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

Philippe MICHEL, Université d'Orsay

29 Janvier, 1997

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

Notations

Nous ferons les conventions suivantes

- $\Lambda(n)$ désigne la fonction de Von Mangolt,
- $\omega(n)$ est le nombre de facteurs premiers distincts de l'entier n,
- $\mathrm{e}(.)$ désigne la fonction $\exp(2i\pi.)$,
- 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,
- si κ est un entier on note $\tau_\kappa(n)=\sum_{d_1\ldots d_\kappa=n} 1$, et $\tau(n)=\tau_2(n)$,
- $n\sim N$ signifie $N\leq n<2N$,
- si (λ_m) est une suite finie de complexes on note $||\lambda(M)||:=(\sum_{m\leq M}\ |\lambda_m|^2)^{1/2}$ sa norme L^2 , et de même $|\lambda(M)|:=\sum_{m\leq M}\ |\lambda_m|$ sa norme L^1,
- pour i entier positif ≥ 0, $\mathrm{sym}_i(\theta)$ désigne la fonction $\sin((i+1)\theta)/\sin\theta$;
- La lettre ε est une commodité de notation pour désigner un réel positif suffisament petit, dont la valeur peut varier d'une ligne à l'autre.
- La lettre ϵ, en revanche, est une variable “fixe”.
- Dans toute la suite, la lettre p indicée ou non, sera réservée pour la désignation d'un nombre premier.

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

Philippe MICHEL, Université d'Orsay

29 Janvier, 1997

1 Introduction

Pour $l, m, q \geq 1$ des entiers, on désigne par $S(l, m; q)$ la somme de Kloosterman

$$Kl(l, m; q) = \sum_{\substack{k mod q \\ (k,q)=1}} \mathrm{e}(\frac{lk + m\overline{k}}{q}).$$

Rappelons que c'est un réel non nul et pour $(lm, q) = 1$ on définit l'argument $\theta_{q,lm}$ par la formule:

$$\cos \theta_{q,lm} := \frac{Kl(l, m; q)}{2^{\omega(q)}\sqrt{q}};$$

La majoration de Weil implique que $\theta_{q,lm}$ est un réel bien défini modulo π. Rappelons que la conjecture de Sato-Tate prédit l'équirépartition sur $[0, \pi]$ des argument $\theta_{p,m}$ relativement à la mesure de Sato-Tate,

$$\mu_{ST}(\theta) := \frac{2}{\pi} \sin^2 \theta d\theta,$$

à m fixé et p décrivant l'ensemble des nombres premiers. Dans [Mi], nous expliquions comment les Théorèmes de *Deligne* sur les Conjectures de Weil (duement complétés par ceux de *Katz*), mélés à des arguments de crible donnaient des éléments sur la répartition des arguments $\theta_{p_1 p_2,m}$ quand p_1 et p_2 décrivent l'ensembles de nombres premiers. Ici nous développons une autre approche, plus analytique. Dans un premier temps nous traitons du problème suivant qui est un affaiblissement de la conjecture de *Sato-Tate*:

Problème. — *Trouver un $\alpha < 1$ le plus petit possible tel que, pour toute suite de nombres complexes (λ_m) on ait, pour tout k entier non nul,*

$$\sum_{1 \leq m \leq P^\alpha} \lambda_m \sum_{\substack{p \leq P \\ (p,m)=1}} \mathrm{sym}_k(\theta_{p,m}) = o_k(||\lambda(P^\alpha)|| \frac{P^{1+\alpha/2}}{\log P}).$$

Comme les fonction $\mathrm{sym}_k\,\theta$ forment une base orthonormale, pour $[0,\pi]$ muni de la mesure μ_{ST}, on voit que pour $\alpha=0$, on retrouve la conjecture de *Sato-Tate*. D'autre part, si (λ_m) est la suite constante égale à 1, le problème admet pour solution tout $\alpha>1/2$ (c'est une conséquence de la Proposition 2.8 de [Mi] rappelée au Lemme 2.8).

