AUTOUR DE LA CONJECTURE DE SATO-TATE POUR LES SOMMES DE KLOOSTERMAN I

P. MICHEL, Université Paris-Sud

Mathématiques, Bât. 425, 91405 ORSAY Cedex.
michel@matups.matups.fr

Notations

Nous ferons les conventions suivantes

e(.) désigne la fonction $\exp(2i\pi.)$ et $\mathrm{e}_q(.)$ la fonction $\exp(2i\pi./q)$,
pour r,s deux entiers (r, s) est leur plus grand diviseur commun,
si $(r, s) = 1$ on note $\overline{r}$ l'inverse de r modulo s,
$\tau_\kappa(n)$ désigne la fonction $\sum_{d_1 \dots d_\kappa | n} 1$,
$n \sim N$ signifie $N \leq n < 2N$,
si $(\lambda_m)_{m \leq M}$ est une suite finie de complexes on note $||\lambda|| := \left(\sum_{m \leq M} |\lambda_m|^2\right)^{1/2}$ sa norme L^2,

pour i entier positif ≥ 0, $\mathrm{sym}_i\, \theta$ désigne la fonction $\sin((i+1)\theta)/\sin\theta$; d'autre part $\mathrm{Sym}_i(SL_2)$ désigne la représentation puissance symétrique i-ième de $SL_2(\mathbb{C})$, elle est de dimension $i+1$, irréductible , et pour tout élément de $SU_2(\mathbb{C})$ de trace $2\cos\theta$, sa trace relativement à la représentation Sym_i est donnée par l'expression $\mathrm{sym}_i\, \theta$.

Dans toute la suite, les lettres p, q indicées ou non, seront réservées pour la désignation d'un nombre premier.

I.— Introduction

Soient l, m, n des entiers, et soit $S(l, m; n)$ la somme de Kloosterman

$$S(l, m; n) = \sum_{\substack{k \bmod n \\ (k,n)=1}} \mathrm{e}\Big(\frac{lk + m\overline{k}}{n}\Big).$$

Rappelons que c'est un réel non nul et que la majoration de Weil nous donne pour p un nombre premier avec $(m, p) = 1$:

$$|S(1, m; p)| \leq 2\sqrt{p};$$

on notera donc $\theta_{p,m}$ l'unique réel de $[0, \pi]$ tel que :

$$\frac{S(1, m; p)}{2\sqrt{p}} = \cos\theta_{p,m}.$$

La conjecture de Sato-Tate affirme alors que :

Conjecture. — *Soit m un entier non nul fixé, pour $P \to \infty$ la suite de réels $\{\theta_{p,m} \mid (m, p) = 1,\ p \leq P\}$ devient équidistribuée pour la mesure de Sato-Tate sur $[0, \pi]$, $\mu_{ST} := \frac{2}{\pi}\sin^2(\theta)d\theta$.*

En termes équivalents, si $\delta(\theta)$ est la mesure de Dirac en θ, on a, au sens de la convergence faible

$$\frac{1}{|\{p \leq P|\ (p, m) = 1\ \}|} \sum_{\substack{p \leq P \\ p \not| m}} \delta(\theta_{p,m}) \ \longrightarrow \mu_{ST},\ (P \to \infty)$$

Par un argument de densité (critère de Weyl), et par orthonormalité des fonctions $\mathrm{sym}_i(\theta)$ relativement à la mesure μ_{ST}, cette conjecture est équivalente à la suivante sur les *moments* des sommes de Kloosterman :

Soit m un entier non nul fixé ,pour tout entier positif i, on a, pour $P \to +\infty$

$$\frac{1}{|\{p \leq P|\ (m,p)=1\ \}|} \sum_{\substack{p \leq P \\ p \not| m}} \mathrm{sym}_i(\theta_{p,m}) \ \to \int_0^\pi \mathrm{sym}_i(\theta)\mu_{ST} = 0. \tag{1.0}$$

On sait extrêmement peu de choses sur cette conjecture ; ainsi, comme l'a remarqué Katz [Ka1], on ne sait pas si il y a une proportion positive de nombres premiers p, tels que les angles $\theta_{p,1}$ tombent dans un intervalle fixé de $[0,\pi]$, de longueur non nulle. Un espoir d'attaquer cette question, serait que la fonction L attachée aux sommes de Kloosterman soit modulaire (cf [Ka1] Introduction), mais pour l'instant cette voie semble très improbable. Une des principales raisons de croire à cette conjecture est le Théorème de Katz ci-dessous, conséquence des travaux de Deligne sur les conjectures de Weil [D] ; on dira avec Katz ([Ka2]) que l'énoncé suivant est de type "vertical" par opposition à l'énoncé (1.0) qui sera dit "horizontal" :

Théorème 0 ([Ka3]). — *Quand $p \to \infty$ les $p-1$ nombres $\{\theta_{p,m}\}_{m=1\ldots p-1}$ deviennent équidistribués pour la mesure de Sato-Tate. Autrement dit, on a, pour tout entier i non nul, et $p \to +\infty$*

$$\frac{1}{p-1} \sum_{m=1}^{p-1} \mathrm{sym}_i(\theta_{p,m}) \ \to \ 0.$$

Jusqu'à présent, la conjecture n'était étayée que par des énoncés verticaux, tels que le précédent [Ka2] ; dans le cas où le module de la somme de Kloosterman est un produit de deux nombres premiers, nous prouvons, dans cet article, un théorème dans la direction "horizontale" de la conjecture de Sato-Tate :

Théorème 1. — *Pour tout entier m non nul, il existe une proportion positive de couples (p,q) de nombres premiers distincts tels que*

$$|\frac{S(1,m;pq)}{4\sqrt{pq}}| \geq 0.16. \tag{1.1}$$

D'autre part, pour tout $\epsilon > 0$, il existe une proportion positive de couples (p,q) de nombres premiers distincts tels que

$$|\frac{S(1,m;pq)}{4\sqrt{pq}}| \leq \epsilon.$$

Proportion positive signifie ici, qu'il existe une constante α positive, telle que le nombre de couples (p,q) vérifiant la condition (1.1) ci-dessus, avec $p \leq x,\ q \leq x$ est minoré par

$$\alpha \frac{x^2}{\log^2 x} + o(\frac{x^2}{\log^2 x}).$$

Une propriété simple, mais fondamentale des sommes de Kloosterman est la propriété de *multiplicativité croisée* : pour $p \neq q$, on a l'égalité

$$\frac{S(1,m;pq)}{4\sqrt{pq}} = \frac{S(1,\overline{q}^2 m;p)}{2\sqrt{p}} \frac{S(1,\overline{p}^2 m;q)}{2\sqrt{q}}, \tag{1.2}$$

propriété que l'on réécrit sous forme condensée

$$\cos\theta_{pq,m} = \cos\theta_{p,\overline{q}^2 m} \cos\theta_{q,\overline{p}^2 m}$$

Ainsi, si on admet la conjecture de Sato-Tate, il n'est pas déraisonnable de penser que les angles $\theta_{pq,m}$ sont uniformément distribués relativement à la mesure $\mu_{ST,2}$, qui est l'image par l'application

$$\Phi : (\theta,\ \theta') \longrightarrow \arccos(\cos\theta \cos\theta'),$$

de la mesure sur $[0,\pi] \times [0,\pi]$, $\mu_{ST} \otimes \mu_{ST}$.

