathcal{L}_{\psi(-\beta x)} \otimes \mathcal{L}_{\chi_2^{k_f}(x)}$, on a le lemme:

Lemme 2.1 *Il existe un faisceau $\mathcal{L}$ lisse sur $\mathbf{G}_m$ de rang 1 et de poids 0 tel que $\det(\mathcal{L} \otimes \mathcal{G}_f(1/2)) = \overline{\mathbf{Q}}_\ell$. Par conséquent, si nous notons $\mathcal{G}'_f := \mathcal{L} \otimes \mathcal{G}_f(1/2)$, on a $G_{arith}(\mathcal{G}'_f) \subset SL_{k_f}$.*

D'autre part pour p assez grand f (mod p) vérifie H.3. et d'après [Ka2] 7.9.6 on a $G^{0,der}_{geom}(\mathcal{G}_f) = SL_{k_f}$, on en déduit donc la

Proposition 2.2 (Katz) *Avec les notations précédentes on a les égalités*

$$SL_{k_f} = G^{0,der}_{geom}(\mathcal{G}'_f) = G_{geom}(\mathcal{G}'_f) = G_{arith}(\mathcal{G}'_f).$$

Nous montrons maintenant le premier résultat vraiment original de cette section. Notons $\mathcal{H}$ l'ensemble des racines $2(k_f-1)$-ièmes ou $2k_f$-ièmes de l'unité suivant que C_f contient ou ne contient pas β. Alors on a le

Théorème 2.3 *Soit $a \in \overline{\mathbf{F}}_p^* - \mathcal{H}$, on a l'égalité*

$$G_{geom}(\mathcal{G}'_f \oplus a^*\mathcal{G}'_f) = SL_{k_f} \times SL_{k_f} \subset GL_{2k_f}.$$

Corollaire 2.4 *Soit $a \notin \mathbf{F}_p \cap \mathcal{H}$, (ρ_1, ρ_2) un couple de représentations irréductibles de SL_{k_f} et ψ' un caractère additif de $\mathbf{F}_p$, on a les majorations*

$$\left| \sum_{t \in \mathbf{F}_p^*} tr(frob_t, \rho_1(\mathcal{G}'_f))\psi'(1/t) \right| \leq \dim \rho_1 (k_f + 1) p^{1/2}.$$

$$\left| \sum_{t \in \mathbf{F}_p^*} tr(frob_t, \rho_1(\mathcal{G}'_f))\overline{tr(frob_{at}, \rho_2(\mathcal{G}'_f))}\psi'(1/t) \right| \leq \dim \rho_1 \dim \rho_2 (k_f + 1) p^{1/2}.$$

Preuve. — Par le théorème précédent, le faisceau $\rho_1(\mathcal{G}'_f) \otimes \rho_2(a^*\mathcal{G}'_f)^\vee \otimes [-1]^*\mathcal{L}_{\psi'(x)}$ (resp. $\rho_1(\mathcal{G}'_f) \otimes [-1]^*\mathcal{L}_{\psi'(x)}$) (ces faisceaux sont définis sur $\mathbf{G}_m \otimes \mathbf{F}_p$) est géométriquement irréductible ($[-1]^*\mathcal{L}_{\psi'(x)}$ est de rang 1). Le corollaire résulte alors de la formule des traces de Lefschetz, des théorèmes fondamentaux de Deligne ([D1]), de la formule de Grothendieck-Ogg-Shafarevitch, ainsi que du Lemme 2.2 de [Mi] pour contrôler les conducteurs de Swan de $\rho_1(\mathcal{G}'_f) \otimes \rho_2(a^*\mathcal{G}'_f)^\vee \otimes [-1]^*\mathcal{L}_{\psi'(x)}$ (resp. $\rho_1(\mathcal{G}'_f) \otimes [-1]^*\mathcal{L}_{\psi'(x)}$).