Dans cet article, ce problème ne sera résolu que pour le premier "moment" $k=1$: on montrera dans la section 3 le

Théorème 1.1 . — *Soient α et β des réels tels que $16/17<\beta\leq 1$ et $1/2\beta<\alpha<1/32(1-\beta)$. Soit (λ_m) une suite le complexes vérifiant pour tout ϵ positif,*

$$|\lambda(M)|\gg_\epsilon M^{\beta/2-\epsilon}||\lambda(M)||.$$

Alors, pour tout $\epsilon>0$ assez petit, on a

$$\sum_{1\leq m\leq P^\alpha}\lambda_m\sum_{\substack{p\leq P\\(p,m)=1}}\frac{Kl(1,m;p)}{2\sqrt{p}}\ll_{\epsilon,\alpha,\beta}|\lambda(P^\alpha)|P^{1-\epsilon}.$$

La condition imposée à la suite (λ_m) signifie que cette dernière est assez bien répartie, et elle est vérifiée par toute fonction caractéristique d'une suite d'entiers assez dense. La valeur $\alpha=\frac{1}{2}$ apparait une fois encore comme une barrière, qu'il est possible de franchir au prix de quelques concessions: par exemple, remplaçant la variable p par un nombre presque premier. On peut jouer avec le crible pour détecter des entiers avec peu de facteurs premiers; ainsi le Théorème 1.1 admet la variante suivante (qu'on ne démontrera pas):

Variante. — *Soient α et θ, deux constantes vérifiant*

$$0<\theta\leq\frac{1}{6},\ \textit{et}\ 1/3+\theta<\alpha\leq 1$$

et (λ_m) des nombres complexes, on a

$$\sum_{m\leq P^\alpha}\lambda_m\sum_{\substack{n\leq P^\theta\\p'|n\to p'>P^\theta\\(n,m)=1}}\frac{Kl(1,m;n)}{\sqrt{n}}\ll_{\epsilon,\alpha,\theta}\ ||\lambda(P^\alpha)||P^{1+\alpha/2-\epsilon},$$

pour tout ϵ assez petit.

Remarque. — Notons – et c'est un peu décevant – que le terme $2^{\omega(n)}$ est absent du dénominateur dans l'expression précédante, ainsi, quand n a beaucoup de facteurs premiers, les termes $Kl(1,m;n)$, sont sommés avec un poids trop important.

Pour montrer ces deux théorèmes, on a recours à des identités combinatoires de type crible, ou encore l'identité de *Heath-Brown* sur les nombres premiers. De telles identités ont déjà étés utilisées avec succès par *Patterson et Heath-Brown* [H-B-P] pour le problème de l'équidistribution des sommes de Gauss cubiques, et beaucoup plus recemment par *Duke, Friedlander et Iwaniec*, qui ont pu démontrer l'équidistribution uniforme des arguments des sommes de *Salié* ([D-F-I]). Grâce à ces identités, on se ramène à majorer des sommes de type I et de type II; Pour traiter les sommes de type I, on doit considérer (pour le premier moment au moins) des expressions de la forme

$$\sum_{s\leq S}\frac{Kl(1,m,rs)}{\sqrt{rs}}. \tag{1}$$

On doit à *Kuznetzov* d'avoir su pour la première fois majorer de façon significative une telle somme ([Ku]): grâce à la formule des traces qui porte maintenant son nom, il a pu prouver pour $r=1$, une majoration de (1) en $O_\epsilon(S^{2/3+\epsilon})$. Rappelons que la formule des traces de *Kuznetzov* est basée sur la décomposition spectrale des séries de *Poincaré* dans le demi plan supérieur, ainsi il pourrait y avoir un lien entre la conjecture de *Sato-Tate* et la théorie des formes modulaires. Cette méthode, a ensuite été fructueusement développée par *Deshouillers* et *Iwaniec*, pour déboucher sur de nombreuses applications arithmétiques. Ici encore, nous utilisons les Théorèmes de *Deshouillers* et *Iwaniec* ([D-I]) pour traiter nos sommes de type I. Faute d'une formule des traces adéquate impliquant des produits de sommes de *Kloosterman*, il nous semble difficile, pour l'instant, de traiter les moments plus grands (les $\mathrm{sym}_k(\theta_{p,m}), k\geq 2$) ou de majorer des sommes de type II par la théorie des formes modulaires. Nous obvions à cette dernière difficulté en utilisant une majoration récente sur les sommes de sommes de *Kloosterman*, due à *Fouvry, Iwaniec et Katz* ([F-I-K]), et qui provient de la géométrie algébrique: après des manipulations élémentaires mais non triviales des variables, ils se ramènent à une somme d'exponentielle qui est majorée, en appendice, par *Katz* à l'aide des théorèmes fondamentaux de *Deligne* [D]. Il est à noter qu'il est possible d'appliquer le même traitement aux sommes de type II correspondantes aux moments supérieurs; c'est ce fait que nous allons exploiter dans la cinquième partie.