Le point de départ de notre preuve est une amélioration du théorème de Katz cité précédemment ; Dans celui-ci, prendre $p-1$ points n'est pas nécessaire pour avoir l'équidistribution : on peut montrer la

Proposition 2. — *Soit $\epsilon > 0$, et pour tout p, soit $\mathcal{M}_p$ un intervalle de longueur $l(\mathcal{M}_p)$ supérieure à $p^{1/2+\epsilon}$, inclus dans $[1,p-1]$. Alors pour tout entier i non nul, et pour $p \to +\infty$, on a*

$$\frac{1}{l(\mathcal{M}_p)} \sum_{m \in \mathcal{M}_p} \mathrm{sym}_i(\theta_{p,m}) \to 0.$$

Cette proposition n'est pas sans rappeler l'inégalité de Polya-Vinogradov sur les sommes de caractères. En fait, notre motivation première était de prouver des variations du théorème vertical, où les entiers m décrivent des ensembles moins réguliers que des intervalles (par exemple définis par convolution multiplicative d' ensembles quelconques "assez denses", ce qui est le cas si m est assujetti à n'avoir que de grands facteurs premiers) ; après des manipulations élémentaires, on est ramené à prouver certaines propriétés géométriques du faisceau de Kloosterman. Alors (cf. Corollaire 2.11), on pourra majorer non trivialement des formes bilinéaires de la forme ((α_m) et (β_n) désignant des complexes) :

$$\sum_m \sum_n \alpha_m \beta_n \,\mathrm{sym}_i(\theta_{p,\overline{mn}^2}).$$

Grâce au crible, on peut alors établir le théorème suivant (nous avons préféré donner une variante, la Proposition 3.2, nécessaire pour le Théorème 1) :

Théorème 3. — *Quand $p \to \infty$, les angles $\{\theta_{p,q}\}_{q<p}$ sont équidistribués pour la mesure de Sato-Tate μ_{ST}, autrement dit, pour tout entier i non nul, on a*

$$\sum_{q<p} \mathrm{sym}_i(\theta_{p,q}) = o_i(\frac{p}{\log p}).$$

On peut aussi, considérer le problème dual : celui de l'équidistribution des angles $\{\theta_{p,m}\}_{m<p}$ où m n'a que de petits facteurs premiers : plus précisement, les angles $\{\theta_{p,m}\}_{m<p}$ sont équidistribués suivant la mesure de Sato-Tate, si m parcourt l'ensemble des entiers m ($1 \leq m < p$), dont tous les facteurs premiers sont inférieurs à $\exp(\sqrt{\log p})$. Nous n'en donnons pas de démontration.

Notre méthode peut s'étendre à des majorations non triviales de sommes de type II

$$\sum_m \sum_n \alpha_m \beta_n \,\mathrm{sym}_i(\theta_{p,f(m,n)}),$$

où $f(m,n)$ est une fraction de $\mathbb{Z}(m,n)$ très générale. Faute d'application nous n'avons pas poursuivi cette étude.

Pour revenir au problème initial, disons qu'il est possible de généraliser le Théorème 1 suivant deux directions : d'une part, quand le module des sommes de Kloosterman est le produit d'un nombre fixé ≥ 2 de nombres premiers distincts ; D'autre part, cette méthode, ainsi que les résultats d'équidistribution qui en découlent (Proposition 2 et Théorème 3) ne sont pas strictement propres aux sommes de Kloosterman. Par exemple, elle peut s'étendre sans trop de difficultés, aux sommes d'exponentielles à un paramètre, obtenues (à l'instar des sommes de Kloosterman) par transformée de Fourier-Deligne-Laumon (ce type de somme a été étudié très complètement par Katz [Ka4]), et également aux sommes de Kloosterman à plusieurs variables,

$$S_j(m;n) := \sum_{\substack{k_1,\ldots k_j \mod j \\ k_1 k_2 \ldots k_j = m \mod n}} \mathrm{e}\big(\frac{k_1 + \ldots + k_j}{n}\big).$$

Les preuves sont essentiellement les mêmes, quoique plus compliquées dans leurs notations, aussi nous avons choisi de n'exposer que le cas le plus simple.

Je tiens à remercier le Professeur E. Fouvry, mon directeur de thèse, pour m'avoir mis en contact avec la conjecture de Sato-Tate, et pour toutes les suggestions qu'il a faites au long de ce travail, ainsi que les Professeurs Katz et Laumon pour d'intéressantes discussions.

II.— Estimations de formes bilinéaires

Le but de cette section, est d'établir des majorations de certaines sommes de types I et II selon la terminologie de la théorie analytique des nombres, relatives aux sommes de Kloosterman. Ces sommes apparaissent naturellement *via* les identités de crible. Ces majorations dépendent de propriétés géométriques du faisceau de Kloosterman démontrées dans la première partie de cette section.

II.1.— Un peu de géométrie algébrique

On se fixe p un nombre premier, $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$, et ℓ un nombre premier $\neq p$, et on fixe $\overline{\mathbb{Q}}_\ell$ une cloture algébrique de $\mathbb{Q}_\ell$ *dans* $\mathbb{C}$.

On commence par rappeler quelques lemmes très classiques (voir [Ka3]). Pour cela, on se donne X_p une courbe affine sur $\mathbb{F}_p$, complément d'un ensemble fini, $\mathcal{S}$ de $\mathbb{P}^1(\mathbb{F}_p)$. On se donne également un faisceau $\mathcal{F}$, sur X_p, lisse, pur de poids 0; rappelons, que celà équivaut à se donner une représentation du groupe fondamental *arithmétique*, π_1^{arith} de X_p relativement à un point géométrique fixé de X_p, dont les traces des frobenius sont des entiers algébriques de valeur absolue égale à 1; la restriction de cette représentation au groupe fondamental *géométrique* π_1^{geom} de X_p (c'est à dire le groupe fondamental de $X_p \otimes \overline{\mathbb{F}}_p$) est appelée représentation géométrique associée. On notera V le sous-espace vectoriel sous-jacent à $\mathcal{F}$, et $G_{geom}(\mathcal{F})$ son groupe de monodromie géométrique. On a

Lemme 2.0 (Formule de Grothendieck-Ogg-Shafarevitch). — *Avec les conventions précédentes, on a l'égalité*

$$\chi_c(X_p \otimes \overline{\mathbb{F}}_p, \mathcal{F}) = (2 - |\mathcal{S}|)rang(\mathcal{F}) - \sum_{s\in\mathcal{S}} \mathrm{Swan}_s(\mathcal{F}).$$

Lemme 2.1. — *Si $G_{geom}(\mathcal{F})$ agit irréductiblement sur V, alors on a*

$$|\sum_{x\in X_p(\mathbb{F}_p)} tr(\mathrm{Frob}_x, \mathcal{F})| \leq |\chi_c(X_p \otimes \overline{\mathbb{F}}_p, \mathcal{F})| p^{1/2}.$$

Preuve. D'après la formule de Lefschetz-Grothendieck, on a

$$\sum_{x\in X_p(\mathbb{F}_p)} tr(\mathrm{Frob}_x, \mathcal{F}) = \sum_{j=0}^{2} (-1)^j tr(\mathrm{Frob}_p \,|H_c^j(X_p \otimes \overline{\mathbb{F}}_p, \mathcal{F})),$$

