ANNALES

DE

L'INSTITUT FOURIER

Étienne FOUVRY & Philippe MICHEL

À la recherche de petites sommes d'exponentielles

Tome 52, n° 1 (2002), p. 47-80.

<http://aif.cedram.org/item?id=AIF_2002__52_1_47_0>

Ann. Inst. Fourier, Grenoble
52, 1 (2002), 47–80

À LA RECHERCHE DE PETITES SOMMES D'EXPONENTIELLES

par É. FOUVRY et P. MICHEL (*)

I. Introduction.

I.1. Énoncé des résultats dans le cas général.

Soit f une fraction rationnelle à coefficients dans $\mathbb{Z}$, qu'on suppose normalisée de sorte que $f = P/Q$, P et Q étant deux polynômes premiers entre eux, dont les coefficients sont premiers entre eux. Soit $n \geqslant 1$ un entier sans facteur carré. Pour m entier vérifiant $(m,n) = 1$, on considère la famille de sommes trigonométriques

$$S_f(m;n) := \sum_{\substack{x \in \mathbb{Z}/n\mathbb{Z} \\ (Q(x),n)=1}} e\Big(\frac{mP(x)\overline{Q(x)}}{n}\Big),$$

où, comme de coutume, $\overline{a}$ désigne, dans la fraction $\frac{\overline{a}}{n}$ ou dans une congruence modulo n, l'inverse de a modulo n lorsque $(a,n) = 1$, et $e(.)$ désigne le caractère additif, $z \mapsto \exp(2\pi i z)$. Plus généralement, pour χ caractère de Dirichlet modulo n, on considère la somme

$$S_f^{\chi}(m;n) := \sum_{\substack{x \in \mathbb{Z}/n\mathbb{Z} \\ (Q(x),n)=1}} \chi(x) e\Big(\frac{mP(x)\overline{Q(x)}}{n}\Big).$$

(*) Recherche subventionnée par la NSF (DMS-97-2992), la Ellentuck Fund et par l'Institut Universitaire de France.
Mots-clés : Sommes d'exponentielles sur un corps fini – Sommes de Kloosterman et de Sali – Monodromie – Loi de Sato-Tate – Grand crible.
Classification math. : 11L05 – 11L07 – 11L20 – 11T23 – 14D05.

Rappelons que ces sommes vérifient une relation de multiplicativité croisée, qui dans le cas des sommes S_f, s'écrit comme

$$S_f(m;n_1n_2) = S_f(m\overline{n_1};n_2)S_f(m\overline{n_2};n_1), \quad \text{pour} \quad (n_1,n_2)=1, \tag{1.1}$$

et dans le cas de S_f^χ s'écrit

$$S_f^\chi(m;n_1n_2) = S_f^{\chi_1}(m\overline{n_2};n_1)S_f^{\chi_2}(m\overline{n_1};n_2), \quad \text{pour} \quad (n_1,n_2)=1, \tag{1.2}$$

où χ_1 et χ_2 sont les uniques caractères modulo n_1 et n_2 tels que $\chi = \chi_1\chi_2$.

Depuis Weil et la démonstration de l'hypothèse de Riemann pour les courbes sur les corps finis, on sait que pour tout p nombre premier assez grand et tout m premier à p, on a la majoration

$$|S_f(m;p)| \leqslant k_f p^{1/2}, \tag{1.3}$$

et

$$|S_f^\chi(m;p)| \leqslant k_f^\chi p^{1/2}, \tag{1.4}$$

avec

$$k_f = \max\big(\deg P, \deg Q\big) + \sharp\{\text{ racines distinctes de } Q\} - 1$$

et

$$k_f \leqslant k_f^\chi \leqslant k_f + 2$$

(voir [Del], par exemple). Les relations (1.1) et (1.3) entraînent donc la majoration

$$|S_f(m;n)| \leqslant k_f^{\omega(n)} n^{1/2} \quad \text{pour} \quad \mu(n) \neq 0 \text{ et } (m,n)=1, \tag{1.5}$$

(avec $\omega(n)$ et $\mu(n)$: nombre de facteurs premiers et fonction de Möbius de l'entier n) et une majoration similaire pour $|S_f^\chi(m;n)|$. L'objet de ce travail est de s'intéresser à l'existence de couples (m,n) tels que la valeur de $|S_f(m;n)|$ soit très petite, à savoir aussi loin que possible de la majoration (1.5). Ce problème est à deux paramètres, il est d'autant plus difficile qu'on fixe la valeur de m ou de n, ou qu'on restreint le nombre de facteurs premiers de l'entier n. Cette question s'inscrit dans le cadre naturel de la conjecture de Sato-Tate horizontale qui prédit l'existence d'une mesure régissant, à m fixé, la répartition des valeurs de

$$\frac{S_f(m;p)}{k_f\sqrt{p},}$$

dans le disque de rayon 1, lorsque p parcourt l'ensemble des nombres premiers. Cette conjecture est prouvée dans très peu de cas, à savoir pour $S_f(1;p)$ avec f polynôme de degré 1 (la somme correspondante

est alors constamment nulle), de degré 2 (S_f est alors une somme de Gauss quadratique), $f(X) = X^3$ (c'est une conséquence de la résolution par Heath-Brown et Patterson ([H-BP]) de la conjecture de Kummer) ou pour les cas s'y ramenant. Pour des f généraux, elle est toujours hors d'atteinte en particulier dans le cas très classique de la fraction rationnelle $f(X) = aX + b/X$, ($S_{aX+b/X}(m;p)$ est alors une somme de Kloosterman). Toutefois, grâce aux travaux de Katz ([K3], [K4]) on sait que si f vérifie les hypothèses H.1, H.2, H.3 (ou H.3′) énoncées dans les théorèmes 1.2 et 1.3 ci-dessous, l'ensemble de $p-1$ nombres

$$\frac{|S_f(m;p)|}{\sqrt{p}} \quad (1 \leqslant m \leqslant p-1),$$

devient équiréparti, sur $[0, k_f]$, selon une certaine mesure, lorsque p tend vers l'infini (loi de Sato-Tate verticale). Ces résultats de Katz sont à l'origine de travaux du deuxième auteur ([Mi1], [Mi2]) qui s'est intéressé à la taille des sommes $S_f(1;pq)$ pour p et q premiers distincts, et f une fraction rationnelle vérifiant les hypothèses génériques H.1, H.2, H.3 (ou H.3′). Il a ainsi prouvé qu'il y a une proportion positive de couples de premiers $(p,q), x < q < p < 2x$, $(x \to \infty)$, tels qu'on ait la minoration

$$|S_f(1;pq)| \gg_{k_f} \sqrt{pq},$$

prouvant ainsi, à la constante k_f^2 près, l'optimalité de la majoration

$$|S_f(1;pq)| \leqslant k_f^2 \sqrt{pq}.$$

Puisqu'il n'y a pas, en général, de relation entre $S_f(\overline{p};q)$ et $S_f(\overline{q};p)$, il n'est pas possible, par la méthode utilisée dans la suite de cet article pour les sommes de Salié, de donner la loi de répartition du rapport $S_f(1,pq)/k_f^2\sqrt{pq}$ pour $q < p \leqslant x$. Toutefois, on peut donner des résultats sur les valeurs extrêmement petites de $S_f(1;pq)$, pour des f très généraux. Étant donnée f, on cherche à prouver l'existence d'une constante $\beta = \beta_f$, telle qu'il existe une infinité de couples (p,q) vérifiant

$$|S_f(1;pq)| \leqslant \sqrt{pq}^{1-\beta}.$$

En fait, on verra que β peut être pris comme fonction de k_f uniquement. Pour le cas classique des sommes de Kloosterman, nous obtenons le

COROLLAIRE 1.1. — *Soit $f(X) = X + X^{-1}$, alors pour tout $\varepsilon > 0$, il existe une infinité de couples (p,q) de nombres premiers distincts, tels qu'on ait la majoration*

$$|S_f(1;pq)| \leqslant \sqrt{pq}^{1-\frac{1}{6}+\varepsilon}.$$

La même propriété est vraie pour $f(X)$ polynôme de degré 3 tel que $f'(X)$ n'ait pas de racine double.

Ce corollaire est un cas particulier des théorèmes 1.2 ou 1.3 ci-dessous, pour l'énoncé desquels nous fixons les notations suivantes : si f est une fraction rationnelle, on désigne par $Z(f')$ l'ensemble des zéros de f' et on pose $C_f := f(Z(f'))$. On montrera le

THÉORÈME 1.2. — *Soit $k \geqslant 2$ et soit f une fraction rationnelle telle que $k_f = k$ et vérifiant les hypothèses suivantes :*

H.1. *Les zéros de $f'(X)$ dans $\mathbb{P}^1(\mathbb{C})$ sont simples (autrement dit $\sharp Z(f') = k_f$),*

H.2. *f sépare les zéros de $f'(X)$ i.e. si z et z' appartiennent à $Z(f')$, on a l'implication $f(z) = f(z') \Rightarrow z = z'$ (autrement dit $\sharp C_f = \sharp Z(f')$),*

H.3. *On a l'implication*

$$\left.\begin{array}{c} s_1 - s_2 = s_3 - s_4 \\ \text{et} \\ s_1,\ s_2,\ s_3,\ s_4 \in C_f \end{array}\right\} \Longrightarrow \left\{\begin{array}{c} s_1 = s_3 \text{ et } s_2 = s_4 \\ \text{ou} \\ s_1 = s_2 \text{ et } s_3 = s_4. \end{array}\right.$$

Alors, pour tout $\varepsilon > 0$, il existe une infinité de couples (p, q) de nombres premiers distincts, tels qu'on ait la majoration

$$|S_f(1; pq)| \leqslant \sqrt{pq}^{1-\beta_k+\varepsilon},$$

avec

$$\beta_2 = \frac{1}{6}, \text{ et } \beta_k = \frac{2}{3(k^2+1)} \text{ pour } k \geqslant 3.$$

Rappelons que les conditions H.1, H.2 et H.3 sont précisément celles de ([K3], 7.10.5, 7.10.6) et on les retrouve dans ([Mi2], théorème 1.1). Le dernier théorème augmente la valeur de β_k pour des f spéciaux. On a le

THÉORÈME 1.3. — *Soit $k \geqslant 2$ et soit f une fraction rationnelle vérifiant l'égalité $k_f = k$ ainsi que les hypothèses* H.1 *et* H.2 *du théorème 1.2. On suppose en outre que f vérifie*

H.3′. *La fonction f est impaire et on a l'implication*

$$\left.\begin{array}{c} s_1 - s_2 = s_3 - s_4 \\ \text{et} \\ s_1,\ s_2,\ s_3,\ s_4 \in C_f \end{array}\right\} \Longrightarrow \left\{\begin{array}{c} s_1 = s_3 \text{ et } s_2 = s_4 \\ \text{ou} \\ s_1 = s_2 \text{ et } s_3 = s_4 \\ \text{ou} \\ s_1 = -s_4 \text{ et } s_2 = -s_3. \end{array}\right.$$

Alors, pour tout $\varepsilon > 0$, il existe une infinité de couples (p,q) de nombres premiers distincts, tels qu'on ait la majoration

$$|S_f(1;pq)| \leqslant \sqrt{pq}^{1-\beta_k+\varepsilon}, \quad \text{avec} \quad \beta_k = \frac{4}{3(k^2+k+2)}.$$

Les conditions H.1, H.2 et H.3′ sont les hypothèses de ([Mi2], théorème 1.2). Bien sûr, il est possible, dans chacun des théorèmes, de donner une minoration du cardinal de l'ensemble des couples (p,q) d'ordre de grandeur fixé, vérifiant l'inégalité demandée. On a voulu fournir la valeur la plus grande de β_k ; par notre méthode, elle est obtenue pour $p \asymp q^2$.

I.2. Remarques sur les hypothèses H.1, H.2, H.3 et H.3′.

On pourra se reporter à [Mi2] pour des exemples de fonctions f satisfaisant aux hypothèses des théorèmes 1.2 et 1.3 mais il est naturel de rendre plus significatives ces conditions et de cerner les champs d'application des théorèmes 1.2 et 1.3. On verra, au §II. 1, que les hypothèses H.1, H.2, H.3 (ou H.3′) impliquent qu'un certain groupe de monodromie géométrique est SL_k (ou Sp_k). Ces deux groupes ont respectivement, pour compacts maximaux, SU_k et USp_k. Pour $k = 2$, ces deux groupes coïncident, ce qui explique pourquoi on obtient la même valeur de β_2 dans chacun des théorèmes 1.2 et 1.3.