Dans la section 4, nous démontrons une généralisation aux autres moments (les $\mathrm{sym}_k(\theta_{p,m}), k\geq 2$) de la majoration de *Fouvry, Iwaniec et Katz* utilisée dans la partie II . Cette généralisation permet de préciser le comportement probabiliste des angles des sommes de Kloosterman $\theta_{s,m}$ (dont on notera la grande régularité puisque dans le théorème ci-dessous on obtient des équivalents !), pour s un nombre sans facteurs carrés; ainsi on montrera le

Théorème 1.2 . — *Soient $(\lambda_m)_m$ une suite de nombres complexes ; Soient $R,\ S,\ M\geq 1$, on pose $x=RS,\ R=x^\theta,\ S=x^{1-\theta},\ M=x^\lambda$ et on suppose vérifiées les conditions* *suivantes:*

$$1/2 \leq \theta < 2/3, \text{ et } 1-\theta < \lambda \leq 1.$$

Alors, pour tout $k \geq 1$ on a l'égalité

$$\sum_{m\leq M}\sum_{r\leq R}\sum_{\substack{s\leq S\\(m,rs)=1}} \mu^2(rs)\left|\frac{Kl(1,m;rs)}{2^{\omega(rs)}\sqrt{rs}}\right|^{2k} = C_k MRS(\log R)^{\alpha_{0,2k}-1}(\log S)^{\alpha_{0,2k}-1}(1+O(\frac{1}{\log x})),$$

où C_k est une constante positive et $\alpha_{0,2k} = \int_{[0,2\pi]}\cos^{2k}\theta\mu_{ST}(\theta) < 1$. De même, pour tout ϵ positif assez petit, on a l'égalité

$$\sum_{m\leq M}\lambda_m\sum_{r\leq R}\sum_{\substack{s\leq S\\(m,rs)=1}} \mu^2(rs)\left(\frac{Kl(1,m;rs)}{2^{\omega(rs)}\sqrt{rs}}\right)^{2k+1} = O_k(||\lambda(M)||M^{1/2}x^{1-\epsilon}).$$

Les constantes implicites dans les symboles dépendant de ϵ, θ, λ et k.

L'intérêt de ce théorème réside d'une part dans la petite taille de la variable $m \leq M$ par rapport à $RS = x$; en effet le même résultat avec $\lambda_m \equiv 1$ et $M > x^{1/2+\epsilon}$ serait une conséquence de la proposition 2.8 de [Mi]. D'autre part , comparant avec la majoration de Weil: $|Kl(1,m;rs)| \leq 2^{\omega(rs)}\sqrt{rs}$, ce Théorème renforce l'intuition (exploitée pour la première fois chez *Hooley* [Ho]) selon laquelle, il existe des compensations liées *à la taille* des sommes de *Kloosterman*; mais celles-ci sont limitées (noter que l'on obtient un équivalent et non une majoration) , il apparaît que la conjecture de *Linnik-Selberg* devrait être conséquence des variations du signe des sommes de Kloosterman: on a fourni ici quelques éléments de réponse à une remarque de *Sarnak* [Sa] précédemment suggérée par *Serre*. Il faut remarquer que la restriction aux r, s *sans facteurs carrés* est innocente: pour $\nu \geq 2$ les sommes de Kloosterman $S(1,m;p^\nu)$ se calculent très explicitement (cf. le Lemme 2.3), on en déduit que les puissances de telles sommes s'écrivent encore comme combinaisons linéaires de sommes de *Kloosterman* (pour les sommes de Salié et $\nu = 1$, on a le même phénomène, ce qui explique en partie le succès de [D-F-I]); à partir de ces remarques, il est possible de généraliser le Théorème 1.2 au cas r, s quelconques, et il est alors possible (et nous ne le ferons pas) de montrer le :