$H_c^0 = 0$ car X_p est affine; $H_c^1(\ ,\mathcal{F})$ est mixte de poids ≤ 1 par le Théorème fondamental de Deligne; $H_c^2(\ ,\mathcal{F}) = 0$ compte-tenu de son interprétation en terme des coinvariants de G_{geom}. □

Le Lemme suivant permet de majorer la caractéristique d'Euler de faisceaux associés à $\mathcal{F}$:

Lemme 2.2. — *Supposons $|\mathcal{S}| \geq 2$. Soit ρ une représentation de $GL(V)$ et $\rho(\mathcal{F})$ le faisceau lisse sur X_p, obtenu par composition de $\mathcal{F}$ avec ρ. Alors on a l'inégalité*

$$|\chi_c(X_p \otimes \overline{\mathbb{F}}_p, \rho(\mathcal{F}))| \leq \dim(\rho).|\chi_c(X_p \otimes \overline{\mathbb{F}}_p, \mathcal{F})|.$$

Preuve. Soit $s \in \mathcal{S}$, et ϵ_s le plus grand saut de $\mathcal{F}$ dans la décomposition de l'inertie sauvage en s, alors on a

$$\epsilon_s \leq \mathrm{Swan}_s(\mathcal{F}) \leq \epsilon_s.rang(\mathcal{F}).$$

En appliquant cette égalité a $\mathcal{F}$ et à $\rho(\mathcal{F})$, on en déduit que

$$\mathrm{Swan}_s(\rho(\mathcal{F})) \leq \dim(\rho)\,\mathrm{Swan}_s(\mathcal{F});$$

on conclut avec le Lemme 2.0. □

Nous en venons au coeur de notre sujet : On note (cf. [Ka3](4.1.4)) $\mathcal{K}l$ le $\overline{\mathbb{Q}_\ell}$-faisceau lisse sur $\mathbb{G}_m(\mathbb{F}_p) := \mathbb{F}_p^*$, dit *faisceau de Kloosterman*, tordu de façon à être pur de poids 0 : qu'il suffise de dire que pour tout point m de $\mathbb{F}_p^*$, on a

$$tr(\mathrm{Frob}_m, \mathcal{K}l) = \frac{S(1, m; p)}{\sqrt{p}} \text{ et } det(\mathrm{Frob}_m, \mathcal{K}l) = 1.$$

Rappelons ([Ka3](4.1.4)) que $\mathcal{K}l$ est lisse, de rang 2, pur de poids 0, de déterminant trivial, modéré en 0 avec un seul bloc de Jordan et totalement sauvage en ∞ avec $\mathrm{Swan}_\infty(\mathcal{K}l) = 1$, et par conséquent avec un seul saut situé en 1/2. Toutes ces données on permit à Katz de determiner le groupe de monodromie géométrique de $\mathcal{K}l$, c'est un des points centraux de [Ka3] ([Ka3] Chap 10) :

Théorème 2.3. — *On a l'égalité*

$$G_{geom}(\mathcal{K}l) = SL_2(\overline{\mathbb{Q}_\ell})$$

Pour $a \in \mathbb{F}_p$, on note le faisceau translaté $\mathcal{K}l_a := trans_a^*(\mathcal{K}l)$, où $trans_a$ est le morphisme de translation :

$$\begin{array}{rccc} trans_a : & \mathbb{G}_m(\mathbb{F}_p) & \to & \mathbb{G}_m(\mathbb{F}_p) \\ & x & \to & ax; \end{array}$$

alors $\mathcal{K}l_a$ hérite des propriétés de $\mathcal{K}l$, en particulier

$$tr(\mathrm{Frob}_m, \mathcal{K}l_a) = \frac{S(1, am; p)}{\sqrt{p}}.$$

Enfin on désigne par $V_{\mathcal{K}l}$ le $\overline{\mathbb{Q}_\ell}$-espace vectoriel sous-jacent à la représentation définie par $\mathcal{K}l$ (et de même pour $\mathcal{K}l_a$). On va prouver que si $a \neq 1$, $\mathcal{K}l$ et $\mathcal{K}l_a$ satisfont au critère de Goursat-Kolchin-Ribet([Ka4]1.8.2) ; le résultat important pour notre propos est le

Lemme 2.4. — *Pour tout faisceau $\mathcal{L}$, lisse de rang 1 sur $\mathbb{G}_m(\overline{\mathbb{F}}_p)$, pour tout $a \in \mathbb{F}_p^*$ $(a \neq 1)$. Les faisceaux (sur $\overline{\mathbb{F}}_p^*$) $\mathcal{K}l$ et $\mathcal{K}l_a \otimes \mathcal{L}$ ne sont pas isomorphes.*

Preuve. on s'inspire de [Ka3]p.270. Le Lemme 2.0, nous donne :

$$\chi_c(\mathbb{G}_m(\overline{\mathbb{F}_p}); \mathcal{K}l \otimes \mathcal{K}l_a) = -\operatorname{Swan}_0(\mathcal{K}l \otimes \mathcal{K}l_a) - \operatorname{Swan}_\infty(\mathcal{K}l \otimes \mathcal{K}l_a)$$

Comme $\mathcal{K}l \otimes \mathcal{K}l_a$ est modéré en 0 ($\mathcal{K}l$ et $\mathcal{K}l_a$ le sont), on voit que $\operatorname{Swan}_\infty(\mathcal{K}l \otimes \mathcal{K}l_a)$ est le degré de la fonction L associée à $\mathcal{K}l \otimes \mathcal{K}l_a$:

$$L(T; \mathcal{K}l \otimes \mathcal{K}l_a) = \exp\Big(\sum_{r \geq 1} S_r \frac{T^r}{r}\Big)$$

où

$$\begin{aligned} S_r &= \sum_{m \in \mathbb{F}_{p^r}^*} tr(\operatorname{Frob}_m, \mathcal{K}l \otimes \mathcal{K}l_a) \\ &= \frac{1}{p^r} \sum_{m \in \mathbb{F}_{p^r}^*} \sum_{x_1, x_2 \in \mathbb{F}_{p^r}^*} \mathrm{e}_p\big(tr_{\mathbb{F}_{p^r}/\mathbb{F}_p}(\overline{x_1} + \overline{x_2} + m(x_1 + a x_2))\big) \\ &= \sum_{x_1 = -a x_2} \mathrm{e}_p\big(tr_{\mathbb{F}_{p^r}/\mathbb{F}_p}(\overline{x_1} + \overline{x_2})\big) \quad - \frac{1}{p^r} \\ &= -1 - \frac{1}{p^r} \text{ (car } a \neq 1) \end{aligned}$$

donc $L = (1-T)(1-p^{-1}T)$, L est de degré 2, c'est à dire que $\operatorname{Swan}_\infty(\mathcal{K}l \otimes \mathcal{K}l_a) = 2$. De même, pour $a = 1$, on voit que $\operatorname{Swan}_\infty(\mathcal{K}l \otimes \mathcal{K}l) = 1$. On en déduit en particulier que $\mathcal{K}l \otimes \mathcal{K}l_a$ est totalement sauvage en ∞, tous ses sauts étant situés en $1/2$; cela ne nous servira pas.