◇

Preuve du Théorème 2.3

D'après la Proposition 2.2, il suffit de montrer l'inclusion

$$SL_{k_f} \times SL_{k_f} \subset G_{geom}(\mathcal{G}'_f \oplus a^*\mathcal{G}'_f).$$

On applique le critère de Goursat-Kolchin-Ribet ([Ka2] 1.8.2): d'après 2.2, il suffit de montrer que pour $a \notin \mathcal{H}$, et pour tout faisceau $\mathcal{L}$, lisse sur $\mathbf{G}_m$ de rang 1, il n'y a pas d'isomorphisme géométrique entre les faisceaux $\mathcal{G}'_f$ et $a^*\mathcal{G}'_f \otimes \mathcal{L}$ ou $a^*\mathcal{G}'^\vee_f \otimes \mathcal{L}$. Nous montrons que si $a \notin \mathcal{H}$ l'isomorphisme $\mathcal{G}'_f \simeq a^*\mathcal{G}'_f \otimes \mathcal{L}$ est impossible, la preuve pour $a^*\mathcal{G}'^\vee_f \otimes \mathcal{L}$ est similaire (remarquer que $a^*\mathcal{G}'^\vee_f = a^*\mathcal{G}'_{-f}$)... On va en fait montrer que les P_∞-représentations $\mathcal{G}'_{f,|P_\infty}$ et $a^*\mathcal{G}'_f \otimes \mathcal{L}_{|P_\infty}$ ne sont pas isomorphes : d'après (6) les sauts de $\mathcal{G}'_f$ et $a^*\mathcal{G}'_f$ pour la ramification sauvage à l'infini étant en 1, $\mathcal{L}$ étant de rang 1, on est dans l'un des deux cas suivants:

- $\mathcal{L}$ n'est pas sauvagement ramifié en ∞;
- $\mathcal{L}_{|P_\infty} \simeq \mathcal{L}_{\psi(\lambda x)}$.

Dans ce dernier cas, on aurait un isomorphisme entre P_∞-représentations

$$\bigoplus_{z\in Z_f} \mathcal{L}_{\psi((f(z)-\beta)x)} \simeq \bigoplus_{z\in Z_f} \mathcal{L}_{\psi((a(f(z)-\beta)+\lambda)x)} \tag{7}$$

soit, en prenant le déterminant, on aurait l'égalité

$$\sum_{z\in Z_f} (f(z)-\beta) = 0 = a\sum_{z\in Z_f} (f(z)-\beta) + k_f\lambda;$$

cela impose $\lambda = 0$ et on se trouve donc dans le premier cas. Dès lors, l'isomorphisme (7) implique que l'ensemble $C'_f := \{f(z)-\beta,\ z\in Z_f\}$ est stable par multiplication par a. On en déduit que a est une racine de l'unité d'ordre divisant k_f-1 ou k_f suivant que C'_f contient ou ne contient pas 0.

Remarque. — Si l'on se place dans le cadre du Théorème 1.2: on suppose f impaire, qui vérifie H.1. H.2. et H.3'. Des énoncés analogues aux précédents sont valables en utilisant la variante 7.9.7 de [Ka2], il reste à remplacer dans les énoncés précédents SL_{k_f} par Sp_{k_f}.

Distribution simultanée de sommes conjuguées

Soient $0 < a_1 < a_2, \ldots < a_n$ n entiers positifs fixés tous distincts, on suppose de plus que p est assez grand de sorte que, pour tout $1 \le i < j \le n$, le quotient $a_i\overline{a_j} \pmod p$ n'est pas une racine $2k_f$-ième où $2(k_f-1)$-ième de l'unité (il suffit pour cela que $p > a_n^{2k_f}$). Soit $\mathcal{H}_{a_1,\ldots,a_n}$ l'ensemble des racines dans $\overline{\mathbf{F}}_p^*$ des polynômes

$$(a_iX)^{2k_f} - a_j^{2k_f} \ (\mathrm{mod}p),\ 1\le i,j\le n,$$

si C'_f ne contient pas 0; et

$$(a_iX)^{2(k_f-1)} - a_j^{2(k_f-1)} \ (\mathrm{mod}p),\ 1\le i,j\le n,$$

si C'_f contient 0. Alors $\sharp\mathcal{H}_{a_1,\ldots,a_n} \le 2k_fn^2$, et on déduit de la preuve du Théorème 2.3 le