Théorème 1.3 . — *Sous les mêmes hypothèses et notations que précedemment, on a les égalités suivantes:*

$$\sum_{m\leq M}\sum_{r\leq R}\sum_{\substack{s\leq S\\(m,rs)=1}} \left|\frac{Kl(1,m;rs)}{2^{\omega(rs)}\sqrt{rs}}\right|^{2k} = C'_k MRS(\log R)^{\alpha_{0,2k}-1}(\log S)^{\alpha_{0,2k}-1}(1+O(\frac{1}{\log x})),$$

où C'_k est positive et pour tout $\epsilon > 0$ assez petit,

$$\sum_{m\leq M}\lambda_m\sum_{r\leq R}\sum_{\substack{s\leq S\\(m,rs)=1}} \left(\frac{Kl(1,m;rs)}{2^{\omega(rs)}\sqrt{rs}}\right)^{2k+1} = O_k(||\lambda(M)||M^{1/2}x^{1-\epsilon}).$$

De façon plus immédiate, on peut aussi donner des Théorèmes de type Sato-Tate en moyenne, pour des modules p presques premiers:

Théorème 1.4 . — *Soient* (λ_m) *et* (μ_n) *deux suites de nombres complexes, et* $\alpha,\ \beta$ *des réels vérifiants les inégalités suivantes*

$$1/3 < \alpha \leq 1/2, \text{ et } \beta > \frac{\alpha}{1-\alpha}. \tag{1.2}$$

Soient $k_1,\ k_2$ *des entiers vérifiant* $k_1 + k_2 > 0$.

Pour tout p_1, *on note* $P_2 := p_1^{\alpha/(1-\alpha)}$ *et* $M := p_1^{\beta}$.

Alors, pour tout $\epsilon > 0$ *assez petit on a la majoration suivante*

$$\sum_{\substack{p_2 \leq P_2 \\ p_1 - p_2}} \sum_{\substack{m \leq M \\ (m, p_1 p_2) = 1}} \mu_{p_2} \lambda_m \operatorname{sym}_{k_1}(\theta_{p_1, m\overline{p_2}^2}) \operatorname{sym}_{k_2}(\theta_{p_2, m\overline{p_1}^2}) \ll_\epsilon ||\lambda(M)|| ||\mu(P_2)|| M^{1/2} P_2^{1/2-\epsilon}.$$

Ce Théorème donne donc l'équidistribution dans $[0,\pi] \times [0,\pi]$ des couples d' angles

$$\{(\theta_{p_1, m\overline{p_2}^2}, \theta_{p_2, m\overline{p_1}^2})\}_{m, p_2},$$

quand p_1 tend vers l'infini, et comme corollaire, celle des angles $\{\theta_{p_1 p_2, m}\}$ sur $[0,\pi]$ muni d'une mesure adéquate. Ici encore, la taille de la variable m est petite par rapport à celle de la variable $p_1 p_2$: $1/3 < \log m / \log p_1 p_2 \leq 1/2$, et on passe le seuil fatidique $1/2$ obtenu dans la proposition 2 de [Mi]. On se rapproche de la conjecture de Sato-Tate pour les nombres composés.

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.

2 Lemmes et notations

Pour tout entier n,

- $n^\flat$ est le produit de $2^{v_2(n)}$ et des facteurs premiers impairs de n dont la valuation est impaire et ≥ 3, par exemple $(2^2 \times 3 \times 5^3)^\flat = 2^2 \times 5$,
- $n^\sharp$ est n divisé par $2^{v_2(n)}$ et par ses facteurs premiers impairs de valuation 1, par exemple $(2^2 \times 3 \times 5^3)^\sharp = 5^3$.