Démontrons maintenant le lemme ; supposons que l'on ait $\mathcal{L} \otimes \mathcal{K}l_a \simeq \mathcal{K}l$, alors $\mathcal{L}$ est modéré en ∞ : en effet si $\mathcal{L}$ était totalement sauvage en ∞, $\mathcal{L}$, étant de rang 1, n'aurait qu'un seul saut, situé en $\operatorname{Swan}_\infty(\mathcal{L}) \geq 1$, alors (cf [Ka3] 1.3), en se restreignant aux I_∞-représentations, on aurait :

$$V_{\mathcal{L}}(\operatorname{Swan}_\infty(\mathcal{L})) \otimes V_{\mathcal{K}l_a}(1/2) \subset V_{\mathcal{L}} \otimes V_{\mathcal{K}l_a}(\max\{\operatorname{Swan}_\infty(\mathcal{L}), 1/2\}) \simeq V_{\mathcal{K}l}(\operatorname{Swan}_\infty(\mathcal{L})) = 0$$

car $\mathcal{K}l$ n'a qu'un seul saut en $1/2$. Comme

$$\dim\ V_{\mathcal{L}}(\operatorname{Swan}_\infty(\mathcal{L})) \otimes V_{\mathcal{K}l_a}(1/2) = \dim\ V_{\mathcal{L}} \otimes V_{\mathcal{K}l_a} = 2,$$

c'est absurde, donc $\mathcal{L}$ est modéré en ∞.

Maintenant, on aurait par hypothèse

$$\mathcal{L} \otimes \mathcal{K}l_a \otimes \mathcal{K}l \simeq \mathcal{K}l \otimes \mathcal{K}l,$$

$\mathcal{L}$ étant modéré en ∞, cela conduirait à

$$\begin{aligned} \operatorname{Swan}_\infty(\mathcal{L} \otimes \mathcal{K}l_a \otimes \mathcal{K}l) &= \operatorname{Swan}_\infty(\mathcal{K}l_a \otimes \mathcal{K}l) = 2 \ (a \neq 1) \\ &= \operatorname{Swan}_\infty(\mathcal{K}l \otimes \mathcal{K}l) = 1, \end{aligned}$$

ce qui est absurde et conclut la preuve du lemme.

□

Comme $\mathcal{K}l^{\check{}}$ (le dual de $\mathcal{K}l$) est isomorphe à $\mathcal{K}l$ ([Ka3] Chap. 4), on en déduit que $\mathcal{K}l$ et $\mathcal{K}l_a$ satisfont au critère de Goursat-Kolchin-Ribet ([Ka4] 1.8.2). De ce critère, on déduit la

Proposition 2.5. — *Pour $a \neq 1 \mod p$; le groupe de monodromie géométrique de faisceau $\mathcal{K}l \oplus \mathcal{K}l_a$ est*

$$G_{geom}(\mathcal{K}l \oplus \mathcal{K}l_a) = SL_2 \times SL_2 \subset GL_4.$$

Ce groupe agit (irréductiblement) sur l'espace vectoriel de dimension 4, $V_{\mathcal{K}l} \oplus V_{\mathcal{K}l_a}$.

Pour prouver le Théorème 1 nous aurons besoin d'une légère variante de cette dernière Proposition :

On note $[-2]$, le morphisme de groupe algébrique de $\mathbb{G}_m(\mathbb{F}_p)$ défini par

$$[-2] : \begin{array}{ccc} \mathbb{G}_m(\mathbb{F}_p) & \longrightarrow & \mathbb{G}_m(\mathbb{F}_p) \\ x & \longrightarrow & x^{-2} \end{array}$$

si $p > 2$, c'est un revêtement étale galoisien de degré 2 de $\mathbb{G}_m(\mathbb{F}_p)$, modérément ramifié en 0 et ∞. Dans ce cas considérons le *pull-back* de $\mathcal{K}l$ par ce morphisme : on a la proposition suivante

Proposition 2.6. — *Si p est impair ; soit a un entier premier à p ; le faisceau pull-back $[-2]^*\mathcal{K}l_a$ est lisse, de rang 2, pur de poids 0 avec*

$$tr(\mathrm{Frob}_m, [-2]^*\mathcal{K}l_a) = \frac{S(1, a\overline{m}^2; p)}{\sqrt{p}},$$

modérément ramifié en ∞, sauvagement ramifié en 0 avec

$$\mathrm{Swan}_0([-2]^*\mathcal{K}l_a) = 2.$$

De plus, si $a \neq 1 \bmod p$, le groupe de monodromie géométrique du faisceau

$$[-2]^*\mathcal{K}l \oplus [-2]^*\mathcal{K}l_a, \ (resp.\ [-2]^*\mathcal{K}l)$$

est isomorphe à $SL_2 \times SL_2 \subset GL_4$ (resp. $SL_2 \subset GL_2$).

Preuve. les 4 premières assertions sont mises pour mémoire, le calcul du conducteur de Swan en 0, résulte de ce que $p \neq 2$ et de [Ka3] 1.14 :

$$\mathrm{Swan}_0([-2]^*\mathcal{K}l_a) = 2\,\mathrm{Swan}_\infty(\mathcal{K}l_a) = 2.$$

La représentation géométrique associée au faisceau $[-2]^*\mathcal{K}l$, est simplement la restriction à un sous-groupe d'indice 2 de la représentation géométrique du faisceau $\mathcal{K}l$. Or, d'après la Proposition 2.5, le groupe de monodromie géométrique du faisceau $\mathcal{K}l \oplus \mathcal{K}l_a$ est isomorphe à $SL_2 \times SL_2 \subset GL_4$ qui est connexe ; et donc, c'est également celui son pull-back par $[-2]$, c'est à dire $[-2]^*\mathcal{K}l \oplus [-2]^*\mathcal{K}l_a$.

□

Si on considère les représentations définies par $\mathcal{K}l \oplus \mathcal{K}l_a$, $[-2]^*\mathcal{K}l \oplus [-2]^*\mathcal{K}l_a$ l'image par ces représentations de π_1^{arith} est contenue dans le groupe de monodromie géométrique associé ; comme c'est expliqué dans [Ka3] Chap. 3, on en déduit, par les Propositions 2.5 et 2.6 et le Lemme 2.2 le :

Théorème 2.7. — *Soit un entier $a \neq 0, 1$, quand $p \to \infty$ les couples de nombres $\{(\theta_{p,m}, \theta_{p,am})\}_{m=1\ldots p-1}$ ainsi que $\{(\theta_{p,\overline{m}^2}, \theta_{p,a\overline{m}^2})\}_{m=1\ldots p-1}$ deviennent équidistribués pour la mesure de Sato-Tate sur $[0,\pi]\times[0,\pi]$: $\mu_{ST}(\theta)\otimes\mu_{ST}(\theta')$. En particulier, pour tout couple d'entiers $i, j \geq 0$ tels que $i + j > 0$, on a les égalités*

$$\frac{1}{p-1}\sum_{m=1}^{p-1} \mathrm{sym}_i(\theta_{p,m})\,\mathrm{sym}_j(\theta_{p,am}) = O_{i,j}(p^{-1/2}). \tag{2.0}$$

$$\frac{1}{p-1}\sum_{m=1}^{p-1} \mathrm{sym}_i(\theta_{p,\overline{m}^2})\,\mathrm{sym}_j(\theta_{p,a\overline{m}^2}) = O_{i,j}(p^{-1/2}). \tag{2.1}$$