Théorème 2.5 *Avec les notations précédentes, si $a \notin \mathcal{H}_{a_1,\ldots,a_n}$, on a l'égalité*

$$G_{geom}(\bigoplus_{i=1}^n \mathcal{G}'_{a_if} \oplus \bigoplus_{i=1}^n a^*\mathcal{G}'_{a_if}) = SL_{k_f}^{2n}.$$

Preuve. — En effet, l'hypothèse que p est $p > a_n^{2k_f}$ assure que pour $i\neq j$, le faisceau $\mathcal{G}'_{a_if}$ n'est pas géométriquement isomorphe (à un twist, par un faisceau de rang 1, près) aux faisceaux $\mathcal{G}'_{a_jf}$ et ${\mathcal{G}'}^\vee_{a_jf}$. L'hypothèse $a\notin\mathcal{H}_{a_1,\ldots,a_n}$ assure elle que pour tout $1\le i,j\le n$ $\mathcal{G}'_{a_if}$ n'est pas géométriquement isomorphe à un twist par un faisceau de rang 1 près aux faisceaux $a^*\mathcal{G}'_{a_jf}$ et $a^*{\mathcal{G}'}^\vee_{a_jf}$, le résultat s'en déduit alors par le critère de Goursat-Kolchin-Ribet.

$\diamond$

Corollaire 2.6 *Soit $a \notin \mathbf{F}_p \cap \mathcal{H}_{a_1,\ldots,a_n}$, $(\rho_1, \rho_2, \ldots, \rho_n)$ n représentations irréductibles de SL_{k_f} et ψ' un caractère additif de $\mathbf{F}_p$, on a les majorations*

$$\left|\sum_{t\in\mathbf{F}_p^*} \psi'(1/t) \prod_{i=i}^{n} tr(frob_t, \rho_i(\mathcal{G}'_{a_i f}))\right| \leq \dim\rho_1 \ldots \dim\rho_n (k_f+1)p^{1/2}.$$

$$\left|\sum_{t\in\mathbf{F}_p^*} \psi'(1/t) \prod_{i=i}^{n} tr(frob_t, \rho_i(\mathcal{G}'_{a_i f}))\overline{tr(frob_{at}, \rho_i(\mathcal{G}'_{a_i f}))}\right| \leq (\dim\rho_1 \ldots \dim\rho_n)^2 (k_f+1)p^{1/2}.$$

2.2 Les sommes de Kloosterman généralisées

Pour tout entier $k \geq 2$, Katz a construit par convolution itérée le faisceau de Kloosterman généralisé $\mathcal{K}l_k$; ce faisceau a les propriétés suivantes ([Ka1] 4.1.1, 11.0.2): on note, pour $a \in \mathbf{F}_p^*$, $\mathcal{K}l_{k,a} := a^*\mathcal{K}l_k$, alors

- *$\mathcal{K}l_{k,a}$ est lisse sur $\mathbf{G}_{\mathrm{m}} \otimes \mathbf{F}_p$, de rang k, et pur de poids 0.*
- *Pour tout $m \in \mathbf{F}_p^*$, on a* $\mathrm{tr}(\mathrm{Frob}_m, \mathcal{K}l_{k,a}) = \dfrac{Kl_k(am;p)}{p^{(k-1)/2}}$.
- *En 0, $\mathcal{K}l_{k,a}$ est modéré avec un seul bloc de Jordan.*
- *En ∞, $\mathcal{K}l_{k,a}$ est totalement sauvage, avec pour unique pente $1/k$, et* $\mathrm{Swan}_\infty(\mathcal{K}l_{k,a}) = 1$
- $\det \mathcal{K}l_{k,a}$ *est trivial.*
- *Il existe un isomorphisme de $\overline{\mathbf{Q}}_\ell$-faisceaux lisses*

$$\mathcal{K}l_{k,(-1)^k a} \widetilde{\to} \mathcal{K}l_{k,a}^\vee.$$

- *Si k est impair, on a $G_{geom}(\mathcal{K}l_{k,a}) = SL_k$*
- *Si k est pair, on a*
  1. *il existe un accouplement parfait, alterné,*

$$(\ ,\ ) : \mathcal{K}l_{k,a} \otimes \mathcal{K}l_{k,a} \to \overline{\mathbf{Q}}_\ell$$

  de faisceaux lisses sur $\mathbf{G}_{\mathrm{m}} \otimes \mathbf{F}_p$.
  2. *$G_{geom}(\mathcal{K}l_{k,a}) = Sp_k$.*