Remarquons ensuite l'implication

$$f = \frac{P}{Q} \text{ vérifie H.1} \Rightarrow \deg P > \deg Q \tag{1.6}$$

(il suffit de regarder l'ordre de ∞ comme zéro possible de f'). On a de même l'implication

$$f \text{ impaire vérifie H.1} \Rightarrow 2|k_f. \tag{1.7}$$

En effet, d'après (1.6), P et Q vérifient $\deg P > \deg Q$, avec $(P,Q) = 1$ et on envisage les deux cas :

- P pair et Q impair : $\deg P$ est pair, et Q a un nombre impair de racines distinctes, puisque 0 est racine d'ordre impair, donc k_f est pair.
- P impair et Q pair : $\deg P$ est impair et Q, qui ne s'annule pas en 0, a un nombre pair de racines distinctes, donc k_f est pair.

Remarquons maintenant l'implication

$$f \text{ impaire vérifie H.1, H.2 et H.3} \Rightarrow k_f = 2 \ ; \tag{1.8}$$

en effet, d'après (1.7), si un tel f vérifiait de plus $k_f > 2$, il vérifierait $k_f \geqslant 4$, et en raison de l'imparité de f, C_f comprendrait au moins 4 éléments distincts, notés s_1, $-s_1$, s_2 et $-s_2$, pour lesquels H.3 n'est pas vérifiée puisqu'on a $s_1 - (-s_2) = s_2 - (-s_1)$.

Par contre, on a trivialement

$$f \text{ impaire vérifie H.1, H.2 et } k_f = 2 \Rightarrow f \text{ vérifie H.3.} \tag{1.9}$$

Ainsi l'ensemble des f vérifiant les hypothèses des théorèmes 1.2 et 1.3 est égal à l'ensemble des f impaires vérifiant $k_f = 2$ et les hypothèses H.1 et H.2 (on verra plus bas que l'hypothèse H.2 est conséquence de H.1 et de la condition $k_f = 2$).

Signalons en outre que les théorèmes 1.2 et 1.3 renseignent simultanément sur les sommes $S_f(1;pq)$ dès que f vérifie H.1 et $k_f = 2$. En effet, puisque $k_f = 2$, on voit d'après l'implication (1.6), que f a deux allures possibles :

- $f = \frac{P}{Q}$ avec $\deg P = 3$ et $\deg Q = 0$. La fonction f est un polynôme du troisième degré $f(X) = aX^3 + bX^2 + cX + d$. Faisant le changement de variables
$$X = 3aY - \frac{b}{3a},$$
on a l'égalité
$$f(X) = 27a^4Y^3 + (3ac - b^2)Y + \frac{2b^3 - 9abc + 27a^2d}{27a^2},$$
ce qui donne pour tout n tel que $(3a, n) = 1$, la relation
$$|S_f(1;n)| = |S_g(1;n)|,$$
où g est le polynôme cubique impair $g(X) = 27a^4X^3 + (3ac - b^2)X$. Dans ce cas, signalons que la condition H.1 signifie que $f(X)$ et $g(X)$ ne sont pas de la forme $a(X - t)^3 + v$, la condition H.2 est toujours satisfaite, et il en est de même pour H.3 et H.3′, d'après (1.9). On peut donc appliquer le théorème 1.2 à f ou le théorème 1.3 à g.
- $f = \frac{P}{Q}$ avec $\deg P = 2$ et $\deg Q = 1$. On écrit donc $f(X) = aX + b + c/(X + u)$ avec a, b, c et u sont des constantes avec $ac \neq 0$. Notons qu'une telle fonction vérifie toujours H.1, H.2 et H.3. On fait le changement de variables $X = Y - u$ et on parvient à l'égalité
$$|S_f(1;n)| = |S_g(1;n)|,$$

avec $g(X) = aX + c/X$. Cette fonction est impaire, vérifie H.1, H.2 et H.3′. Le théorème 1.3 s'applique aussi à la fonction g.

Pour terminer, mentionnons qu'on dispose de résultats similaires pour des sommes de Kloosterman multidimensionnelles (*cf.* [K2] pour leur étude détaillée)

$$\mathrm{Kl}_k(1;pq) = \sum_{\substack{x_1,\ \ldots,x_k \pmod{pq} \\ x_1 x_2 \ \ x_k \equiv 1 \pmod{pq}}} e\Big(\frac{x_1 + \ldots + x_k}{pq}\Big);$$

ainsi, pour tout ε on a la majoration $|\mathrm{Kl}_k(1;pq)| \leqslant \sqrt{pq}^{k-1-\beta_k+\varepsilon}$ pour un infinité de couples (p,q) de nombres premiers distincts, l'exposant β_k étant celui du théorème 1.2 si k est impair et celui du théorème 1.3 si k est pair.

I.3. Le cas particulier des sommes de Salié.

L'étude analogue pour les sommes $S_f^\chi(1;p)$ nécessite davantage de précautions dans la présentation, puisque le caractère χ dépend de p. Toutefois, si à chaque p, on associe de façon naturelle un caractère χ, on peut, là aussi, rechercher la répartition des rapports

$$\frac{S_f^\chi(1;p)}{k_f^\chi \sqrt{p}},$$

lorsque $p \to \infty$. Lorsque χ est le caractère de Legendre modulo p ($p \geqslant 3$) et que $f(X) = X + 1/X$, il s'agit d'une somme de Salié et la répartition du rapport précédent est connue : en effet le lemme 3.1 ci-dessous entraîne que le rapport

$$\frac{S_{X+1/X}^\chi(1;p)}{2\sqrt{p}}$$

se répartit, lorsque $p \to \infty$, suivant la mesure $\frac{1}{2}(\delta_1 + \delta_i)$, ($\delta_\alpha$ est la mesure de Dirac au point α).

Le cas où $f(X) = X - 1/X$ est lui aussi connu, c'est une conséquence triviale du résultat profond de Duke, Friedlander et Iwaniec, concernant l'équirépartition des racines de l'équation $n^2 + 1 \equiv 0$ modulo p, pour p tendant vers l'infini ([DFI]). On voit que le rapport

$$\frac{S_{X-1/X}^\chi(1;p)}{2\sqrt{p}}$$

est équiréparti sur le segment $[-1,+1]$, suivant la mesure $\frac{1}{2}\Big(\delta_0+\frac{1}{\pi}\frac{\mathrm{d}x}{\sqrt{1-x^2}}\Big)$. En fait chacun des exemples précédents est relatif aux sommes de Salié, sommes qui ont le privilège d'avoir une expression assez explicite (voir Lemme 3.1). Pour terminer, rappelons que le cas $f(X)=X$, χ étant le caractère d'ordre cubique $(\ /\pi)_3$ où $p=\pi\overline{\pi}$ (avec $p\equiv 1$ modulo 3 et π primaire) est résolu dans [H-BP].

Nous nous concentrons maintenant sur les sommes de Salié

$$T(a,b;n)=\sum_{\substack{(x,n)=1\\ x \bmod n}}\Big(\frac{x}{n}\Big)e\Big(\frac{ax+b\overline{x}}{n}\Big),$$

où $n\geqslant 3$ est un entier impair sans facteur carré et $\big(\frac{\cdot}{n}\big)$ est le symbole de Jacobi correspondant. On a donc la relation $T(a,b;n)=S^{(\frac{\cdot}{n})}_{aX+b/X}(1;n)$ et la formule de multiplicativité croisée (1.2) devient alors

$$T(a,b;mn)=T(a\overline{n},b\overline{n};m)T(a\overline{m},b\overline{m};n) \tag{1.10}$$

pour $\mu^2(mn)=1$. On a vu précédemment qu'une somme de mesures de Dirac gouverne la répartition des valeurs des rapports $T(1,1;n)/2\sqrt{n}$, lorsque n est un nombre premier. Le premier théorème concerne la répartition de ce rapport lorsque n est produit de deux nombres premiers distincts. La mesure correspondante est alors continue. En réservant toujours les lettres p et q aux nombres premiers, on a le

THÉORÈME 1.4. — *Les deux ensembles de rapports*

$$\Big\{\frac{T(1,1;pq)}{4\sqrt{pq}};\ pq\equiv 1 \bmod 4,\ q<p\leqslant x\Big\}$$

et

$$\Big\{\frac{T(1,1;pq)}{4i\sqrt{pq}};\ pq\equiv 3 \bmod 4,\ \ q<p\leqslant x\Big\}$$

sont équirépartis sur $[0,1]$, *pour la mesure* $\frac{\mathrm{d}t}{\pi\sqrt{t(1-t)}}$, *lorsque* x *tend vers l'infini.*

Dans l'énoncé précédent, on a compté les couples de nombres premiers (p,q) sous la diagonale d'un carré. On peut se demander ce qu'il advient si on s'intéresse aux couples de nombres premiers sous l'hyperbole $pq\leqslant x$. Le résultat précédent de répartition des rapports est alors identique et est plus facile à montrer, car, par le théorème des nombres premiers, la plus grande part des couples consiste en des couples (p,q) avec q très petits par rapport à p c'est-à-dire $q\leqslant \exp\big((\log x)^{1-o(1)}\big)$. Il n'est pas nécessaire d'appliquer

des majorations de sommes de Kloosterman courtes (*cf.* Lemme 4.2 ci-dessous), un théorème de répartition en moyenne des nombres premiers dans les progressions arithmétiques de type Barban-Davenport-Halberstam suffit. Dans cet ordre d'idées, voir la remarque ([Mi1], p. 77–78).

Le dernier théorème concerne les valeurs extrêmement petites de $T(1,1;pq)$, pour $q < p$ et $q \to \infty$. Le lemme 3.1 montrera que $T(1,1;pq)$ n'est jamais nul, et le lemme 3.2 que, lorsque $pq \equiv 1$ modulo 4, la valeur minimale de cette somme est positive et peut être très proche de $\frac{\pi^2\sqrt{pq}}{4q^2}$. Nous étudions la fréquence de cet événement par le

THÉORÈME 1.5. — *Soit P et Q, deux réels vérifiant $P \geqslant Q$. Alors, pour $Q \to \infty$, on a les relations*

$$\sharp\left\{(p,q),\ pq \equiv 1 \bmod 4,\ P<p\leqslant 2P,\ Q<q\leqslant 2Q, \left|\frac{T(1,1;pq)}{4\sqrt{pq}} - \frac{\pi^2}{4q^2}\right| \leqslant \frac{100}{q^3}\right\}$$

$$= \frac{\log 2}{2}\cdot\frac{P}{\log P \log Q}(1+o(1)), \tag{1.11}$$

uniformément pour $Q^2 \leqslant P$, et

$$\sharp\left\{(p,q),\ pq \equiv 1 \bmod 4,\ P<p\leqslant 2P,\ Q<q\leqslant 2Q, \left|\frac{T(1,1;pq)}{4\sqrt{pq}} - \frac{\pi^2}{4q^2}\right| \leqslant \frac{100}{q^3}\right\}$$

$$\gg \frac{P}{\log P \log Q}, \tag{1.12}$$

uniformément pour $Q \leqslant P^{0,52}$.

Enfin, si, sous la forme donnée en (5.3), la conjecture d'Elliott-Halberstam est vraie, la relation (1.11) *est vraie, uniformément pour $Q \leqslant P^{1-\varepsilon}$, avec ε réel positif quelconque.*

Le cas où $pq \equiv 3$ modulo 4 est évidemment identique à condition de diviser par i la quantité $\frac{\pi^2}{4q^2}$ (voir Lemme 3.2). En choisissant, dans le théorème 1.5, relation (1.12), respectivement $Q = P^{0,52}$ et $Q = P^{1-\varepsilon}$, on a directement le

COROLLAIRE 1.6. — *Il existe une infinité d'entiers n ayant exactement deux facteurs premiers comptés avec multiplicité, tels qu'on ait*

$$|T(1,1;n)| \asymp (\sqrt{n})^{-\frac{7}{19}}.$$

Si, sous la forme donnée en (5.3), la conjecture d'Elliott-Halberstam est vraie, l'énoncé précédent reste vrai en remplaçant l'exposant $-\frac{7}{19}$ par $-(1-\varepsilon)$, avec ε réel positif quelconque.

Ce corollaire montre ainsi qu'il existe des sommes de Salié $T(1,1;pq)$ minuscules, en particulier de module inférieur à chaque terme de cette somme.

I.4. Remarques.