Preuve. cela résulte des Lemmes 2.1 et 2.2, et du fait que le faisceau lisse sur $\mathbb{G}_m(\mathbb{F}_p)$, pur de poids 0,

$$\mathrm{Sym}_i([-2]^*\mathcal{K}l)\otimes\mathrm{Sym}_j([-2]^*\mathcal{K}l_a),$$

est, par construction, géométriquement irréductible pour $i+j>0$ par la Proposition 2.6. □

II.2.— Inégalités de type Polya-Vinogradov

Soit $g(m)$, une fonction sur $\mathbb{F}_p$, et $\mathcal{M}_p$ un intervalle inclus dans $[1, 2p]$ de longueur au plus p ; on veut majorer des sommes incomplètes de la forme

$$\sum_{m\in\mathcal{M}_p} g(m).$$

La méthode classique est de compléter ces sommes par transformation de Fourier ; en effet, cette dernière somme vaut

$$\sum_{k\in\mathbb{F}_p} \mathcal{F}(g,k;p)\sum_{m\in\mathcal{M}_p} \mathrm{e}_p(km),$$

où $\mathcal{F}$ désigne la transformée de Fourier :

$$\mathcal{F}(g,k;p) := \frac{1}{p}\sum_{x\in\mathbb{F}_p} g(x)\,\mathrm{e}_p(-kx);$$

on a alors

$$\left|\sum_{m\in\mathcal{M}_p} g(m) - \frac{l(\mathcal{M}_p)}{p}\sum_{m=1}^{p} g(m)\right| \ll p\sum_{k=1}^{p-1}\frac{1}{k}|\mathcal{F}(g,k;p)|. \tag{2.3}$$

On applique maintenant ce raisonnement à diverses fonctions g définies sur $\mathbb{F}_p^*$, que l'on étend par 0 sur $\mathbb{F}_p$ tout entier.

Proposition 2.8. — *Soient $i,\ j$ des entiers tels que $i+j>0$. Soit $a\in\mathbb{F}_p,\ (a\neq 1)$ (si $a=0$ on fait la convention que $j=0$ et $\mathrm{sym}_j(\theta_{p,a\overline{m}^2})=1$). Alors, pour tout $k\in\mathbb{F}_p$, on a les égalités*

$$\mathcal{F}(\mathrm{sym}_i(\theta_{p,\overline{m}^2})\,\mathrm{sym}_j(\theta_{p,a\overline{m}^2}),k;p)=O_{i,j}(p^{-1/2}).$$

Preuve. Si $k=0$, on applique le Théorème 2.7; dans le cas contraire, on raisonne comme suit : rappelons qu'à un caractère non trivial ψ de $\mathbb{F}_p$ est associé un faisceau ,$\mathcal{L}_\psi$, sur $\mathbb{A}^1(\mathbb{F}_p)$; on rappelle également ([Ka3] Chap. 4.) que ce faisceau est lisse, de rang 1, , pur de poids 0, sauvagement ramifié en ∞, de conducteur de Swan 1. D'après le Lemme 2.1, la Proposition 2.8 sera démontrée si on prouve que le groupe de monodromie géométrique du faisceau $\mathcal{L}_\psi\otimes\mathrm{Sym}_i([-2]^*\mathcal{K}l)\otimes\mathrm{Sym}_j([-2]^*\mathcal{K}l_a)$ sur $\mathbb{G}_m(\overline{\mathbb{F}}_p)$ agit irréductiblement (si $i=0$ le terme Sym_i n'apparait simplement pas dans l'expression précédente) , et qu' on peut borner la caractéristique d' Euler de ce faisceau par une constante indépendante de p : cette dernière partie est accomplie grâce à la formule de Grothendieck-Ogg-Shafarevitch (Lemme 2.0 et 2.2); en effet, les conducteurs de Swan des faisceaux $\mathcal{L}_\psi$, $\mathrm{Sym}_i([-2]^*\mathcal{K}l)$, $\mathrm{Sym}_j([-2]^*\mathcal{K}l_a)$ sont eux-même majorés par des constantes indépendantes de p. Pour la première partie, on remarque que $\mathcal{L}_\psi$ étant de rang 1, la représentation géométrique associée à $\mathcal{L}_\psi\otimes\mathrm{Sym}_i([-2]^*\mathcal{K}l)\otimes\mathrm{Sym}_j([-2]^*\mathcal{K}l_a)$ ne diffère de celle associée à $\mathrm{Sym}_i([-2]^*\mathcal{K}l)\otimes\mathrm{Sym}_j([-2]^*\mathcal{K}l_a)$ que par multiplication par des scalaires. Comme cette dernière est irréductible (Proposition 2.6), il en est de même de la première. □

Compte tenu de (2.3) appliqué à $g(m)=\mathrm{sym}_i(\theta_{p,\overline{m}^2})\,\mathrm{sym}_j(\theta_{p,a\overline{m}^2})$, et de la Proposition 2.8, on obtient en sommant sur k, le

Corollaire 2.9. — *Si $a\neq 0,1(\ mod\ p)$, si i et j sont des entiers tels que $i+j>0$, et avec la convention de la Proposition 2.8, on a l'égalité*

$$\sum_{\substack{m\in\mathcal{M}_p\\ m\not\equiv 0(\mathrm{mod}\ p)}}\mathrm{sym}_i(\theta_{p,\overline{m}^2})\,\mathrm{sym}_j(\theta_{p,a\overline{m}^2})=O_{i,j}\big(p^{1/2}\log p\big).$$

Le Corollaire 2.9 majore donc non trivialement la fonction $\mathrm{sym}_i(\theta_{p,\overline{m}^2})\,\mathrm{sym}_j(\theta_{p,a\overline{m}^2})$ sur tout intervalle de longueur $\gg p^{1/2}\log p$. Ceci est à rapprocher de la célèbre inégalité de Polya-Vinogradov sur les sommes de caractères. On peut aussi voir ce Corollaire comme une majoration de type I. Signalons que les Corollaires 2.9 et 2.10 (ci-dessous) sont valables (et même plus faciles à démontrer) si la fraction rationnelle $m\to\overline{m}^2$ est remplacée par $m\to m$. En particulier, le Corollaire 2.9 donne

$$\sum_{\substack{m\in\mathcal{M}_p\\ m\not\equiv 0(\mathrm{mod}\ p)}}\mathrm{sym}_i(\theta_{p,m})=O_i(p^{1/2}\log p),$$

ce qui fournit la démonstration de la Proposition 2.