De manière analogue au Théorème 2.3, on montre le

Théorème 2.7 . — *Si k est pair, et si $a \neq 1$, alors, le groupe de monodromie géométrique du faisceau $\mathcal{K}l_k \oplus \mathcal{K}l_{k,a}$ est $Sp_k \times Sp_k$.*

Si k est impair et si $a \neq \pm 1$ alors, le groupe de monodromie géométrique du faisceau $\mathcal{K}l_k \oplus \mathcal{K}l_{k,a}$ est $SL_k \times SL_k$.

Preuve. — On applique à nouveau le critère de *Goursat-Kolchin-Ribet*. Il suffit donc de montrer que

Pour $a \neq 1$ (si k est pair) ou pour $a \neq \pm 1$ (si k est impair), pour tout faisceau, $\mathcal{L}$, lisse sur $\mathbf{G}_{\mathrm{m}} \otimes \overline{\mathbf{F}}_p$, de rang 1, il n'existe pas d'isomorphisme de faisceaux lisses sur $\mathbf{G}_{\mathrm{m}} \otimes \overline{\mathbf{F}}_p$ de la forme suivante

$$\mathcal{K}l_k \otimes \mathcal{L} \simeq \mathcal{K}l_{k,a}, \quad \mathcal{K}l_k^\vee \otimes \mathcal{L} \simeq \mathcal{K}l_{k,a}.$$

Supposons que $\mathcal{L}$ existe, ainsi que l'un des deux isomorphismes ci-dessus; alors $\mathcal{L}$ est modérément ramifié en ∞ : sinon, $\mathcal{L}$ étant de rang 1 et son conducteur de *Swan* en ∞ étant un entier, le seul saut de $\mathcal{L}$ en ∞ serait entier, donc ≥ 1; or, le seul saut des faisceaux $\mathcal{K}l_{k,a'}$ en ∞ est $1/k < 1$, ce serait incompatible avec l'isomorphisme précédent.

Le résultat suivant ([Ka1] 10.4.1 p. 171) est une généralisation du calcul de conducteurs de *Swan*, établi pour $k = 2$ au Lemme 2.4 de [Mi]:

$$\mathrm{Swan}_\infty(\mathcal{K}l_{k,a} \otimes \mathcal{K}l_{k,a'}) = k - 1 \qquad si\ a = (-1)^k a'$$

$$\mathrm{Swan}_\infty(\mathcal{K}l_{k,a} \otimes \mathcal{K}l_{k,a'}) = k \qquad si\ a \neq (-1)^k a'$$

On en déduit, avec la relation $\mathcal{K}l_{k,a}^\vee \simeq \mathcal{K}l_{k,(-1)^k a}$, les égalités suivantes

$$\mathrm{Swan}_\infty(\mathcal{K}l_k^\vee \otimes \mathcal{K}l_k) = k - 1\ et\ \mathrm{Swan}_\infty(\mathcal{K}l_k^\vee \otimes \mathcal{K}l_{k,a}) = k\ si\ a \neq 1.$$

Elles montrent que le premier isomorphisme $\mathcal{K}l_k \otimes \mathcal{L} \simeq \mathcal{K}l_{k,a}$ est impossible pour $a \neq 1$, car on aurait ($\mathcal{L}$ étant modéré en ∞)

$$\begin{aligned} k \quad &= \mathrm{Swan}_\infty(\mathcal{K}l_k^\vee \otimes \mathcal{K}l_{k,a}) \\ &= \mathrm{Swan}_\infty(\mathcal{K}l_k^\vee \otimes \mathcal{K}l_k \otimes \mathcal{L}) \\ &= \mathrm{Swan}_\infty(\mathcal{K}l_k^\vee \otimes \mathcal{K}l_k) = k - 1. \end{aligned}$$

Dans le cas où k est pair, $\mathcal{K}l$ est isomorphe à son dual, ce qui montre du même coup, l'impossibilité du second isomorphisme.