Peut-on améliorer la constante $\frac{7}{19}$, dans le corollaire 1.6, en se donnant plus de liberté en travaillant avec des entiers ayant exactement trois facteurs premiers? Apparemment ce cas est bien plus ardu, puisque, si $n = pqr$ avec p, q et r premiers, il faut, par la méthode présentée au §V, contrôler simultanément les parties fractionnaires de $\frac{\overline{pq}}{r}$, $\frac{\overline{pr}}{q}$ et $\frac{\overline{qr}}{p}$.

À la différence des sommes de Salié, il nous semble très difficile de prouver pour un f général (disons $f(X) = X + 1/X$), l'existence d'une infinité de couples de nombres premiers (p,q) vérifiant

$$|S_f(1;pq)| \leqslant 1.$$

Cette difficulté est due, d'une part à l'absence de lien entre $S_f(\overline{p},q)$ et $S_f(\overline{q};p)$, et d'autre part à l'apparente inefficacité de l'analyse de Fourier à détecter des éléments de trace minuscule dans $\mathrm{SU}_k(\mathbb{C})$ ou dans $\mathrm{USp}_k(\mathbb{C})$. Dans le même ordre d'idées, rappelons que toute somme de Kloosterman $S_{aX+b/X}(1;p)$ est un réel non nul. Il reste à trouver une minoration réaliste de la valeur absolue de cette somme. En effet, des raisonnements sur la norme de cette somme dans l'extension cyclotomique $\mathbb{Q}(\mathrm{e}^{\frac{2\pi\imath}{p}})/\mathbb{Q}$, conduisent, pour p suffisamment grand, à la minoration

$$|S_{aX+b/X}(1;p)| \geqslant p^{-c_0 p},$$

avec c_0 constante absolue strictement positive. Cette minoration semble bien loin de la réalité.

Pour conclure cette introduction, on rappelle ce qui est connu sur le problème de l'existence de très petites sommes de caractères multiplicatifs

$$\sum_{1\leqslant x\leqslant p} \chi(f(x)) \tag{1.13}$$

pour χ caractère modulo p et f polynôme à coefficients entiers. Lorsque $\deg f = 1$ cette somme est nulle; lorsque $\deg f = 2$ et χ est le caractère de Legendre, cette somme vaut $p-1$ ou -1, suivant que modulo p, f est ou n'est pas un carré parfait. Signalons que pour $\chi = (\frac{-}{p})$, la somme (1.13), lorsqu'elle est non nulle, vaut au moins 1 en valeur absolue. Les problèmes

intéressants commencent lorsque $\deg f = 3$ et χ symbole de Legendre. En effet la somme

$$\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \chi\Big(\frac{x^3+ax+b}{p}\Big)$$

s'interprète comme $-a_p(E)$, où $a_p(E)$ est l'habituelle quantité liée à la réduction modulo p de la courbe elliptique $E/\mathbb{Q}$ d'équation $y^2 = x^3 + ax + b$. La nullité de cette somme équivaut, pour p, à être un nombre premier supersingulier pour E. Dans le cas où E est CM, on sait, depuis Deuring [Deu], que, asymptotiquement, 50% des nombres premiers sont supersinguliers pour E. Par contre, si E n'est pas CM, l'existence d'une infinité de p supersinguliers a été prouvée par Elkies [E]. Toutefois la preuve de Elkies et de ses successeurs (voir [FM], par exemple) exhibe un ensemble de supersinguliers qui est bien loin d'avoir la densité conjecturée par Lang et Trotter [LT]. Enfin, l'existence de petites valeurs de la somme (1.13) pour des polynômes f de degré supérieur, est un domaine de recherches quasiment inexploré.

Remerciements. — Cet article a été écrit lors de deux séjours du deuxième auteur à l'Institute for Advanced Study pendant l'année 1999–2000 et l'automne 2000–2001. Il remercie cette institution pour son hospitalité et ses excellentes conditions de travail. Enfin, les auteurs remercient les rapporteurs de leurs judicieuses remarques.

II. Le cas général : théorèmes 1.2 et 1.3.

II.1. Présentation du cadre de travail.

Les lettres p et q désignent toujours des nombres premiers. Soit f une fraction rationnelle vérifiant les hypothèses des théorèmes 1.2 ou 1.3. Par (1.1) et (1.3), on cherche une majoration de la forme

$$|S_f(\overline{p};q)| \leqslant (pq)^{\frac{1-\beta}{2}} p^{-\frac{1}{2}}$$

pour β aussi grand que possible. Pour ce faire on utilisera les techniques d'équirépartition de sommes d'exponentielles développées par Katz ([K2], [K3]) et utilisées ensuite dans ([Mi1], [Mi2]). Pour chaque f vérifiant les hypothèses ci-dessus, pour tout nombre premier q assez grand, tout premier $\ell \neq q$, on construit un $\overline{\mathbb{Q}_\ell}$-faisceau de rang k, sur $\mathbb{P}^1_{\mathbb{F}_q}$, noté $\mathcal{S}_f$ qui vérifie les propriétés suivantes (*cf.* [K3], 7.9–7.10) :

- $\mathcal{S}_f$ est pur et de poids zéro,
- pour tout $a \in \mathbb{F}_q^\times$, on a
$$|\operatorname{tr}(\mathrm{Frob}_a \ ; \ \mathcal{S}_f)| = \frac{|S_f(\overline{a}; q)|}{\sqrt{q}},$$
- $\mathcal{S}_f$ est lisse sur $\mathbb{G}_{\mathbb{F}_q}^m$, sauvagement ramifié en 0, modérément ramifié en ∞,
- $\mathcal{S}_f$ est géométriquement irréductible, son groupe de monodromie géométrique $G_{\text{géom}}$ vaut SL_k si f vérifie H.1, H.2, H.3, ou Sp_k si f vérifie H.1, H.2, H.3′,
- les groupes de monodromie géométrique et arithmétique de $\mathcal{S}_f$ coïncident.

Remarque. — Il est bon de noter que le faisceau naïf $\mathcal{F}_f$ que l'on construit directement à partir de f par transformée de Fourier-Deligne-Laumon et qui vérifie l'égalité
$$\operatorname{tr}(\mathrm{Frob}_a \ ; \ \mathcal{S}_f) = -\frac{S_f(\overline{a}; q)}{\sqrt{q}},$$
ne satisfait pas en général la dernière des cinq propriétés énoncées ci-dessus. En effet pour forcer les groupes de monodromie géométrique et arithmétique à coïncider, il est nécessaire de tordre $\mathcal{F}_f$ par un faisceau de rang 1 de sorte que le déterminant du faisceau obtenu soit arithmétiquement trivial. Comme cela est expliqué dans [K3], 7.11–7.12 (voir aussi [K1], Cor. 13), cela est possible et on obtient alors un faisceau $\mathcal{S}_f$ qui n'est pas nécessairement unique et qui vérifie
$$\operatorname{tr}(\mathrm{Frob}_a \ ; \ \mathcal{S}_f) = \alpha_{f,q} \frac{S_f(\overline{a}; q)}{\sqrt{q}},$$
où $\alpha_{f,q}$ est un nombre complexe de module 1 qui dépend de la caractéristique. Ajoutons que sa détermination exacte est un problème subtil qui n'est pas résolu en général. Heureusement dans cet article, seules les normes des sommes nous intéressent.

Soit K un compact maximal de $G_{\text{géom}}(\mathbb{C})$ (on prendra pour K soit $\mathrm{SU}_k(\mathbb{C})$ pour le théorème 1.2, soit $\mathrm{USp}_k(\mathbb{C})$ pour le théorème 1.3) ; on note μ_H sa mesure de Haar, $K^\natural$ l'espace des classes de conjugaison, et μ_{ST} la mesure de Sato-Tate associée (l'image de μ_H par la projection canonique). Chaque classe de frobenius Frob_a pour $a \in \mathbb{F}_q^\times$, définit alors une classe de conjugaison $\theta_{a,q}^\natural \in K^\natural$, pour laquelle
$$|\operatorname{tr}(\theta_{a,q}^\natural)| = \frac{|S_f(\overline{a}; q)|}{\sqrt{q}}.$$

Dans cette situation, on a ([K3], 7.9, 7.10) :

THÉORÈME 2.1. — *Sous les hypothèses précédentes, quand $q \to \infty$, les classes de conjugaison $\{\theta_{a,q}^{\natural}\}_{a\in\mathbb{F}_q^\times} \subset K^{\natural}$, deviennent équiréparties pour la mesure de Sato-Tate μ_{ST}, i.e. pour toute fonction f, continue sur $K^{\natural}$, on a*

$$\lim_{q\to\infty} \frac{1}{q-1} \sum_{a\in\mathbb{F}_q^\times} f(\theta_{a,q}^{\natural}) = \int_{K^{\natural}} f(\theta^{\natural})\, \mathrm{d}\mu_{\mathrm{ST}}.$$

Exemple 2.2. — Si $f(X) = X + X^{-1}$, on a l'égalité $G_{\text{géom}} = \mathrm{SL}_2$ et $K^{\natural}$ s'identifie alors à l'intervalle $[0,\pi]$ muni de la mesure $\mu_{\mathrm{ST}} = \frac{2}{\pi}\sin^2\theta \mathrm{d}\theta$.

La suite de la preuve consiste en une exploitation du théorème 2.1 et des techniques de grand crible pour montrer l'existence d'une infinité de couples de premiers (p,q) tels que

$$\left|\frac{S_f(\overline{p};q)}{\sqrt{q}}\right| = |\operatorname{tr}(\theta_{p,q}^{\natural})| \leqslant \sqrt{pq}^{\,-\beta_k},$$

où β_k est positif et ne dépend que de k.

II.2. Majoration de sommes de Weyl I.

Soit ρ une représentation irréductible non triviale de $K = G_{\text{géom}}$ et $\dim\rho$ sa dimension. On considère la somme de Weyl suivante associée à ρ

$$W_\rho(P,Q) = \frac{1}{PQ} \sum_{\substack{P<p\leqslant 2P \\ p\neq q}} \sum_{Q<q\leqslant 2Q} \log p \log q\, \operatorname{tr}(\rho(\theta_{p,q}^{\natural})). \tag{2.1}$$

La majoration triviale de cette somme est $|W_\rho(P,Q)| \ll \dim\rho$. Décomposant les p en classes de congruence modulo q, on a pour chaque q $(Q < q \leqslant 2Q)$, la majoration

$$\left|\sum_{\substack{P<p\leqslant 2P \\ p\neq q}} \log p\, \operatorname{tr}(\rho(\theta_{p,q}^{\natural}))\right| \leqslant \frac{1}{q-1} \sum_{\chi \bmod q} |\theta(2P;\chi) - \theta(P;\chi)||S_\rho(\chi;q)|, \tag{2.2}$$

où χ parcourt l'ensemble des caractères complexes de $\mathbb{F}_q^\times$, et où on a posé

$$\theta(x;\chi) = \sum_{p\leqslant x} \log p\, \chi(p), \quad \text{et} \quad S_\rho(\chi;q) = \sum_{a\in\mathbb{F}_q^\times} \overline{\chi}(a) \operatorname{tr}(\rho(\theta_{a,q}^{\natural})).$$

On a alors le

LEMME 2.3. — *Pour toute représentation ρ irréductible et non triviale de $G_{\text{géom}}$, et pour tout caractère χ de $\mathbb{F}_q^\times$, on a la majoration*

$$|S_\rho(\chi;q)| \leqslant k \dim \rho \, \sqrt{q}.$$

Preuve. — Comme les groupes de monodromie géométrique et arithmétique de $\mathcal{S}_f$ coïncident, on peut former par composition le faisceau $\rho(\mathcal{S}_f)$, celui-ci est géométriquement irréductible, de même que $\rho(\mathcal{S}_f) \otimes \mathcal{L}_{\overline{\chi}}$, où $\mathcal{L}_{\overline{\chi}}$ est le $\overline{\mathbb{Q}_\ell}$-faisceau de rang 1, associé au caractère $\overline{\chi}$. Comme $\mathcal{L}_{\overline{\chi}}$ est modéré en 0 et ∞, la ramification sauvage de $\rho(\mathcal{S}_f)$ n'est pas modifiée par ce twist. Originellement ([K3], 7.9, 7.10), $\mathcal{S}_f$ n'est sauvagement ramifié qu'en 0, tous les sauts étant en 1. Le lemme se déduit alors de la formule des traces de Lefschetz, de la formule de Grothendieck-Ogg-Schafarevich et des bornes triviales pour le conducteur de Swan de $\rho(\mathcal{S}_f) \otimes \mathcal{L}_{\overline{\chi}}$ (voir par exemple [Mi1], Lemmes 2.0, 2.1, 2.2). □

Nous déduisons maintenant la

PROPOSITION 2.4. — *Soit ρ comme précédemment. Alors pour tout $Q \leqslant P$, on a la majoration*

$$W_\rho(P,Q) \ll k \dim \rho \Big(Q^{-\frac{1}{2}} + (Q/P)^{\frac{1}{2}} \Big) (\log P)^{\frac{9}{2}}.$$

Preuve. — Par le lemme 3.3 ci-dessous, on a la majoration

$$\sum_{D<d\leqslant 2D} \sum_{\substack{\chi \bmod d \\ \chi \text{ primitif}}} |\psi(P;\chi)| \ll (\log DP)^{\frac{7}{2}} \Big(P + D^{\frac{5}{4}} P^{\frac{3}{4}} + D^2 P^{\frac{1}{2}} \Big),$$

avec $\psi(x;\chi)$ défini en (3.2). Si on somme sur des modules q premiers, seul le caractère principal χ_0 modulo q n'est pas primitif. Insérant la majoration triviale $\psi(P;\chi_0) \ll P$ et la majoration habituelle $|\psi(P;\chi) - \theta(P;\chi)| \ll P^{\frac{1}{2}}$, on obtient finalement

$$\sum_{Q<q\leqslant 2Q} \log q \sum_{\chi \bmod q} |\psi(P;\chi)| \ll (\log PQ)^{\frac{7}{2}} \Big(PQ + P^{\frac{3}{4}} Q^{\frac{5}{4}} + P^{\frac{1}{2}} Q^2 \Big).$$

Il reste à regrouper (2.1), (2.2), le lemme 2.3 et l'inégalité précédente pour conclure la preuve de la proposition 2.4. □

II.3. Majoration de sommes de Weyl II.