Le premier lemme est une identité combinatoire due à *Heath-Brown* [H-B]

Lemme 2.1 . — *soit $J \geq 1$ et $n < 2x$. Alors on a l'égalité*

$$\Lambda(n) = \sum_{j=1}^{J} (-1)^j \binom{J}{j} \sum_{s_1,\ldots,s_j \leq x^{1/J}} \ldots \sum \mu(s_1)\ldots\mu(s_j) \sum_{c_1\ldots c_j.s_1\ldots s_j = n} \ldots \sum \log(c_1).$$

Lemme 2.2 . — *Soit $\kappa < 1/2$ et $R \geq 1$, alors on a la majoration*

$$\sum_{r\sim R} \left(r^\flat r^\sharp\right)^\kappa \ll_\kappa R\log(2R).$$

Preuve. — On a l'inégalité,

$$\sum_{r\sim R} \frac{(r^\flat r^\sharp)^\kappa}{r} \leq \frac{1}{1-2^{\kappa-1}} \prod_{p\leq 2R} \left(1 + \frac{1}{p} + \frac{1+p^{2\kappa-1}}{p^{2-2\kappa}-1}\right) \ll \log(2R),$$

d'après la formule de *Mertens*.

□

Nous énonçons maintenant quelques propriétés classiques des sommes de *Kloosterman*:

Lemme 2.3 . — *On a les propriétés suivantes*

1. *la majoration conséquence des travaux de* Weil
$$|Kl(l,m;n)| \leq (l,m,n)^{1/2} n^{1/2} 2^{\omega(n)};$$
2. *la propriété de multiplicativité croisée , ie: si $(r,s)=1$*
$$Kl(l,m;rs) = Kl(l,m\overline{s}^2;r)Kl(l,m\overline{r}^2;s);$$

3. si $q = p^a$, on a les égalités

$$|Kl(1,m;p^a)| = \mu(p^a)^2, \ \textit{si } p|m$$
$$Kl(1,m;p^a) = p^{a/2} \sum_{\substack{x (\bmod p^a) \\ x^2 \equiv m (\bmod p^a)}} \mathrm{e}(\frac{2x}{p^a}), \ \textit{si } (m,p) = 1 \textit{ et } a > 1.$$

Le lemme suivant est une généralisation du Théorème 2 de [F-I-K]; ce Théorème y était démontré avec les contraintes supplémentaires: “r sans facteurs carrés, $(r,s) = 1$”.

Lemme 2.4 . — *Soient a, r deux entiers premiers entre eux, et (λ_m) une suite de complexes. Alors, pour tout ϵ positif, on a l'inégalité*

$$(2) \quad \sum_{s \leq S} |\sum_{m \leq M} \lambda_m Kl(a,m;rs)|^2 \ll_\epsilon \quad \|\lambda(M)\|^2 M S^2 r^{1+\epsilon} \times$$
$$\Big(r^{\flat 1/4} r^{\sharp 1/6} (r^{-1/4} + r^{1/4} S^{-1/2}) + S M^{-1} \Big).$$

Cette généralisation du Théorème 2 de [F-I-K], quoique très élémentaire, est pénible, et sa longueur semble disproportionnée par rapport aux contraintes dont on veut s'affranchir (r sans facteur carré); aussi, nous en reportons la preuve en appendice.

Remarque. — Ce lemme est intéressant quand $r > 1, \ r < S^2, \ S < M$.

Le Lemme précédent provient pour sa partie la plus difficile de la géométrie algébrique (en caractéristique fixée); le suivant est de nature modulaire. C'est une version légèrement améliorée du Théorème 10 de [D-I]: on tient compte, ici, d'un éventuel “défaut de platitude” – mesuré par le paramètre Z – de la fonction $\mathcal{C}^\infty$ de pondération, $g(m,n,r,s,c)$.