Dans le cas où k est impair, l'égalité $\mathrm{Swan}_\infty(\mathcal{K}l \otimes \mathcal{K}l_{k,a}) = k$ si $a \neq -1$ permet de prouver, de même, l'impossibilité du second isomorphisme.

◇

On en déduit le corollaire suivant

Corollaire 2.8 . — *Si k est pair et $a \neq 1$, le groupe de monodromie géométrique du faisceau*

$$[k]^*\mathcal{K}l_k \oplus [k]^*\mathcal{K}l_{k,a},$$

est isomorphe à $Sp_k \times Sp_k$.

Si k est impair et $a \neq \pm 1$, le groupe de monodromie géométrique du faisceau

$$[k]^*\mathcal{K}l_k \oplus [k]^*\mathcal{K}l_{k,a}$$

est isomorphe à $SL_k \times SL_k \subset GL_{2k}$.

Preuve. — Si $p > k$, le morphisme $x \to x^k$ définit un revêtement étale de $\mathbf{G}_m$ de degré k et le faisceau $[k]^*\mathcal{K}l_k \oplus [k]^*\mathcal{K}l_{k,a}$ est simplement la restriction du faisceau $\mathcal{K}l_k \oplus \mathcal{K}l_{k,a}$ à un sous groupe d'indice k du groupe fondamental géométrique de $\mathbf{G}_m$; or $Sp_k \times Sp_k$ et $SL_k \times SL_k$ sont connexes, il n'admettent pas de sous groupes d'indices finis non triviaux et par conséquent $G_{geom}([k]^*\mathcal{K}l_k \oplus [k]^*\mathcal{K}l_{k,a})$ est le plus gros possible et vaut suivant la parité de k, $Sp_k \times Sp_k$ ou $SL_k \times SL_k$.

◇

Comme précédemment, on déduit de ce corollaire le

Corollaire 2.9 *Soit $a \neq \pm 1$; soit (ρ_1, ρ_2) un couple de représentations irréductibles de SL_k si k est impair ou de Sp_k si k est pair et ψ' un caractère additif de $\mathbf{F}_p$, alors on a les majorations*

$$\left|\sum_{t\in\mathbf{F}_p^*} tr(frob_{t^k}, \rho_1(\mathcal{K}l_k))\psi'(1/t)\right| \leq \dim \rho_1 (k+1)p^{1/2}.$$

$$\left|\sum_{t\in\mathbf{F}_p^*} tr(frob_{t^k}, \rho_1(\mathcal{K}l_k))\overline{tr(frob_{at^k}, \rho_2(\mathcal{K}l_k))}\psi'(1/t)\right| \leq \dim \rho_1 \dim \rho_2 (k+1)p^{1/2}.$$

3 Un résultat de crible

Dans cette section nous rappelons sans démontration un résultat de crible qui est démontré implicitement dans [Mi] (Cor 2.9, Cor 2.11, Prop. 3.2) et que nous donnons en toute généralité dans l'espoir qu'elle puisse avoir d'autres applications.

On considère la situation suivante: on se donne $g(m)$ une fonction de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ à valeurs complexes majorée par 1 en valeur absolue, que l'on prolonge à $\mathbf{N}$ tout entier par périodicité. Soient C, C' et H, trois réels positifs, on considère les propriétés suivantes sur g:

Propriété I(C). — *On dit que g vérifie la propriété $I(C)$, si, pour tout caractère additif (trivial ou non), ψ, de $\mathbf{F}_p$, on a la majoration*

$$|\sum_{m\in\mathbf{F}_p} g(m)\psi(m)| \leq Cp^{1/2}.$$

Propriété II(C', H). — *On dit que g vérifie la propriété $II(C', H)$, s'il existe un ensemble $\mathcal{H}$ de $\mathbf{F}_p^*$ de cardinal au plus H, tel que pour tout caractère additif, ψ, de $\mathbf{F}_p$, et pour tout élément n de $\mathbf{F}_p^*$, $n \notin \mathcal{H}$, on a la majoration*

$$|\sum_{m\in\mathbf{F}_p} g(m)\overline{g(mn)}\psi(m)| \leq C'p^{1/2}.$$

On a alors le Théorème très général suivant:

Théorème 3.1 . — *Soient C, C', H trois constantes positives, x un réel positif, alors, pour tout p nombre premier compris entre x et $2x$ et toute fonction g de $\mathbf{F}_p$ majorée en valeur absolue par 1, qui vérifie les propriétés I(C) et II(C',H), on a la majoration (uniforme en p)*

$$\sum_{\substack{x\leq q<2x\\ q\neq p}} g(q) \ \ll_{C,C',H} \ \frac{x\log\log x}{\log^2 x}.$$

De plus la constante impliquée dans le symbole de Landau ci-dessus est de la forme $O(C + H^{1/2} + C'^{1/2})$.

La preuve de cette proposition suit celle de la proposition 3.2 de [Mi], il suffit dans la preuve de remplacer les expressions $\mathrm{sym}_i(\theta'_{p,q})$ par $g(q)$ et d'utiliser les propriétés I(C) et II(C', H) pour montrer les analogues des Corollaires 2.9 et 2.10 de *loc. cit.*

D'après le Corollaire 2.4, pour toute représentation irréductible ρ_1 de SL_{k_f}, la fonction de $\mathbf{F}_p^*$ définie par

$$g(m) = \frac{tr(frob_{1/m}, \rho_1(\mathcal{G}'_f))}{\dim \rho_1}$$

vérifie les hypothèses I(C) et II(C', H) avec $C = C' = k_f + 1$, et $H = 2k_f + 1$ dès que p est assez grand (dépendant seulement de f).

De même, le corollaire 2.9 implique que pour toute représentation ρ_1 de SL_k si k est impair ou de Sp_k si k est pair, la fonction définie par

$$g(m) = \frac{tr(frob_{1/m^k}, \rho_1(\mathcal{K}l_k))}{\dim \rho_1}$$

vérifie les hypothèses I(C) et II(C', H) avec $C = C' = k + 1$, et $H = 2k + 1$ dès que p est assez grand (dependant seulement de k).

4 Démonstration du Théorème 1.1

On se contentera ici de montrer le Théorème 1.1, la preuve des Théorèmes 1.2, 1.3 et 1.4 est tout à fait similaire (il suffit d'utiliser dans la section précédente les corollaires 2.9 et 2.6 à la place du Corollaire 2.4).

Choisissons un plongement de $\overline{\mathbf{Q}}_\ell$ dans $\mathbf{C}$ et K un compact maximal de $SL_{k_f}(\mathbf{C})$. Comme cela est expliqué dans [Ka1] Chap. 3, pour $t \in \mathbf{F}_p^*$ la partie semi-simple du frobenius en t agissant sur $\mathcal{G}'_f$ définit de manière unique une classe de conjugaisons de K que l'on note $\theta_{f,p,t}$; d'après Deligne ([D1]) et le Théorème de Katz 2.2, quand $p \to +\infty$, la famille des "angles" $\{\theta_{f,p,t}\}_{t=1\ldots p-1}$ devient équidistribuée sur $K^\natural$ relativement à la mesure de Sato-Tate $\mu_{ST,SL_{k_f}}$. Comme conséquence directe de la section précédente nous avons la Proposition 4.1 où la variable t est assujettie à décrire des nombres premiers.

Proposition 4.1 . — *On adopte les notations et les hypothèses du Théorème 1.1. Quand $x \to +\infty$ et uniformément pour tout nombre premier $x \leq p < 2x$, les $x/\log x + o(x/\log x)$ classes de conjugaisons $\{\theta_{f,p,\overline{q}}\}_{x\leq q<2x}$ deviennent équidistribués sur $K^\natural$ relativement à la mesure $\mu_{ST,K}$: autrement dit, pour tout sous-ensemble mesurable $\mathcal{A} \subset K^\natural$, on a l'égalité*

$$|\{x \leq q < 2x,\ q \neq p,\ \theta_{f,p,\overline{q}} \in \mathcal{A}\}| = (\mu_{ST,K}(\mathcal{A}) + o(1))\frac{x}{\log x},\ x \to +\infty;$$

Cette égalité est uniforme en $x \leq p < 2x$.