On fixe g une fonction radiale sur $\mathbb{C}$, non nulle à valeurs dans $\mathbb{R}^+$, infiniment différentiable, ayant pour support le compact $\{z, |z| \leqslant 1\}$. Soit

$0 < \Delta < 1$ un paramètre. On considère la fonction centrale g_Δ sur K définie par

$$g_\Delta : \theta \to g\Big(\frac{\mathrm{tr}(\theta)}{\Delta}\Big).$$

Par abus de notation, on notera encore g_Δ la fonction sur $K^\natural$ correspondante. On a alors une décomposition en série de Fourier absolument et uniformément convergente ([Su], Chap. II, Thm 8.1)

$$g_\Delta(\theta) = \int_K g_\Delta(\theta')\mathrm{d}\mu_H(\theta') + \sum_\rho \widehat{g_\Delta}(\rho)\,\mathrm{tr}(\rho(\theta)),$$

où ρ parcourt l'ensemble des représentations irréductibles de K non triviales (donc de $G_{\text{géom}}$) et

$$\widehat{g_\Delta}(\rho) = \int_K g_\Delta(\theta')\overline{\mathrm{tr}(\rho(\theta'))}\mathrm{d}\mu_H(\theta').$$

Posons maintenant

$$W_{g_\Delta}(P,Q) = \frac{1}{PQ}\sum_{\substack{P<p\leqslant 2P\\ p\neq q}}\sum_{Q<q\leqslant 2Q} \log p\ \log q\ g_\Delta(\theta^\natural_{p,q}).$$

Remarquons que si on prouve la non nullité de cette somme, on déduit l'existence d'une somme $S_f(\overline{p};q)$ de module $\ll \Delta\sqrt{q}$. Par la proposition 2.4 on obtient, pour $P \geqslant Q$, la majoration

(2.3)

$$\Big|W_{g_\Delta}(P,Q) - (1+o(1))\int_K g_\Delta(\theta)\mathrm{d}\mu_H(\theta)\Big| \ll \|g_\Delta\|^\natural (\log Q)^{\frac{9}{2}}\Big(Q^{-\frac{1}{2}} + (Q/P)^{\frac{1}{2}}\Big)$$

où

$$\|g_\Delta\|^\natural = \sum_\rho \dim\rho\ |\widehat{g_\Delta}(\rho)|.$$

II.4. Estimation du terme principal.

Dans cette partie, on estime, en fonction de Δ, le terme principal de $W_{g_\Delta}(P,Q)$, à savoir

$$\int_K g_\Delta(\theta)\mathrm{d}\mu_H(\theta),$$

en distinguant suivant les valeurs de K. Pour cela, on a recours aux formules d'intégration de Weyl ([KS], Chap. 5).

- *Le cas* $K = \mathrm{USp}_k$.

On est dans le cadre des hypothèses du théorème 1.3, et, d'après (1.7), l'entier k est pair, on l'écrit sous la forme $2k$ dans le lemme suivant :

LEMME 2.5. — *Soit* $k \geqslant 1$. *On a l'encadrement*

$$\Delta \ll_{k,g} \int_{\mathrm{USp}_{2k}} g_\Delta(\theta) \mathrm{d}\mu_H(\theta) \ll_{k,g} \Delta.$$

Preuve. — On utilise la forme explicite des formules d'intégration de Weyl ([KS], 5.0.4) :

$$\int_{\mathrm{USp}_{2k}} g_\Delta(\theta)\mathrm{d}\mu_H(\theta) = \frac{1}{k!}\int_{[0,\pi]^k} g\Big(\frac{\sum_{j=1}^k \cos x_j}{\Delta}\Big) \times \Big(\prod_{i<j}(2\cos x_i - 2\cos x_j)\Big)^2 \prod_j \frac{2}{\pi}\sin^2 x_j \mathrm{d}x_j,$$

puis on fait le changement de variable $u_j = \cos x_j$, l'intégrale devient donc

$$\int_{\mathrm{USp}_{2k}} g_\Delta(\theta)\mathrm{d}\mu_H(\theta) = \frac{4^{\frac{k(k-1)}{2}}}{k!}\int_{[-1,1]^k} g\Big(\frac{\sum_{j=1}^k u_j}{\Delta}\Big) \times \Big(\prod_{i<j}(u_i - u_j)\Big)^2 \prod_j \frac{2}{\pi}\sqrt{1-u_j^2}\mathrm{d}u_j. \tag{2.4}$$

Pour majorer, on a trivialement la relation

$$\int_{\mathrm{USp}_{2k}} g_\Delta(\theta)\mathrm{d}\mu_H(\theta) \ll \int_{[-1,1]^k} g\Big(\frac{\sum_{j=1}^k u_j}{\Delta}\Big)\prod_j \mathrm{d}u_j = \Delta^k \int_{[-\frac{1}{\Delta},\frac{1}{\Delta}]^k} g\Big(\sum_{j=1}^k v_j\Big)\prod_j \mathrm{d}v_j,$$

dans cette dernière intégrale k-uple, on intègre d'abord par rapport à v_k, puisque g est à support compact, cette intégrale est en $O_g(1)$, puis on intègre par rapport aux autres variables, d'où

$$\int_{\mathrm{USp}_{2k}} g_\Delta(\theta)\mathrm{d}\mu_H(\theta) \ll \Delta^k(1/\Delta)^{k-1} \ll \Delta.$$

Pour la minoration, on part de la relation (2.4) et on rappelle que $g(x) > 0$ pour $|x| < 1$. Soient $(x_i)_{1\leqslant i\leqslant k}$ une suite de réels vérifiant

$$-1 + \frac{1}{2k^2} < x_1 < x_2 < \cdots < x_{k-1} < x_k < 1 - \frac{1}{2k^2}$$

$$x_{i+1} - x_i > \frac{1}{2k^2} \ (1 \leqslant i \leqslant k-1)$$

et

$$x_1 + \cdots + x_k = 0.$$

On désigne par $\mathcal{I}_j$ $(j = 1, \ldots, k-1)$ l'intervalle de centre x_j et de longueur $\frac{1}{10k^6}$. En raison de la construction précédente, on voit que pour Δ suffisamment petit et u_j fixés dans l'intervalle $\mathcal{I}_j$ $(1 \leqslant j \leqslant k-1)$, l'inéquation en l'inconnue u_k,

$$-\Delta/2 \leqslant u_1 + u_2 + \cdots + u_{k-1} + u_k < \Delta/2$$

admet pour solutions, un intervalle de longueur Δ, noté $\mathcal{J}_{u_1,\ldots,u_{k-1}}$ tel que

$$\mathcal{J}_{u_1,\ldots,u_{k-1}} \subset \Big[x_k - \frac{1}{9k^5}, x_k + \frac{1}{9k^5}\Big].$$

Il est alors facile de voir que si $(u_1, \ldots, u_{k-1})$ appartient à $\mathcal{I}_1 \times \cdots \times \mathcal{I}_{k-1}$ et si u_k appartient à $\mathcal{J}_{u_1,\ldots,u_{k-1}}$, la fonction à intégrer dans la partie droite de (2.4) est $\gg_{k,g} 1$ puisque les u_j ne sont pas trop proches les uns des autres ni trop proches de ± 1. Enfin, pour terminer la preuve de la minoration du lemme 2.5, il reste à vérifier que la mesure des $(u_1, \ldots, u_k)$ comme ci-dessus est $\gg_k \Delta$, ce qui est évident, puisque $\mathcal{J}_{u_1,\ldots,u_{k-1}}$ est de longueur Δ. □

- *Le cas* $K = \mathrm{SU}_k$, $(k \geqslant 3)$.

(En effet, puisqu'au lemme 2.5, a été traité le cas $\mathrm{USp}_2 = \mathrm{SU}_2$, on peut se restreindre au cas où $k \geqslant 3$).

LEMME 2.6. — *Pour* $k \geqslant 3$ *et* $k \neq 4$, *on a*

$$\Delta^2 \ll_{k,g} \int_{\mathrm{SU}_k} g_\Delta(\theta) \mathrm{d}\mu_H(\theta) \ll_{k,g} \Delta^2.$$

Pour $k = 4$, *on a*

$$\Delta^2 \ll_g \int_{\mathrm{SU}_4} g_\Delta(\theta) \mathrm{d}\mu_H(\theta) \ll_g \Delta^2 \log(1/\Delta).$$

Preuve. — Notons d'abord que, comme g est une fonction radiale, on a (voir par exemple [KS], Cor. 1.3.2)

$$\int_{\mathrm{SU}_k} g_\Delta(\theta) \mathrm{d}\mu_H(\theta) = \int_{\mathrm{U}_k} g_\Delta(\theta) \mathrm{d}\mu_H(\theta).$$

Pour le groupe U_k, la formule de Weyl donne ([KS], 5.0.3)

$$(2.5) \quad \int_{\mathrm{U}_k} g_\Delta(\theta) \mathrm{d}\mu_H(\theta) = \frac{1}{k!} \int_{[0,2\pi]^k} g\Big(\frac{\sum_{j=1}^k e^{ix_j}}{\Delta}\Big) \prod_{\ell<j} |e^{ix_\ell} - e^{ix_j}|^2 \prod_j \frac{\mathrm{d}x_j}{2\pi}.$$

Prouvons la majoration. Puisque $g(z) = 0$ pour $|z| > 1$, on a la relation

(2.6)
$$\int_{\mathrm{U}_k} g_\Delta(\theta)\mathrm{d}\mu_H(\theta) \ll_{k,g} \lambda\big(\{(x_1,\dots,x_k) \in [0,2\pi]^k, |e^{ix_1}+\dots+e^{ix_k}| \leqslant \Delta\}\big),$$

où λ est la mesure de Lebesgue. R. Cerf nous a aimablement fait remarquer que l'évaluation d'une telle mesure est un problème bien connu des probabilistes, sous le nom de *vol aléatoire* (voir [Sp], p. 104) par exemple). On a le

LEMME 2.7. — *Soit $n \geqslant 1$, $X_1,\dots,X_n$, n variables aléatoires indépendantes, à valeurs sur le cercle unité, telles que l'argument de chacune des X_i soit équiréparti entre 0 et 2π. Alors, pour tout $r > 0$, on a l'égalité*

$$\frac{1}{2}\Big(P\Big[\Big|\sum_{i=1}^n X_i\Big| < r\Big] + P\Big[\Big|\sum_{i=1}^n X_i\Big| \leqslant r\Big]\Big) = r\int_0^\infty J_1(rt)J_0^n(t)\mathrm{d}t,$$

où $J_\ell(t)$ est la fonction de Bessel d'ordre ℓ.