Corollaire 2.10. — *Soit $\epsilon > 0$, et pour tout p, soit $\mathcal{M}_p$ un intervalle de longueur $l(\mathcal{M}_p)$ supérieure à $p^{1/2+\epsilon}$ inclus dans $[1, 2p-1]$, quand $p \to \infty$ les couples de nombres $\{(\theta_{p,\overline{m}^2}, \theta_{p,a\overline{m}^2})\}_{m\in\mathcal{M}_p,(m,p)=1}$ deviennent équidistribués pour la mesure de Sato-Tate sur $[0,\pi]\times[0,\pi]$*

Nous pouvons maintenant traiter des sommes de type II, en montrant le

Corollaire 2.11. — *Soient $(\alpha_m)_{m\leq M}$, $(\beta_n)_{n\leq N}$, des suites de complexes, $MN \leq 2p-1$, alors pour tout $i \geq 1$, on a la relation*

$$\sum_{\substack{1\leq m\leq M\\ 1\leq n\leq N\\ (mn,p)=1}} \alpha_m\beta_n \operatorname{sym}_i(\theta_{p,\overline{mn}^2}) \ \ll_i \|\alpha\|\|\beta\|(MN)^{1/2}\big(N^{-1/2}+M^{-1/2}p^{1/4}(\log p)^{1/2}\big).$$

Preuve. Par l'inégalité de Cauchy-Schwarz la somme considérée vérifie

$$\Big|\sum\Big|^2 \leq \ \|\alpha\|^2 \sum_{n_1,n_2} \beta_{n_1}\overline{\beta_{n_2}} \sum_m \operatorname{sym}_i(\theta_{p,\overline{mn_1}^2}) \operatorname{sym}_i(\theta_{p,\overline{mn_2}^2})$$
$$\ll \|\alpha\|^2\|\beta\|^2 M + \|\alpha\|^2 \sum_{n_1\not\equiv\pm n_2 (\mathrm{mod}\, p)} \beta_{n_1}\overline{\beta_{n_2}} \sum_m \operatorname{sym}_i(\theta_{p,\overline{mn_1}^2}) \operatorname{sym}_i(\theta_{p,\overline{mn_2}^2}).$$

Si $n_1 \not\equiv \pm n_2 \mod p$, une légère adaptation du Corollaire 2.9 donne

$$\sum_m \operatorname{sym}_i(\theta_{p,\overline{mn_1}^2}) \operatorname{sym}_i(\theta_{p,\overline{mn_2}^2}) \ll_i \ p^{1/2}\log p$$

et

$$\sum_{n_1\not\equiv n_2 (\mathrm{mod}\, p)} \beta_{n_1}\overline{\beta_{n_2}} \ll \|\beta\|^2 N$$

et le corollaire est démontré. Ce corollaire est intéressant pour $M \gg p^{1/2}\log p$ et $N \geq 1$. □

Remarque. Tous les résultats 2.8, 2.9, 2.10, 2.11 restent vrais si on remplace dans les expressions $\theta_{p,\overline{m}^2}$ par des $\theta_{p,b\overline{m}^2}$, où $(b,p)=1$, et les majorations sont indépendantes de b.

III.— l'Intrusion du crible

Nous allons maintenant établir une variante du Théorème 3, nécessaire à la preuve du Théorème 1 (la Proposition 3.2) ; on commence par un résultat intermédiaire, impliquant des entiers sans petits facteurs premiers puis on passera aux nombres premiers. Le lecteur verifiera sans peine que pour démontrer le Théorème 3, il suffit de remplacer dans les expressions ci-dessous, les $\theta'_{p,m}$ par des $\theta_{p,m}$.

Soit $P(z) = \prod_{p'<z} p'$ pour $z \geq 2$. Pour détecter les entiers avec de grands facteurs premiers nous aurons recours au Lemme de crible suivant (voir par exemple le corollaire du Lemme 1 de [F-I]), qui est obtenu par itération de l'identité de Buchstab :

Lemme 3.0. — *Soit $f_z(m)$ la fonction caractéristique des entiers $\{m\ ;\ p'|m \Longrightarrow p' > z\}$ et soit $F(m)$ une fonction arithmétique s'annulant pour presque tout m, alors si $D \geq z \geq 2$ on a la majoration :*

$$\big|\sum_m f_z(m)F(m)\big| \leq \sum_{\substack{d\leq D\\ d|P(z)}} \big|\sum_m F(dm)\big| + \sum_{p'<z} \sum_{\substack{D/p'^2\leq d<D/p'\\ p'd|P(z)}} \big|\sum_m f_{p'}(m)F(p'dm)\big|.$$

Soit x un réel positif assez grand, et p un nombre avec $p \sim x$. Pour simplifier les notations on posera pour tout $m \in \mathbb{F}_p^*$

$$\theta'_{p,m} := \theta_{p,\overline{m}^2}.$$

Dans un premier temps, nous montrerons la

Proposition 3.1. — *Posons*

$$z = \frac{x^{1/2}}{\log^{100} x},$$

alors, on a pour tout $i \geq 1$, on a

$$\sum_{m\sim x,(m,p)=1} f_z(m)\,\mathrm{sym}_i(\theta'_{p,m}) \ll_i \frac{x}{\log^2 x}$$

Compte tenu du fait que pour tout $\beta < 1$, on a $|\{m \sim x; p'|m \Longrightarrow p' > x^\beta\}| \gg x/\log x$, cette proposition implique l'équidistribution, quand $p \to \infty$, des $\theta_{p,\overline{m}^2}$ pour les nombres $m \sim x$ ayant tous leurs facteurs premiers $> \frac{x^{1/2}}{\log^{100} x}$.

Preuve. On pose $z = \dfrac{x^{1/2}}{\log^{100} x}$, soit $D > z$ à déterminer ; d' après le Lemme 3.0, on a :

$$\begin{aligned}\big|\sum_{\substack{m\sim x\\ p\not|m}} f_z(m)\,\mathrm{sym}_i(\theta'_{p,m})\big| \leq & \sum_{\substack{d\leq D\\ d|P(z)}} \big|\sum_m \mathrm{sym}_i(\theta'_{p,dm})\big| \\ & + \sum_{p'<z} \sum_{\substack{D/p'^2\leq d<D/p'\\ p'd|P(z)}} \big|\sum_m f_{p'}(m)\,\mathrm{sym}_i(\theta'_{p,p'dm})\big|.\end{aligned}$$

Le premier terme du membre de droite est majoré par

$$Dx^{1/2}\log x \tag{3.0}$$

en vertu du Corollaire 2.9 (appliqué avec $j = 0$). Le deuxième terme de droite est une somme de type II ; on la décompose en

$$S_1 + S_2 := \sum_{p'\leq z'} + \sum_{z'<p'<z} \tag{3.1}$$

avec $z' = x^{1/8}$. S_2 est la somme difficile : on pose $\Delta = 1 + \log^{-\delta} x$ (δ à fixer ultérieurement), et par un découpage Δ-adique on veut rendre les variables p', m et d indépendantes.