En effet par le théorème de Peter-Weyl, il suffit de montrer que pour toute représentation irréductible ρ de SL_{k_f} on a

$$\sum_{x\leq q<2x,\ q\neq p} tr(\rho(\theta_{f,p,\overline{q}})) = o(\frac{x}{\log x}),\ x \to +\infty;$$

c'est précisement ce qui a été démontré dans la section précédente et on a même une majoration en $O_{k_f}(\dim \rho \frac{x \log\log x}{\log^2 x})$...

Soient maintenant A et B deux ensembles mesurables de $K^\natural$, notons

$$\mathcal{C}^A(x) = \{(p,q)|\ p \neq q,\ x \leq p,q < 2x,\ \theta_{f,p,\overline{q}} \in A\}$$
$$\mathcal{D}^B(x) = \{(p,q)|\ p \neq q,\ x \leq p,q < 2x,\ \theta_{f,q,\overline{p}} \in B\}.$$

D'après la proposition précédente, on a les égalités

$$|\mathcal{C}^A(x)| = (\mu_{ST,K}(A) + o(1))\frac{x^2}{\log^2 x},\ |\mathcal{D}^B(x)| = (\mu_{ST,K}(B) + o(1))\frac{x^2}{\log^2 x};$$

et on a donc l'inégalité

$$|\mathcal{C}^A(x) \cap \mathcal{D}^B(x)| \geq (\mu_{ST,K}(A) + \mu_{ST,K}(B) - 1 + o(1))\frac{x^2}{\log^2 x}.$$

Choisissons maintenant $A = B = \{k \in K^\natural,\ |tr(std(k))| > \alpha(SL_{k_f}, std) - \epsilon\}$, par définition de $\alpha(SL_{k_f}, std)$ on a donc

$$|\mathcal{C}^A(x) \cap \mathcal{D}^B(x)| \gg \frac{x^2}{\log^2 x}.$$

Par définition de $\mathcal{G}'_f$, on a l'égalité

$$|tr(\theta_{f,p,\overline{q}})| = \frac{|S_f(\overline{q}; p)|}{p^{1/2}},$$

d'autre part, on a la relation de multiplicativité croisée $S_f(1; pq) = S_f(\overline{q}; p)S_f(\overline{p}; q)$, de sorte que pour $(p, q) \in \mathcal{C}^A(x) \cap \mathcal{D}^B(x)$ on a la minoration (1). La majoration (2) s'obtient de même en prenant $A = \{k \in K^\natural,\ |tr(std(k))| \leq \epsilon\}$ et $B = K^\natural$.

Le Théorème 1.3 s'obtient de même en utilisant, cette fois, la relation de multiplicativité croisée

$$Kl_k(1; pq) = Kl_k(\overline{q}^k; p)Kl(\overline{p}^k; q).$$

Références

[D1] P. DELIGNE. — *La conjecture de Weil II*, Publ.Math.IHES 52 (1981), 313-428.

[D2] P. DELIGNE. — *Application de la formule des traces aux sommes trigonométriques*, SGA 4 1/2, Springer Lecture Notes in Math. 569, Springer-Verlag (1977).

[DFI] W. DUKE, J.B. FRIEDLANDER and H. IWANIEC. — *Equidistribution of roots of quadratic congruences of prime moduli*, Annals of Math. 141 (1995), 423-441.

[G] P.X. GALLAGHER. — *The large sieve and probabilistic galois theory*, Proc. Symp. Maths. 23 (1973), 91-101.

[HB-P] D.R. HEATH-BROWN and S.J. PATTERSON. — *The distribution of Kummer Gauss sums at prime arguments*, J. Reine Angew. Math. 310 (1979), 111-130.

[Ka1] N.M. KATZ. — *Gauss Sums, Kloosterman Sums and Monodromy Groups,* Annals of Maths. Studies 116, PUP.

[Ka2] N.M. KATZ. — *Exponential sums ans differential equations,* Annals of Maths. Studies 124, PUP.

[Ka3] N.M. KATZ. — *Exponential sums over finite fields and differential equations over the complex numbers: some interactions,* Bull. Am. Math. Soc. vol 23, p. 269.

[Mi] P. MICHEL. — *Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman I*, Invent. Math. 121, (1995) 61-78.