Ainsi, par (2.5) et le lemme 2.7, pour prouver la majoration du lemme 2.6, il suffit de montrer que l'intégrale

$$I_k(r) := r\int_0^\infty J_1(rt)J_0^k(t)\mathrm{d}t,$$

vérifie

$$I_k(r) \ll_k r^2, \quad k = 3 \text{ ou } k \geqslant 5 \tag{2.7}$$

et

$$I_4(r) \ll r^2\log(1/r), \tag{2.8}$$

lorsque r tend vers 0 (en fait on peut remplacer ces majorations par des équivalences mais nous n'en aurons pas besoin).

Rappelons quelques propriétés des fonctions de Bessel. On a ([EMOT], p. 4, p. 85)

LEMME 2.8. — *On a les relations*

$$J_0(x) = 1 - \frac{x^2}{4} + O(x^4), \quad J_1(x) = \frac{x}{2} + O(x^3) \ (x \to 0) \tag{2.9}$$

$$\begin{aligned} &J_0(x) \ll \min(1, x^{-\frac{1}{2}}),\\ &J_1(x) \ll \min(x, x^{-\frac{1}{2}}),\\ &J_1'(x) = J_0(x) - J_1(x)/x \ (x > 0) \end{aligned} \tag{2.10}$$

$$J_0(x) = \sqrt{\frac{2}{\pi}} x^{-\frac{1}{2}} \cos\left(x - \frac{\pi}{4}\right) + O(x^{-\frac{3}{2}}) \ (x \to \infty). \tag{2.11}$$

D'abord, par (2.10), on a $J_0(x) \ll 1$ et $J_1(rx) \ll rx$, ce qui donne la majoration

$$r \int_0^1 J_1(rx) J_0^k(x) \mathrm{d}x \ll r^2. \tag{2.12}$$

Il reste à étudier

$$I_k'(r) = r \int_1^\infty J_1(rx) J_0^k(x) \mathrm{d}x. \tag{2.13}$$

Pour majorer cette intégrale lorsque $k \geqslant 5$, on utilise le fait que $J_0(x)$ tend vers 0 à l'infini : par (2.10), on a $J_0(x) \ll x^{-\frac{1}{2}}$ et $J_1(rx) \ll rx$, ce qui donne

$$I_k'(r) \ll r^2 \quad (k \geqslant 5). \tag{2.14}$$

Pour $k = 3$ on utilise les oscillations de la fonction J_0 à l'infini (voir (2.11)), sous la forme

$$J_0^3(x) = \left(\frac{2}{\pi}\right)^{\frac{3}{2}} x^{-3/2} \cos^3\left(x - \frac{\pi}{4}\right) + O(x^{-5/2}). \tag{2.15}$$

Le terme d'erreur de (2.15) reporté dans (2.13) donne une contribution en $O(r^2)$, ce qui est acceptable. Pour la contribution du terme principal de (2.15), on écrit

$$\cos^3\left(x - \frac{\pi}{4}\right) = \sum_{j=-3}^{j=3} a_j e^{ijx},$$

où les a_j sont des nombres complexes tels que $a_0 = 0$. On est donc ramené à traiter des intégrales oscillantes

$$K_j(r) := r \int_1^\infty J_1(rx) x^{-3/2} e^{ijx} \mathrm{d}x, \ (j \neq 0).$$

Une intégration par parties donne

$$K_j(r) = \left[r J_1(rx) x^{-3/2} (ij)^{-1} e^{ijx} \right]_1^\infty - r \int_1^\infty \left(r J_1'(rx) x^{-3/2} - (3/2) J_1(rx) x^{-5/2} \right) (ij)^{-1} e^{ijx} \mathrm{d}x,$$

puis (2.9) et (2.10) fournissent $J_1'(x) \ll 1$, ce qui donne

$$K_j(r) \ll r^2 \ (j \neq 0),$$

d'où

$$I_3'(r) \ll r^2. \tag{2.16}$$

Le cas où $k = 4$ est un peu étrange; suivant la même démarche que pour $k = 3$, on écrit

$$J_0^4(x) = \frac{4}{\pi^2} x^{-2} \cos^4(x - \pi/4) + O(x^{-3}), \tag{2.17}$$

que l'on reporte dans (2.13). Le terme d'erreur de (2.17) ne pose aucun problème, sa contribution est en $O(r^2)$. On développe

$$\cos^4(x - \pi/4) = \sum_{j=-4}^{4} b_j e^{ijx}, \tag{2.18}$$

mais cette fois on a b_0 non nul, il vaut même $3/8$. On est donc ramené à étudier

$$\widetilde{K}_j(r) := r \int_1^\infty J_1(rx) x^{-2} e^{ijx} \mathrm{d}x.$$

On traite $\widetilde{K}_j$ comme K_j, lorsque $j \neq 0$, on montre ainsi par une intégration par parties

$$\widetilde{K}_j(r) \ll r^2 \ (j \neq 0). \tag{2.19}$$

Les relations (2.17), (2.18) et (2.19) produisent l'égalité

$$I_4'(r) = \frac{3}{2\pi^2} \widetilde{K}_0(r) + O(r^2) = \frac{3}{2\pi^2} r^2 \int_r^\infty J_1(x) x^{-2} \mathrm{d}x + O(r^2).$$

Cette dernière intégrale est décomposée en

$$\int_r^\infty \ldots = \int_r^1 \ldots + \int_1^\infty \ldots$$

La deuxième intégrale de la ligne précédente est en $O(1)$, pour la première on utilise (2.9) sous la forme

$$\int_r^1 J_1(x) x^{-2} \mathrm{d}x = \int_r^1 \Big(\frac{x}{2} + O(x^3) \Big) x^{-2} \mathrm{d}x = \frac{1}{2} \log(1/r) + O(1),$$

ceci conduit à l'estimation asymptotique

$$I_4(r) = \frac{3}{4\pi^2} r^2 \big(\log(1/r) + O(1) \big), \tag{2.20}$$

ce qui, couplé à (2.12) donne un renseignement plus précis que la majoration annoncée pour $I_4(r)$. Les relations (2.12), (2.14), (2.16) et (2.20) donnent alors les majorations du lemme 2.6 dans tous les cas.

Passons à la minoration. La technique est assez proche de celle utilisée pour l'intégrale sur le groupe USp_{2k}. Soit $\delta > 0$ très petit ($\delta = \frac{1}{100k^4}$) convient. Puisque

$$\sum_{m=1}^{k} e\Big(\frac{m}{k}\Big) = 0,$$

on voit que pour tout $(x_1, \ldots, x_{k-2})$ tel que $|x_m - \frac{m}{k}| \leqslant \delta$, il existe des réels a_{k-1} et a_k tels que

$$\sum_{m=1}^{k-2} e(x_m) + e(a_{k-1}) + e(a_k) = 0$$

et $|a_{k-1} - \frac{k-1}{k}|$, $|a_k - 1| \leqslant \frac{1}{k^3}$.

Lorsque $x_1, \ldots, x_{k-2}$ sont fixés et que Δ est petit, on a, par le théorème des accroissements finis, l'inégalité

$$\Big|\sum_{m=1}^{k} e(x_m)\Big| \leqslant \Delta,$$

dès qu'on a $|x_{k-1} - a_{k-1}| \leqslant c_0\Delta$ et $|x_k - a_k| \leqslant c_0\Delta$, pour une certaine constante absolue $c_0 > 0$.

Signalons que tous les x_m ci-dessus sont, modulo 1, à une distance mutuelle $\gg_k 1$, par conséquent on a toujours $|e^{ix_\ell} - e^{ix_j}| \gg_k 1$, pour tout $\ell < j$. Retournant vers la formule (2.5), insérant les remarques précédentes et en se souvenant que g a pour support le disque unité, on obtient la minoration

$$\int_{\mathrm{U}_k} g_\Delta(\theta)\mathrm{d}\mu_H(\theta) \gg \Delta^2. \qquad \square$$

II. 5. Majoration du terme d'erreur.

Pour majorer $\|g_\Delta\|^\natural$, on utilise l'observation de Katz ([K2], Chap. 3), conséquence de la formule d'intégration de Weyl. Rappelons que les fonctions centrales sur K correspondent aux fonctions sur un tore maximal T de K, invariantes par le groupe de Weyl W. Comme $T \simeq (\mathbb{S}^1)^r$ (r désigne le rang de K), une fonction de h sur T de classe $\mathcal{C}^\infty$ admet une décomposition en série de Fourier classique :

$$h(t) = \sum_{n \in \mathrm{Hom}(T, \mathbb{S}^1)} \widehat{h}(n) t^n, \ \widehat{h}(n) = \int_T h(t') t'^{-n} \mathrm{d}\mu_H(t')$$

et on définit une semi-norme naturelle

$$\|h\|_1 := \sum_{n \in \mathrm{Hom}(T, \mathbb{S}^1) - \{0\}} |\widehat{h}(n)|.$$

L'observation de Katz est que pour toute fonction g de T invariante par W, il existe une fonction h de T telle que $\|g\|^\natural = \|h\|_1$. Cette fonction est définie

de la manière suivante : fixant une orientation sur $\mathrm{Hom}(T,\mathbb{S}^1)\otimes_{\mathbb{Z}}\mathbb{R}\simeq\mathbb{R}^r$, on note R_+ l'ensemble des racines positives correspondantes, on pose

$$\varphi:=\frac{1}{2}\sum_{\alpha\in\mathbb{R}_+}\alpha \text{ et } J(\varphi)(t)=\sum_{w\in W}\varepsilon(w)t^{\varphi\circ w},$$

où $\varepsilon(w)$ est le déterminant de $w\in\mathrm{GL}_r$. Noter que pour les groupes K que nous considérons, on a $\varphi\in\mathrm{Hom}(T,\mathbb{S}^1)\simeq\mathbb{Z}^r$. Alors il existe un opérateur différentiel D_{Weyl} sur T d'ordre $|R_+|$ tel que si l'on pose

$$h:=\frac{1}{|W|}D_{\mathrm{Weyl}}(J(\varphi)g)$$

on a $\|g\|^\natural=\|h\|_1$.

Fixons une $\mathbb{Z}$-base de $\mathrm{Hom}(T,\mathbb{S}^1)\simeq\mathbb{Z}^r$, et $\{n_j^*\}_{j=1,\dots,r}$ la base duale, on pose, pour $n\in\mathrm{Hom}(T,\mathbb{S}^1)$, $n_j:=n_j^*(n)$ et D_j est l'opérateur différentiel d'ordre 1 caractérisé par $D_jt^n=n_jt^n$. Pour $J\subset\{1,\dots,r\}$, on pose $D_J=\prod_{j\in J}D_j$. Ainsi, si h est de classe $\mathcal{C}^\infty$, on a

$$n_j\widehat{h}(n)=\widehat{D_jh}(n),\ \Big(\prod_{j\in J}n_j\Big)\widehat{h}(n)=\widehat{D_Jh}(n).$$

Pour g_Δ, et $h_\Delta=|W|^{-1}D_{\mathrm{Weyl}}(J(\varphi)g_\Delta)$, on a donc

$$\begin{aligned}\|h_\Delta\|_1&=\sum_{\substack{I\cup J=\{1,\dots,r\}\\ I\cap J=\emptyset}}\sum_{\substack{i\in I\\ j\in J}}\sum_{\substack{n,|n_i|\leqslant\Delta^{-1}\\ |n_j|>\Delta^{-1}}}\frac{1}{\prod_{j\in J}|n_j|}\Big|\widehat{D_Jh_\Delta}(n)\Big|\\ &\leqslant\sum_{\substack{I\cup J=\{1,\dots,r\}\\ I\cap J=\emptyset}}\sum_{\substack{i\in I\\ j\in J}}\Big(\sum_{\substack{n,|n_i|\leqslant\Delta^{-1}\\ |n_j|>\Delta^{-1}}}\frac{1}{\prod_{j\in J}|n_j|^2}\Big)^{\frac12}\Big(\sum_n|\widehat{D_Jh_\Delta}(n)|^2\Big)^{\frac12}\\ &\ll\sum_{\substack{I\cup J=\{1,\dots,r\}\\ I\cap J=\emptyset}}\sum_{\substack{i\in I\\ j\in J}}\Delta^{(|J|-|I|)/2}\|D_Jh_\Delta\|_2\end{aligned}$$

par l'identité de Parseval. Comme h_Δ est l'image de g_Δ par un opérateur différentiel d'ordre $|R_+|$ et D_J est d'ordre $|J|$, on a par les lemmes 2.5 et 2.6 la majoration $||D_Jh_\Delta||_2\ll_{g,k}(\Delta^{-1})^{|R_+|+|J|}\Delta^{\frac{\kappa}{2}}$ avec $\kappa=1$ si $K=\mathrm{USp}_k$ et $\kappa=2$ si $K=\mathrm{SU}_k$ avec $k\geqslant3$ (lorsque dans ce cas, on a $k=4$, il faut même multiplier par $\big(\log(1/\Delta)\big)^{\frac12}$); on obtient donc

$$\begin{aligned}(2.21)\qquad\|g_\Delta\|^\natural=||h_\Delta||_1&\ll_{k,g}\sum_{\substack{I\cup J=\{1,\dots,r\}\\ I\cap J=\emptyset}}\sum_{\substack{i\in I\\ j\in J}}\Delta^{\frac{|J|-|I|}{2}-|J|-|R_+|+\frac{\kappa}{2}},\\ &\ll_{k,g}\Delta^{\frac{\kappa-r-2|R_+|}{2}}=\Delta^{\frac{\kappa-\dim K}{2}},\end{aligned}$$

en utilisant la relation $r+2|R_+|=\dim K$ et en multipliant cette majoration par $\big(\log(1/\Delta)\big)^{\frac12}$ lorsque $\kappa=2$ et $k=4$.