III.1.— Découpage des variables

Soient $P'^*,\ D'^*,\ M^*$ des variables à valeurs dans les ensembles respectifs

$$P'^* \in \{\ z,\ \Delta^{-1}z, \Delta^{-2}z, \ldots\} \cap]z'\Delta^{-1}, z]$$
$$D'^* \in \{\ D/z',\ \Delta^{-1}D/z', \ldots\} \cap]\Delta^{-1}, D/z']$$
$$M'^* \in \{\ xz^2/(Dz'),\ \Delta^{-1}xz^2/(Dz'), \ldots\} \cap]\Delta^{-1}, xz^2/(Dz')].$$

La somme S_2 est somme des $O(\log^{3\delta+3} x)$ sommes de la forme

$$S(P'^*, D'^*, M'^*) = \sum_{p',d} \Big| \sum_{m} f_{P'^*}(m) \operatorname{sym}_i(\theta'_{p,p'dm}) \Big|, \tag{3.2}$$

où les variables $p',\ d,\ m$ satisfont d'une part

$$p' \in]P'^*\Delta^{-1}, P'^*],\ d \in]D'^*\Delta^{-1}, D'^*],\ m \in]M'^*\Delta^{-1}, M'^*], \tag{3.3}$$

et vérifient de surcroit les conditions

$$z' < p' < z;\quad \frac{D}{p'^2} \le d < \frac{D}{p'};\quad p'dm \sim x$$

$$p'd | P(z);\quad p'' | m \Longrightarrow p'' > p'.$$

Il est clair que certaines sommes $S(P'^*, D'^*, M'^*)$ sont nulles ; par exemple, si $P'^*D'^*M'^* > 2x\Delta^3$ ou si $D'^* < D/P'^{*2}$. La contribution à S_2 des sommes $S(\ )$ telles que

$$P'^*D'^*M'^*\Delta^{-3} < x \text{ ou bien } P'^*D'^*M'^* \ge 2x$$

est majorée par

$$(i+1) \sum_{x \le n \le x\Delta^3} \tau_3(n)\ + (i+1) \sum_{2x\Delta^{-3} \le n \le 2x} \tau_3(n) \ll x(\log x)^{2-\delta}.$$

Cela nous permet de supprimer les conditions $x \le p'dm < 2x$. De même, la contribution à S_2 des sommes $S(\ )$ telles que l'une des conditions suivantes n'est pas vérifiée, est majorée par $x(\log x)^{1-\delta}$,

$$\frac{D}{P'^{*2}\Delta^{-2}} \le D'^*\Delta^{-1},\ D'^* < \frac{D}{P'^*};$$

on peut donc supprimer la condition $D/p'^2 \le d < D/p'$; de même, on lève la contrainte $z' < p' < z$. Finalement, par le Théorème des Nombres Premiers, l'erreur totale que l'on

fait en négligeant, pour chaque somme $S(\ )$, la contrainte $p''|m \Longrightarrow p'' > p'$ est majorée par

$$\begin{aligned}
&\ll \sum_{z'<p'<z} \sum_{d\le D} \sum_{\substack{m\le 2x/dp' \\ \exists p',\ p"|m, p'\Delta^{-1}\le p''<p'}} 1 \\
&\ll \sum_{z'<p'<z} \sum_{d\le D} \sum_{p'\Delta^{-1}\le p''<p'} \frac{2x}{p'dp''} \\
&\ll \{ \sum_{z'<p'<z} \sum_{d\le D} \frac{1}{p'd} \{\log_2(p') - \log_2(p'\Delta^{-1}) + \exp(-c\sqrt{\log z'})\} \\
&\ll \frac{x\log D}{\log^{\delta} x} \ll \frac{x}{\log^{\delta-1} x},
\end{aligned}$$

où c est une constante positive ; cette erreur est admissible si $\delta \ge 3$.

III.2.— Application des majorations des sommes de type II

Après ce travail préliminaire, on voit qu'il ne reste plus qu'à considérer les sommes $S(P'^*, D'^*, M'^*)$ du type (3.2), où le triplet (P'^*, D'^*, M'^*) est pris dans l'ensemble E de cardinal $\ll \log^{3\delta+3} x$ défini par

$$E := \big\{(P'^*, D'^*, M'^*)\ ;\ z'\Delta < P'^* < z,\ \frac{D}{P'^{*2}\Delta^{-3}} \le D'^* < \frac{D}{P'^*},\ x\Delta^3 \le P'^*D'^*M'^* < 2x\big\}$$

et dans ces nouvelles sommes $S(\ )$ les variables $p',\ d,\ m$ satisfont seulement aux conditions (3.3). On applique alors le Corollaire 2.11 avec pour choix de variables (voir les notations de 2.11)

$$\delta = 4,\ D = z\log^{49} x,\ \frac{D}{z} \ll \text{"}N\text{"} = P'^*D'^* \ll D,\ \text{"}M\text{"} = M'^* \gg \frac{x}{D} = x^{1/2}\log^{51} x$$

et la contribution à S_2 des $O(\log^{15} x)$ sommes $S(P'^*, D'^*, M'^*)$ est

$$\ll_i\ x\log x.\log^{15+1/2} x\big\{\log^{-49/2} x + \log^{1/2} p\log^{-51/2} x\ \big\} \ll \frac{x}{\log^2 x},$$

c'est donc un terme admissible. Par conséquent

$$S_2 \ll \frac{x}{\log^2 x} \tag{3.4}$$

On traite maintenant S_1 (cf (3.1)) ; pour chaque $p' \le z' = x^{1/8}$ fixé, on fait un découpage similaire sur les variables m et d, avec le même Δ. Le terme d'erreur du à ce découpage est un $O_i(x/p'\log^3 x)$. Il reste ensuite à majorer $O(\log^{10} x)$ sommes où les variables d et m varient dans des intervalles de la forme

$$d \in]D'^*\Delta^{-1}, D'^*],\ m \in]M'^*\Delta^{-1}, M'^*],$$

vérifiant les conditions $x\log^{-3}x/p' < D'^*M'^* < 2x$ et $1 < D/p'^2 \leq D'^* \leq D/p'$, appliquant à nouveau le Corollaire 2.11, on trouve que $|S_1|$ est majorée par

$$\begin{aligned} &\ll_i \sum_{p'<z'}\left(\frac{x}{p'\log^3 x}+\log^{10}x.\frac{x}{p'}(\frac{p'}{D^{1/2}}+\frac{p^{1/4}D^{1/2}\log^2 x}{x^{1/2}})\right) \\ &\ll_i \frac{x}{\log^2 x} \end{aligned} \tag{3.5}$$

Compte tenu de (3.0), (3.1), (3.4), (3.5) on conclut la preuve de la Proposition 3.1

□

III.3.— Passage aux nombres premiers

Notre but est de montrer la Proposition suivante, analogue du Théorème 3 :

Proposition 3.2. — *Soit m un entier non nul fixé, et $x > m$ un réel, p un nombre premier tel que $x \leq p < 2x$. Alors, pour tout i entier non nul, on a l'égalité*

$$\sum_{\substack{x\leq q<2x\\ q\neq p}} \mathrm{sym}_i(\theta_{p,m\overline{q}^2}) \ll_k \frac{x\log\log x}{\log^2 x},$$

et, pour tout ensemble mesurable $A \subset [-\pi,\pi]$, soit $\mathbf{1}_A$ sa fonction caractéristique ; on a l'égalité

$$\sum_{\substack{x\leq q<2x\\ q\neq p}} \mathbf{1}_A(\theta_{p,m\overline{q}^2}) = \mu_{ST}(A)\frac{x}{\log x}+o(\frac{x}{\log x}).$$

En outre, les constantes apparaissant dans les symboles de Landau sont uniformes pour $m < x$ et ne dépendent pas de p.