Exemple 2.9. — Pour $k = 2$, on a nécessairement $K = \mathrm{SU}_2 = \mathrm{USp}_2$, on a alors $\kappa = 1$, $\dim K = 3$ et on trouve la majoration $\ll \Delta^{-1}$.

II. 6. Fin de l'estimation.

Par (2.3), par les lemmes 2.5 et 2.6 et par (2.21) on obtient la minoration

$$W_{g_\Delta} \gg_{k,g} \Delta^{\kappa} - O_{k,g}\Big(\Delta^{(\kappa-\dim K)/2}(\log Q)^4(\log(1/\Delta))^{\frac{1}{2}}(Q^{-\frac{1}{2}} + (Q/P)^{\frac{1}{2}})\Big)$$

où $\kappa = 1$ pour $K = \mathrm{USp}_k$ ($k \geqslant 2$) et $\kappa = 2$ pour $K = \mathrm{SU}_k$ ($k \geqslant 3$). Prenant alors $P = Q^2$, on voit que si on choisit $\Delta = \sqrt{PQ}^{-2/3(\dim K+\kappa)+\varepsilon}$, avec $\varepsilon > 0$, on a pour Q assez grand, l'inégalité $W_{g_\Delta}(P, Q) > 0$, ceci termine la preuve des théorèmes 1.2 et 1.3 puisque

$$\dim \mathrm{SU}_k = k^2 - 1, \ \dim \mathrm{USp}_k = \frac{k}{2}(k+1). \qquad \square$$

III. Lemmes sur les sommes de Salié et sur les nombres premiers.

Dans ce paragraphe, on donne les matériaux nécessaires à la preuve des théorèmes 1.4 et 1.5 relatifs aux sommes de Salié. Le point de départ est l'évaluation classique des sommes de Salié en fonction des solutions d'une équation quadratique. On introduit le symbole $\lambda(n)$ défini sur les entiers impairs par la formule

$$\lambda(n) = \begin{cases} 1 & \text{si } n \equiv 1 \bmod 4 \\ i & \text{si } n \equiv 3 \bmod 4. \end{cases}$$

Ceci posé, on a le

LEMME 3.1 ([Sa], [Mo], Thm 1 par exemple). — *Soient a et b deux entiers non divisibles par $p \geqslant 3$. La somme de Salié $T(a, b; p)$ vérifie les égalités*

$$T(a, b; p) = 2\lambda(p)\Big(\frac{a}{p}\Big)\sqrt{p}\cos\frac{2\pi h}{p}, \text{ si } \Big(\frac{ab}{p}\Big) = 1$$

(h est alors une des solutions de $h^2 - 4ab \equiv 0$ modulo p) et

$$T(a, b; p) = 0, \text{ si } \Big(\frac{ab}{p}\Big) = -1.$$

Rappelons la formule de réciprocité

$$\frac{\overline{m}}{n}+\frac{\overline{n}}{m}\equiv\frac{1}{mn} \bmod 1, \tag{3.1}$$

valable pour m et n entiers premiers entre eux.

En combinant les formules (1.2) et (3.1), le lemme 3.1, la formule de réciprocité quadratique et le théorème des accroissements finis, on obtient directement le

LEMME 3.2. — *Pour p et q nombres premiers impairs distincts, on a l'égalité*

$$T(1,1;pq)=4\lambda(pq)\cos\Big(\frac{2\pi\overline{q}}{p}\Big)\Big(\cos\Big(\frac{2\pi\overline{q}}{p}\Big)+\frac{2\pi\theta_{p,q}}{pq}\Big)\sqrt{pq},$$

où $\theta_{p,q}$ est un réel tel que $|\theta_{p,q}|\leqslant 1$.

Ce lemme apparaît sous une autre forme par exemple dans ([I2], Cor. 4.11). Nous passons maintenant aux résultats nécessaires de la théorie des nombres premiers. Ces résultats concernent la fonction $\pi(x;d,a)$ qui compte le cardinal de l'ensemble des nombres premiers inférieurs à x et congrus à a modulo d, et les fonctions dérivées à savoir $\psi(x;d,a)=\sum_{n\leqslant x,\ n\equiv a \pmod d}\Lambda(n)$. Mais, puisque le signe d'une somme de Salié dépend fortement des congruence modulo 4, il faut aussi introduire les fonctions

$$\pi(x;d,a;4,b)=\sum_{\substack{p\leqslant x,\ p\equiv b \bmod 4\\ p\equiv a \bmod d}}1$$

et

$$\psi(x;d,a;4,b)=\sum_{\substack{n\leqslant x,\ n\equiv b \bmod 4\\ n\equiv a \bmod d}}\Lambda(n).$$

Pour commencer, rappelons le résultat suivant ([V], Thm 1, [Da], p. 162 par exemple) qui donne, grâce à l'inégalité de grand crible, la valeur moyenne de la fonction

$$\psi(x;\chi)=\sum_{n\leqslant x}\chi(n)\Lambda(n), \tag{3.2}$$

pour χ caractère de Dirichlet. On a

LEMME 3.3. — *On suppose $D\geqslant 1$ et $x\geqslant 2$. Alors, on a l'estimation*

$$\sum_{d\leqslant D}\frac{d}{\varphi(d)}\sum_{\substack{\chi \bmod d\\ \chi \text{ primitif}}}\max_{y\leqslant x}|\psi(y;\chi)|$$
$$\ll x(\log xD)^3+x^{\frac34}D^{\frac54}(\log xD)^{\frac{23}{8}}+x^{\frac12}D^2(\log xD)^{\frac72}.$$

Il est bien connu que ce lemme, couplé au théorème de Siegel-Walfisz, conduit au théorème de Bombieri-Vinogradov, qui affirme que, en moyenne, les fonctions $\pi(x;d,a)$ et $\psi(x;d,a)$ ont un comportement harmonieux, pour $d \leqslant x^{\frac{1}{2}}(\log x)^{-A}$, où A est une certaine constante positive. Le problème de contrôler le comportement en moyenne de la fonction $\pi(x;d,a)$ dans des progressions arithmétiques de module d avec $\log d/\log x \geqslant 1/2+\varepsilon$ n'est toujours pas résolu *stricto sensu*. Il est presque résolu dans l'énoncé suivant de Bombieri, Friedlander et Iwaniec qui est l'aboutissement d'une série de travaux de ces auteurs et de Fouvry, où, pour contourner la barrière du grand crible, on utilise la méthode de dispersion et des majorations de sommes de Kloosterman. On a

LEMME 3.4 ([BFI], Main Thm). — *Soit $a \neq 0$, $x \geqslant y \geqslant 3$, et $D^2 \leqslant xy$. Il existe une constante absolue B, telle qu'on ait les majorations*

$$\sum_{\substack{D<d\leqslant 2D\\(d,a)=1}} \Big|\psi(x;d,a)-\frac{x}{\varphi(d)}\Big| = O_a\Big(x\Big(\frac{\log y}{\log x}\Big)^2(\log\log x)^B\Big) \tag{3.3}$$

et

$$\sum_{\substack{D<d\leqslant 2D\\(d,2a)=1}} \Big|\psi(x;d,a;4,b)-\frac{x}{2\varphi(d)}\Big| = O_a\Big(x\Big(\frac{\log y}{\log x}\Big)^2(\log\log x)^B\Big) \ (b=\pm 1). \tag{3.4}$$

Si on est moins exigeant en ne demandant non plus des équivalents en moyenne mais des minorations valables pour presque tout module d, on peut alors dépasser la valeur critique $\sqrt{x}$ pour ces modules. On a

LEMME 3.5 ([BH], Thm 1). — *Il existe un réel $\alpha > 0$ et une fonction $C : [0.5, 0.52] \to [\alpha,\infty[$, tels que, pour tout $a \neq 0$, pour tout θ $(0.5 \leqslant \theta \leqslant 0.52)$, tout $x \geqslant 2$ on ait l'inégalité*

$$\sharp\Big\{d;(d,a)=1,\ x^\theta < d \leqslant 2x^\theta,\ \pi(2x;d,a)-\pi(x;d,a) < \frac{C(\theta)x}{\varphi(d)\log x}\Big\} = O_a\big(x^\theta \log^{-2} x\big), \tag{3.5}$$

et pour tout $a \neq 0$, pour tout θ $(0.5 \leqslant \theta \leqslant 0.52)$, tout $x \geqslant 2$ et pour $b = \pm 1$, on ait l'inégalité

$$\sharp\Big\{d;(d,2a)=1,\ x^\theta<d\leqslant 2x^\theta,\ \pi(2x;d,a;4,b)-\pi(x;d,a;4,b)<\frac{C(\theta)x}{2\varphi(d)\log x}\Big\} = O_a\big(x^\theta \log^{-2} x\big). \tag{3.6}$$

Plus précisément, Baker et Harman montrent (3.5) avec une fonction $C(\theta)$ décroissante telle que $C(0,52) = 0,16$, et telle que la valeur de $C(0,5)$

puisse être prise arbitrairement proche de 1. Pour être rigoureux, on ne trouve dans les références citées ni la formule (3.4) ni la formule (3.6). Il n'est pas possible de passer directement de (3.3) et (3.5) à (3.4) et (3.6), puisque en écrivant $\psi(x;d,a;4,b)=\psi(x;4d,a_d)$, le nombre a_d dépend de d. Il faut donc adapter la preuve des formules (3.3) et (3.5) pour insérer sur les n comptés par la fonction ψ ou les p comptés par la fonction π, la condition $n\equiv b$ modulo 4 ou la condition $p\equiv b$ modulo 4. Cette adaptation a déjà été faite par Fouvry ([F], p. 389–390) où il a fallu introduire la condition supplémentaire $p\equiv 2$ modulo 3, et par Heath-Brown ([H-B], p. 29–30). Il suffit de suivre l'adaptation mise au point dans chacun de ces travaux.

Enfin, Baker et Harman étudient la fonction $\pi(x;d,a)$ et non la fonction $\pi(2x;d,a)-\pi(x;d,a)$. La modification de leur preuve est immédiate : il suffit de considérer l'ensemble $\{n;x<n\leqslant 2x,\ n\equiv a \bmod d\}$ pour le cribler, au lieu de l'ensemble $\{n;\ n\leqslant x,\ n\equiv a \bmod d\}$.

IV. Preuve du théorème 1.4.

On pose donc que p et q sont des nombres premiers tels que $3\leqslant q<p$. On s'intéresse uniquement au cas où $pq\equiv 1$ modulo 4, l'autre cas se traitant de même. Nous nous restreignons même au cas

$$p\equiv q\equiv 1 \mod 4,$$

le cas $p\equiv q\equiv 3$ modulo 4, étant absolument identique. On note $\{y\}$ la partie fractionnaire du réel y.

La première étape de la preuve du théorème 1.4 est la

PROPOSITION 4.1. — *Lorsque $x\to\infty$, l'ensemble*

$$\mathcal{E}(x)=\Big\{\Big\{\frac{\overline{q}}{p}\Big\};3\leqslant q<p\leqslant x,\ p\equiv q\equiv 1 \mod 4\Big\}$$

est équiréparti sur $[0,1[$.

Preuve. — Par le critère de Weyl, il suffit de montrer que, pour tout entier $a\neq 0$, on a

$$\sum_{p\leqslant x}\sum_{q<p} e\Big(\frac{a\overline{q}}{p}\Big)=o\big(\sharp\mathcal{E}(x)\big) \tag{4.1}$$

(on a volontairement oublié les conditions de congruence $p\equiv q\equiv 1$ mod 4, pour alléger les notations ; ces conditions n'apportent aucune difficulté supplémentaire). En fait, puisque $\sharp\mathcal{E}(x)\sim\frac{x^2}{8\log^2 x}$, on voit que (4.1) est une

conséquence de la relation

$$S_a(p) := \sum_{q<p} e\Big(\frac{a\overline{q}}{p}\Big) = o\Big(\frac{p}{\log p}\Big) \text{ pour tout } a \neq 0. \tag{4.2}$$

En d'autres termes nous montrons l'équirépartition modulo 1 de l'ensemble $\{\{\frac{\overline{q}}{p}\};\ q < p\}$, lorsque p est un premier fixé. La preuve de (4.2) n'est pas structurellement différente de celle de [Mi1], Prop. 3.2, ou de sa version axiomatisée [Mi2], Thm 3.1, mais nous espérons que la présentation donnée ci-dessous est plus élégante. Nous aurons besoin des deux lemmes suivants. Le premier est une conséquence très classique des majorations de Weil des sommes de Kloosterman :

LEMME 4.2. — *Soit t et u deux réels tels que $0 < u - t < p$. On a alors l'inégalité*

$$\sum_{t<n\leqslant u} e\Big(\frac{a\overline{n}}{p}\Big) = O(p^{\frac{1}{2}} \log p),$$

où la constante implicite du O peut être choisie indépendante de t, de u et de l'entier a non divisible par p.

Le second est une conséquence de l'égalité à la base du crible d'Iwaniec (voir, par exemple [I1], Lemma 1, [FI], Lemma 1). En notant $f_z(n)$ la fonction caractéristique des entiers n dont tous les diviseurs premiers sont supérieurs à z, on a

LEMME 4.3. — *Soient $D \geqslant z \geqslant 2$. Il existe deux suites de réels λ_d et $\sigma_{p,d}$ vérifiant*

- *pour tout $d \geqslant 1$ et tout premier p, on a $|\lambda_d| \leqslant 1$ et $|\sigma_{p,d}| \leqslant 1$;*
- *on a l'implication $\lambda_d \neq 0 \Rightarrow d < D$;*
- *on a l'implication $\sigma_{p,d} \neq 0 \Rightarrow p < z$, $\frac{D}{p^2} \leqslant d < \frac{D}{p}$ et tout diviseur premier de d est $> p$;*

telles que, pour toute fonction arithmétique $F(n)$ nulle pour n suffisamment grand, on ait l' égalité

$$\sum_n f_z(n)F(n) = \sum_{d\leqslant D} \lambda_d \sum_m F(dm) + \sum_{p<z} \sum_{d<D/p} \sigma_{p,d} \sum_n f_p(n)F(pdn).$$

Preuve de (4.2). — On pose

$$z = D = \sqrt{p}/\exp(\sqrt{\log p}).$$

On a donc, par le théorème des nombres premiers, l'égalité

$$S_a(p) = \sum_{n<p} f_z(n) e\Big(\frac{a\overline{n}}{p}\Big) + O\Big(p \log^{-\frac{3}{2}} p\Big),$$

puis le lemme 4.3 donne l'égalité

$$S_a(p) = \sum_{d\leqslant D} \lambda_d \sum_{dm<p} e\Big(\frac{a\overline{dm}}{p}\Big) + \sum_{p'<z} \sum_{d<D/p'} \sigma_{p',d} \sum_{\substack{m \\ p'dm<p}} f_{p'}(m) e\Big(\frac{a\overline{p'dm}}{p}\Big) + O\Big(p \log^{-\frac{3}{2}} p\Big).$$

La première somme de la ligne précédente est une somme de type I : l'entier m décrit un intervalle de longueur $< p$, le lemme 4.2 permet de majorer directement cette somme sur m donnant l'égalité

$$\begin{aligned} S_a(p) &= \sum_{p'<z} \sum_{d<D/p'} \sigma_{p',d} \sum_{\substack{m \\ p'dm<p}} f_{p'}(m) e\Big(\frac{a\overline{p'dm}}{p}\Big) + o\Big(\frac{p}{\log p}\Big) \\ &= \mathfrak{S}_a(p) + o\Big(\frac{p}{\log p}\Big), \end{aligned} \tag{4.3}$$

par définition. La somme $\mathfrak{S}_a(p)$ est une somme de type II. Il faut faire apparaître une forme bilinéaire avec des variables de tailles convenables. Mais cette stratégie dépend de l'ordre de grandeur de p'. Pour ce faire, on décompose $\mathfrak{S}_a(p)$ en

$$\begin{aligned} \mathfrak{S}_a(p) &= \sum_{p'\leqslant D^{\frac{1}{4}}} \ldots + \sum_{D^{\frac{1}{4}}<p'<z} \ldots \\ &= \mathfrak{S}_a^\sharp(p) + \mathfrak{S}_a^\flat(p), \end{aligned} \tag{4.4}$$

par définition. On transforme $\mathfrak{S}_a^\sharp(p)$ ainsi :

$$\big|\mathfrak{S}_a^\sharp(p)\big| \leqslant \sum_{p'\leqslant D^{\frac{1}{4}}} \big|\mathfrak{L}_a(p,p')\big|, \tag{4.5}$$

avec

$$\mathfrak{L}_a(p,p') = \sum_m f_{p'}(m) \sum_{d\in\mathcal{D}_{p,p',m}} \sigma_{p',d} e\Big(\frac{a\overline{p'dm}}{p}\Big),$$

où, en raison du support de la fonction $\sigma_{p',d}$, la variable d parcourt l'intervalle

$$\mathcal{D}_{p,p',m} = \Big[\frac{D}{p'^2}, \min\Big(\frac{D}{p'}, \frac{p}{p'm}\Big)\Big[.$$

On contrôle l'ordre de grandeur de la variable m par un découpage dyadique d'où l'inégalité

$$\mathfrak{L}_a(p,p') \ll \log p. \Big| \sum_{M<m\leqslant 2M} f_{p'}(m) \sum_{d\in\mathcal{D}_{p,p',m}} \sigma_{p',d} e\Big(\frac{a\overline{p'dm}}{p}\Big)\Big|,$$

valable pour un certain M vérifiant : $M \leqslant \frac{pp'}{D}$, (sinon l'intervalle $\mathcal{D}_{p,p',m}$ est vide). On applique l'inégalité de Cauchy-Schwarz, on développe et on intervertit les sommations, d'où

$$\mathfrak{L}_a(p,p') \ll \log p.M^{\frac{1}{2}}\Big\{\sum_{d,d'<\min\left(\frac{D}{p'},\frac{p}{p'M}\right)}\sum\Big|\sum_{m\in\mathcal{I}_{d,d',p,p'}} e\Big(\frac{a(\overline{d}-\overline{d'})\overline{p'm}}{p}\Big)\Big|\Big\}^{\frac{1}{2}},$$

où $\mathcal{I}_{d,d',p,p'}$ est un intervalle inclus dans $[M,2M]$. Le lemme 4.2 majore la somme sur m lorsque $d \neq d'$, sinon on utilise la majoration triviale, d'où l'inégalité

$$\mathfrak{L}_a(p,p') \ll \log p.M^{\frac{1}{2}}\Big\{\min{}^2\Big(\frac{D}{p'},\frac{p}{p'M}\Big)p^{\frac{1}{2}}\log p + \min\Big(\frac{D}{p'},\frac{p}{p'M}\Big)M\Big\}^{\frac{1}{2}}.$$

On transforme l'expression précédente suivant que $1 \leqslant M \leqslant \frac{p}{D}$, ou que $\frac{p}{D} < M \leqslant \frac{pp'}{D}$, puis on prend la valeur la pire de M qui est, suivant les cas, $\frac{p}{D}$ ou $\frac{pp'}{D}$, pour parvenir finalement à la relation

$$\mathfrak{L}_a(p,p') \ll p^{\frac{3}{4}}p'^{-1}D^{\frac{1}{2}}\log^{\frac{3}{2}} p + pD^{-\frac{1}{2}}\log p.$$

On reporte cette majoration dans (4.5), pour écrire

$$\mathfrak{S}_a^\sharp(p) \ll p^{\frac{3}{4}}D^{\frac{1}{2}}\log^2 p + pD^{-\frac{1}{4}} = o\Big(\frac{p}{\log p}\Big), \tag{4.6}$$

en tenant compte de la valeur de D.

Dans l'étude de $\mathfrak{S}_a^\flat(p)$, on veut considérer $p'd$ comme une seule variable, mais il faut que les variables p' et m ne soient plus liées arithmétiquement par le facteur $f_{p'}(m)$. Dans ce but, on pose $\Delta = 1 + (\log p)^{-10}$ et on désigne par P' tout réel $\leqslant z\Delta^{-1}$, de la forme $D^{\frac{1}{4}}\Delta^k$ $(k = 0, 1, \ldots)$. Notons que le nombre de tels P' est en $O\big(\log^{11} p\big)$. Ceci étant fixé, on décompose

$$\mathfrak{S}_a^\flat(p) = \sum_{P'} \mathfrak{S}_a^\flat(p,P'), \tag{4.7}$$

avec

$$\mathfrak{S}_a^\flat(p,P') = \sum_{\substack{P'<p'\leqslant P'\Delta\\ p'<z}}\sum_m f_{p'}(m)\sum_{\substack{d\\ p'dm<p}}\sigma_{p',d}e\Big(\frac{\overline{ap'dm}}{p}\Big).$$

On approche la somme précédente par

$$\widetilde{\mathfrak{S}}_a^\flat(p,P') = \sum_{\substack{P'<p'\leqslant P'\Delta\\ p'<z}}\sum_m f_{P'}(m)\sum_{\substack{d\\ p'dm<p}}\sigma_{p',d}e\Big(\frac{\overline{ap'dm}}{p}\Big).$$

Cette modification de la fonction $f_{P'}$ est négligeable, puisqu'on a facilement

$$\begin{aligned}\big|\mathfrak{S}_a^\flat(p,P') - \widetilde{\mathfrak{S}}_a^\flat(p,P')\big| &\ll \sum_{P'<p'\leqslant P'\Delta}\ \sum_{P'<p''\leqslant P'\Delta}\ \sum_d \frac{p}{p'p''d}\\ &\ll p\Big[\log\frac{\log P'\Delta}{\log P'}\Big]^2\log p\\ &\ll p\log^{-21}p.\end{aligned}\tag{4.8}$$

En regroupant (4.7) et (4.8), on a, pour un certain P' vérifiant $D^{\frac14}\leqslant P'\leqslant z\Delta^{-1}$, la relation

$$\mathfrak{S}_a^\flat(p)\ll\big|\widetilde{\mathfrak{S}}_a^\flat(p,P')\big|\log^{11}p+o\Big(\frac{p}{\log p}\Big).\tag{4.9}$$

On écrit

$$\widetilde{\mathfrak{S}}_a^\flat(p,P')=\sum_m f_{P'}(m)\sum_{\substack{P'<p'\leqslant P'\Delta\\ p'<z}}\ \sum_{\substack{d\\ p'dm<p}}\sigma_{p',d}e\Big(\frac{a\overline{p'dm}}{p}\Big),$$

on constate ensuite qu'un entier n a au plus une seule écriture sous la forme $n=p'd$, avec $\sigma_{p',d}\neq0$, il existe donc des coefficients c_n (avec $|c_n|\leqslant1$) tels qu'on ait l'égalité

$$\widetilde{\mathfrak{S}}_a^\flat(p,P')=\sum_m f_{P'}(m)\sum_{\substack{P'\leqslant n\leqslant D\\ mn<p}}c_n e\Big(\frac{a\overline{mn}}{p}\Big).$$

On fait un découpage dyadique de la variable m. Ainsi, pour un certain M vérifiant

$$M\leqslant pP'^{-1},$$

on a la relation

$$\widetilde{\mathfrak{S}}_a^\flat(p,P')\ll\log p\sum_{M<m\leqslant2M}\Big|\sum_{\substack{P'\leqslant n\leqslant D\\ mn<p}}c_n e\Big(\frac{a\overline{mn}}{p}\Big)\Big|.$$