Preuve. La deuxième partie de la Proposition 3.2 se déduit de la première par un argument de densité. On montrera la première partie pour $m = 1$,(observons que cette restriction a peu d'importance dès lors que $m < x$. Pour $p \sim x$ on a $(m,p) = 1$, et la translation de $\mathbb{F}_p^*$, $x \to mx$, est tout à fait innocente du point de vue de la géométrie algébrique, voir la remarque qui suit le corollaire 2.11). On utilise alors la Proposition 3.1 et un argument d'inversion du rôle des variables : en effet, dans la somme de la Proposition 3.1, peu d'entiers m ne sont pas premiers. On veut montrer que, pour tout $i \geq 1$, on a

$$\sum_{x\leq q\leq 2x} \mathrm{sym}_i(\theta'_{p,q}) = o_i(\frac{x}{\log x}).$$

Or,

$$\begin{aligned} \sum_{q\sim x} \mathrm{sym}_i(\theta'_{p,q}) = O_i(x^{1/2}) &+ \sum_{\substack{m\sim x,(m,p)=1\\ p'|m\to p'>x^{1/2}\log^{-100}x}} \mathrm{sym}_i(\theta'_{p,m}) \\ &- \sum_{\substack{m=p_1p_2\sim x\\ p_1,p_2>x^{1/2}/log^{100}x\\ p_1<\sqrt{2x}}} \mathrm{sym}_i(\theta'_{p,m}). \end{aligned}$$

Par la Proposition 3.1, le premier terme de gauche est un $O_i(\frac{x}{\log^2 x})$, et par le Théorème des Nombres Premiers, on a, pour une constante $c > 0$, la majoration suivante du deuxième terme

$$\begin{aligned}
&\ll_i \sum_{x^{1/2}\log^{-100} x < p_1 < \sqrt{2x}} \frac{2x}{p_1 \log(2x/p_1)} \\
&\ll_i \frac{x}{\log x}\left\{\log\left(\frac{\log\sqrt{2x}}{\log(x^{1/2}\log^{-100} x)}\right) + \exp(-c\sqrt{\log x})\right\} \\
&\ll_i \frac{x\log\log x}{\log^2 x} = o_i(\frac{x}{\log x}).
\end{aligned}$$

□

IV.— Conclusion

Soit m un entier fixé. Le Théorème 1 est alors un cas particulier du Théorème suivant :

Théorème 4. — *Soit $x > m$. Soient A et B deux ensembles mesurables de $[-\pi, \pi]$, on définit l'ensemble mesurable $\Phi(A,B) = \arccos(\cos A \cos B)$; on pose*

$$\mathcal{C}^{\Phi(A,B)}(x) := \{(p,q) | p \neq q,\ x \leq p, q < 2x,\ \theta_{pq,m} \in \Phi(A,B)\ \};$$

alors on a la minoration

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

Preuve. Posons

$$\mathcal{C}^A(x) := \{(p,q) | p \neq q,\ x \leq p, q < 2x,\ \theta_{p,m\overline{q}^2} \in A\ \},$$

$$\mathcal{C}^B(x) := \{(p,q) | p \neq q,\ x \leq p, q < 2x,\ \theta_{q,m\overline{p}^2} \in B\ \}$$

alors d'après la Proposition 3.2, on a

$$\begin{aligned}
|\mathcal{C}^A(x)| &= \sum_{p\sim x}\left\{\mu_{ST}(A)\frac{x}{\log x} + o(\frac{x}{\log x})\right\} \\
&= \mu_{ST}(A)\frac{x^2}{\log^2 x} + o(\frac{x^2}{\log^2 x})
\end{aligned}.$$

et de même pour $|\mathcal{C}^B(x)|$; par multiplicativité croisée (1.2),

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

□

Soit $I = [a, b]$ un intervalle de $[0, 1]$, on pose $A_I := \{\theta \in [-\pi, \pi],\ |\cos\theta| \in I\}$; alors $\mu_{ST}(A_I) = f(a) - f(b)$, où f est la fonction

$$f(a) = \mu_{ST}(A_{[a,1]}) = \frac{2}{\pi}(\arccos a - a\sqrt{1-a^2});$$

pour la première partie du Théorème 1, on choisit

$$A = B = A_{[0.4,1]} \text{ et on a } 2\mu_{ST}(A_{[0.4,1]}) > 1, \text{ donc } |\mathcal{C}^{\Phi(A,B)}(x)| \gg \frac{x^2}{\log^2 x}$$

pour la seconde,

$$A = [-\pi, \pi],\ B = A_{[0,\epsilon]} \text{ et } \mu_{ST}(A) + \mu_{ST}(B) \geq 1 + \epsilon.$$

Cette discussion conclut la preuve du Théorème 1.

Remarque. On peut, plus généralement, à l'aide du Théorème 4, déterminer des intervalles I de $[0, 1]$ tels que pour une proportion positive de couples (p, q) on ait

$$|\cos\theta_{pq,1}| \in I.$$

Remarque. Comme me l'a montré E. Fouvry, il est facile d'avoir le résultat suivant :

Pour tout $\epsilon > 0$, il existe une constante positive $\alpha(\epsilon)$, telle que le nombre de couples (p, q) tels que $p \neq q,\ pq \leq x$ vérifiant de surcroit

$$|\frac{S(1, 1; pq)}{4\sqrt{pq}}| \leq \epsilon,$$

est minoré par

$$\alpha(\epsilon)\frac{x \log\log x}{\log x},$$

pour x assez grand.

On obtient donc le bon ordre de grandeur. Pour ce faire, on choisit p très petit, plus précisement, on prendra $\log x \leq p \leq \exp(\sqrt{\log x})$. La condition

$$|\frac{S(1, \overline{q}^2; p)}{2\sqrt{p}}| \leq \epsilon,$$

suffit. On regroupe donc les q suivant les classes de congruences de p et il nous suffit de minorer la somme

$$\sum_{\log x \leq p \leq \exp(\sqrt{\log x})} \sum_{\substack{m \in \mathbb{F}_p^* \\ |S(1,\overline{m}^2;p)/2\sqrt{p}| \leq \epsilon}} \pi(\frac{x}{p}; p, m).$$

La variante suivante du Théorème 0,

$$\sum_{\substack{m \in \mathbb{F}_p^* \\ |S(1,\overline{m}^2;p)/2\sqrt{p}| \leq \epsilon}} 1 \gg_\epsilon p,$$

et le théorème de Siegel-Walfisz permettent de conclure.

Il est clair qu'une telle méthode ne marche pas si on impose à p et q d'être de la même taille (*ie.* $p \leq x,\ q \leq x$), ou que l'on veut obtenir des *minorations* sur les sommes de Kloosterman.

Bibliographie

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

[F-I] E. Fouvry et H. Iwaniec. — *On a theorem of Bombieri-Vinogradov type,* Mathematika, Vol 27 Part2 (1992),135-152.

[Ka1] N.M. Katz. — *Sommes d'exponentielles,* Astérisque 79, Soc. Math. de France (1978).

[Ka2] N.M. Katz. — *Exponential sums over finite fields and Differential equations over the complex numbers : some interactions,* Bull. Am. Math. Soc., Vol 23, n2, p.269.

[Ka3] N.M. Katz. — *Gauss Sums, Kloosterman Sums and Monodromy Groups,* Annals of Maths. Studies 116, PUP.

[Ka4] N.M. Katz. — *Exponential sums and Differential equations,* Annals of Maths. Studies 124, PUP.

Philippe MICHEL
Mathématiques, Bât. 425
Université Paris-Sud
91405 ORSAY CEDEX

michel@matups.matups.fr