L'inégalité de Cauchy-Schwarz conduit à

$$\widetilde{\mathfrak{S}}_a^\flat(p,P')\ll\log p\ \ M^{\frac12}\Big\{\sum_{n_1,\ n_2\leqslant\min(D,\frac{p}{M})}\Big|\sum_{m\in\mathcal{I}_{n_1,n_2,p}}e\Big(\frac{a(\overline{n_1}-\overline{n_2})\overline{m}}{p}\Big)\Big|\Big\}^{\frac12},$$

où $\mathcal{I}_{n_1,n_2,p}$ est un intervalle inclus dans $[M,2M]$. Le lemme 4.2 donne

$$\begin{aligned}\widetilde{\mathfrak{S}}_a^\flat(p,P')&\ll\log p\ \ M^{\frac12}\Big\{\min{}^2\Big(\frac{p}{M},D\Big)p^{\frac12}\log p+\min\Big(\frac{p}{M},D\Big)\cdot M\Big\}^{\frac12}\\ &\ll\log^{\frac32}p\ \big(p^{\frac34}D^{\frac12}+pP'^{-\frac12}+pD^{-\frac12}\big).\end{aligned}$$

Il reste à reporter cette majoration dans (4.9), d'utiliser la valeur minimale de P' et la valeur de D pour conclure par

$$\mathfrak{S}_a^\flat(p) = o\Big(\frac{p}{\log p}\Big). \tag{4.10}$$

En regroupant (4.3), (4.4), (4.6) et (4.10), on a $S_a(p) = o\big(\frac{p}{\log p}\big)$, ceci prouve la relation (4.2) et par là-même la proposition 4.1. □

Le passage de la proposition 4.1 au théorème 1.4 est une application du lemme 3.2. Soit $n = pq$ le produit de deux nombres premiers congrus à 1 modulo 4, avec $q < p$. Le lemme 3.2 entraîne l'encadrement

$$\cos^2 2\pi\frac{\overline{q}}{p} - \frac{2\pi}{n} \leqslant \frac{T(1,1;pq)}{4\sqrt{pq}} \leqslant \cos^2 2\pi\frac{\overline{q}}{p} + \frac{2\pi}{n}.$$

Notons

$$E(x;\beta,\alpha) := \sharp\Big\{\{\frac{\overline{q}}{p}\} \in \mathcal{E}(x), \beta \leqslant \{\frac{\overline{q}}{p}\} \leqslant \alpha\Big\}.$$

Ainsi, lorsque $0 \leqslant a < b \leqslant 1$, on a, pour tout $\varepsilon > 0$ l'encadrement

$$\begin{aligned}
&E(x;\beta+\varepsilon,\alpha-\varepsilon) + E\Big(x;\frac{1}{2}+\beta+\varepsilon,\frac{1}{2}+\alpha-\varepsilon\Big)\\
&\qquad + E\Big(x;\frac{1}{2}-\alpha+\varepsilon,\frac{1}{2}-\beta-\varepsilon\Big) + E(x;1-\alpha+\varepsilon,1-\beta-\varepsilon) - O_\varepsilon(1)\\
&\leqslant \sharp\Big\{(p,q), q<p\leqslant x,\ p\equiv q\equiv 1 \bmod 4,\ a\leqslant \frac{T(1,1;pq)}{4\sqrt{pq}} \leqslant b\Big\}\\
&\leqslant E(x;\beta-\varepsilon,\alpha+\varepsilon) + E\Big(x;\frac{1}{2}+\beta-\varepsilon,\frac{1}{2}+\alpha+\varepsilon\Big)\\
&\qquad + E\Big(x;\frac{1}{2}-\alpha-\varepsilon,\frac{1}{2}-\beta+\varepsilon\Big) + E(x;1-\alpha-\varepsilon,1-\beta+\varepsilon) + O_\varepsilon(1),
\end{aligned}$$

où α et β sont les nombres compris entre 0 et $\frac{1}{4}$ tels que $\cos^2 2\pi\alpha = a$ et $\cos^2 2\pi\beta = b$. On applique alors la proposition 4.1, puis on fait tendre ε vers 0. On a alors prouvé le théorème 1.4. □

V. Preuve du théorème 1.5.

Cherchons maintenant des sommes de Salié très petites. On se restreint au cas où $p,\ q \equiv 1$ modulo 4, le cas où $p,\ q \equiv 3$ modulo 4 étant similaire. En intervertissant les rôles de p et q, on voit que le lemme 3.2 entraîne l'égalité

$$\frac{T(1,1,pq)}{4\sqrt{pq}} = \sin\Big(\frac{\pi}{2}\big(1-4\frac{\overline{p}}{q}\big)\Big)\cdot\Big(\sin\big(\frac{\pi}{2}\big(1-4\frac{\overline{p}}{q}\big)\big) + O\big(\frac{1}{pq}\big)\Big), \tag{5.1}$$

par conséquent la somme $T(1,1;pq)$ est d'autant plus petite que la fraction $\frac{\overline{p}}{q}$ est proche de $\frac{1}{4}$ ou $\frac{3}{4}$ modulo 1, c'est-à-dire

$$1-4\frac{\overline{p}}{q}=\pm\frac{1}{q} \bmod 2.$$

Ceci a lieu si et seulement si on a

$$\overline{p}\equiv\pm\frac{q-1}{4} \bmod q, \tag{5.2}$$

puisqu'on a supposé $q\equiv 1$ modulo 4. La relation (5.2) équivaut à $p\equiv\pm 4$ modulo q.

En conclusion, si $q\equiv 1$ modulo 4 et $p\equiv\pm 4$ modulo q on a, grâce à (5.1), la relation

$$\frac{T(1,1;pq)}{4\sqrt{pq}}=\frac{\pi^2}{4q^2}\Big(1+O(\frac{1}{p})\Big),$$

et il n'est pas possible d'avoir la relation

$$\frac{T(1,1;pq)}{4\sqrt{pq}}=a\frac{\pi^2}{4q^2}(1+o(1))$$

avec une constante réelle a telle que $0<a<1$, pour une infinité de (p,q) avec $q<p$.

Il reste à prouver l'existence de tels p et q comme ci-dessus et d'évaluer leur cardinal lorsqu'on impose $P<p\leqslant 2P$ et $Q<q\leqslant 2Q$. On désigne par $A(P,Q)$ ce cardinal. Il vérifie

$$A(P,Q)=\Big(\frac{1}{\log P}+o(1)\Big)\sum_{\substack{Q<q\leqslant 2Q\\ q\equiv 1 \bmod 4}}\big(\psi(2P;q,\pm 4;4,1)-\psi(P;q,\pm 4;4,1)\big).$$

La formule (3.4) donne pour $A(P,Q)$ l'équivalent asymptotique

$$A(P,Q)\sim\frac{\log 2}{2}\,\frac{P}{\log P.\log Q},$$

sous la condition $Q^2\leqslant P$.

Si on se contente d'une minoration de $A(P,Q)$, on suppose $Q\leqslant P^{0,52}$ et on applique le lemme 3.5 (majoration (3.6)) sous la forme

$$A(P,Q)=\sum_{\substack{Q<q\leqslant 2Q\\ q\equiv 1 \bmod 4}}\big(\pi(2P;q,\pm 4;4,1)-\pi(P;q,\pm 4;4,1)\big)\gg\frac{P}{\log P.\log Q}.$$

Enfin, la dernière partie de l'énoncé du théorème 1.5 requiert la forme suivante de la conjecture d'Elliott-Halberstam ([EH]) :

Pour tout entier $a \neq 0$ et tout $\varepsilon > 0$ on a la relation

$$\sum_{d \leqslant x^{1-\varepsilon}} \max_{(a,d)=1} \left| \pi(x; d, a) - \frac{\pi(x)}{\varphi(d)} \right| = O_\varepsilon(x \log^{-3} x). \tag{5.3}$$

Sous cette hypothèse, les calculs se font comme précédemment mais avec le choix $Q \leqslant P^{1-\varepsilon}$. □

BIBLIOGRAPHIE

[BH] R. C. BAKER et G. HARMAN, The Brun-Titchmarsh Theorem on average, Analytic Number Theory, Proceedings of a Conference in honor of H. Halberstam, vol. 1, Birkhaüser, Progress in Mathematics, 138 (1996), 39–103.

[BFI] E. BOMBIERI, J. FRIEDLANDER et H. IWANIEC, Primes in Arithmetic Progressions to Large Moduli. II, Math. Annalen, 277 (1987), 361–393.

[Da] H. DAVENPORT, Multiplicative Number Theory, Graduate Texts in Mathematics, 74 (Second Edition), Springer-Verlag (1980).

[Del] P. DELIGNE, Application de la formule des traces aux sommes trigonométriques, SGA4 1/2, Springer Lecture Notes in Math., 569, Springer-Verlag (1977).

[Deu] M. DEURING, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, 14 (1941), 197–272.

[DFI] W. DUKE, J. B. FRIEDLANDER et H. IWANIEC, Equidistribution of roots of a quadratic congruence to prime moduli, Ann. of Math. (2), 141 (1995), 423–441.

[E] N. ELKIES, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, Inv. Math., 89 (1987), 207–220.

[EH] P. D. T. A. ELLIOTT et H. HALBERSTAM, A conjecture in prime number theory, Symp. Math., 4 (INDAM Rome, 1968–69), 59–72.

[EMOT] A. ERDELYI, W. MAGNUS, F. OBERHETTINGER et F. G. TRICOMI, Higher Transcendental Functions, vol II, Mc Graw-Hill Book Company, Inc., 1953.

[F] E. FOUVRY, Théorème de Brun-Titchmarsh; Application au théorème de Fermat, Invent. Math., 79 (1985), 383–407.

[FI] E. FOUVRY et H. IWANIEC, On a theorem of Bombieri-Vinogradov type, Mathematika, 27 (1980), 135–152.

[FM] E. FOUVRY et M. R. MURTY, On the Distribution of Supersingular Primes, Canadian Journal of Mathematics, 48 (1996) 81–104.

[H-B] D. R. HEATH-BROWN, Artin's conjecture for primitive roots, Q. J. Math. Oxford II, 37 (1986), 27–38.

[H-BP] D. R. HEATH-BROWN et S. J. PATTERSON, The distribution of Kummer sums at prime arguments, J. reine u. angewandte Math., 310 (1979), 111–130.

[I1] H. IWANIEC, Rosser's sieve, Acta. Arith., 36 (1980), 171–202.

[I2] H. IWANIEC, Topics in Classical Automorphic Forms, Graduate Studies in Mathematics, 17, American Mathematical Society (1997).

[K1] N. M. KATZ, Monodromy groups attached to families of exponential sums, Duke Math. J., 54-1 (1987), 41–56.

[K2] N. M. KATZ, Gauss Sums, Kloosterman Sums and Monodromy Groups, Annals of Maths. Studies 116, Princeton University Press.

[K3] N. M. KATZ, Exponential sums and differential equations, Annals of Math. Studies, 124, Princeton University Press.

[K4] N. M. KATZ, Exponential sums over finite fields and differential equations over the complex numbers, some interactions, Bull. Am. Math. Soc., 23 (1990), 269–309.

[KS] N. M. KATZ, P. SARNAK, Random Matrices, Frobenius Eigenvalues and Monodromy, Colloquium Pub., 45, Amer. Math. Soc., Providence, Rhode Island (1999).

[LT] S. LANG et H. TROTTER, Frobenius in GL_2-extensions, Springer Lecture Notes in Math., 504, Springer-Verlag (1976).

[Mi1] P. MICHEL, Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman I, Invent. Math., 121 (1995), 61–78.

[Mi2] P. MICHEL, Minoration de sommes d'exponentielles, Duke Math. J., 95 (1998), 227–240.

[Mo] L. J. MORDELL, On some exponential sums related to Kloosterman sums, Acta Arith., 21 (1972), 65–69.

[Sa] H. SALIÉ, Über die Kloostermannschen Summen $S(u, v; q)$, Math. Zeitschr., 34 (1931), 91–109.

[Sp] F. SPITZER, Principles of Random Walk, The University Series in Higher Mathematics, Van Nostrand Company (1964).

[Su] M. SUGIURA, Unitary Representations and Harmonic Analysis – An Introduction, (Second Edition), North-Holland Mathematical Library, 1990.

[V] R. C. VAUGHAN, Mean Value Theorems in Prime Number Theory, J. London Math.Soc.(2), 10 (1975), 153–162.

Manuscrit reçu le 20 novembre 2000,
accepté le 10 septembre 2001.

Étienne FOUVRY,
Université Paris-Sud
Mathématiques, Bât. 425
91405 Orsay Cedex (France).
fouvry@math.u-psud.fr
&
Philippe MICHEL,
Université Montpellier II, CC 051
Mathématiques
34095 Montpellier Cedex (France).
michel@math.univ-montp2.fr