Lemme 2.5 . — *Soient (a_m), $(b_{n,r,s})$ des complexes, soit $Z \geq 1$, et soit $g(m,n,r,s,c)$ une fonction $\mathcal{C}^\infty$ à support compact dans $[M,2M] \times [N,2N] \times [R,2R] \times [S,2S] \times [C,2C]$, telle que pour tout ν_1, ν_2, ν_3, ν_4, ν entiers vérifiant $0 \leq \nu_1, \ldots, \nu_4 \leq 2$, $1 \leq \nu \leq 2$,*

$$|\frac{\partial^{\nu_1+\nu_2+\nu_3+\nu_4}}{\partial^{\nu_1} m \partial^{\nu_2} n \partial^{\nu_3} r \partial^{\nu_4} s} g(m,n,r,s,c)| \ll \frac{1}{M^{\nu_1} N^{\nu_2} R^{\nu_3} S^{\nu_4}},$$
$$\int_{[C,2C]} |\frac{\partial^{\nu_1+\ldots+\nu_4+\nu}}{\partial^{\nu_1} m \ldots \partial^{\nu_4} s \partial^{\nu} c} g(m,n,r,s,c)| dc \ll \left(\frac{Z}{C}\right)^{\nu-1} \frac{1}{M^{\nu_1} N^{\nu_2} R^{\nu_3} S^{\nu_4}}.$$

Soit la somme

$$\begin{aligned} L^{\pm}(C,M,N,R,S) = & \sum_{\substack{r\sim R, s\sim S\\ (r,s)=1}} \sum_{m\sim M, n\sim N} a_m b_{n,r,s} \\ & \sum_{(c,r)=1} g(m,n,r,s,c) S(m\overline{r}, \pm n; sc); \end{aligned}$$

alors, pour tout $\epsilon > 0$, on a la majoration

$$L^{\pm}(C,M,N,R,S) \ll_\epsilon (CMNRS)^\epsilon Z^4 L(C,M,N,R,S) \|a(M)\|.\|b(N,R,S)\|;$$

où on a noté

$$\begin{aligned} L(C,M,N,R,S)^2 = \quad & C^2S^3R^2Z \\ & + SR\frac{(S^2RC^2+MN+SMC^2)(S^2RC^2+MN+SNC^2)}{S^2RC^2+MN} \\ & + S^2C^3\sqrt{(SR+N)RM}. \end{aligned}$$

Les lemmes suivant seront utilisés dans les preuve du Théorème 1.2.

Le premier dit que pour la plupart des entiers n, le produit des petits facteurs premiers de n est petit. Plus précisément, on a le

Lemme 2.6 . — *([Te1]) Pour $2 \leq u \leq v \leq x$, on a*

$$|\{n \leq x; \prod_{p\leq u, p^\nu \| n} p^\nu > v\}| \ll x \exp(-c_0 \frac{\log v}{\log u}),$$

où c_0 est une constante positive absolue.

Le deuxième est un lemme trigonométrique

Lemme 2.7 . — *Pour tout entier $k \geq 1$, on a*

$$\cos^k \theta = \sum_{i=0}^{k} \alpha_{i,k} \operatorname{sym}_i(\theta),$$

où les $\alpha_{i,k}$ sont des rationnels positifs ou nuls, et $\alpha_{0,k} = \int_{[0,\pi]} \cos^k(\theta)\mu_{ST}(\theta)$

Preuve. — On a l'identité

$$\cos^{k+1}\theta = \frac{1}{2^k} \sum_{i=0}^{[(k+1)/2]} \binom{k+1}{i} \cos((k+1-2i)\theta) \ + \ \mathit{Constante}$$

Le lemme s'en déduit en dérivant cette égalité.

□

Soit r un entier, pour toute fonction f complexe de $\mathbf{Z}/r\mathbf{Z}$, on définit sa *transformée de Fourier additive*, fonction de $\mathbf{Z}/r\mathbf{Z}$, par la formule

$$\mathcal{F}(f,j;r) := \sum_{x\in\mathbf{Z}/r\mathbf{Z}} f(x)\,\mathrm{e}(\frac{-jx}{r}).$$

(si f est seulement définie sur $(\mathbf{Z}/r\mathbf{Z})^*$, comme par exemple $\mathrm{sym}_i(\theta_{r,m})$, on la prolonge par zéro sur $\mathbf{Z}/r\mathbf{Z}$.)

Pour la fonction $f(m) = \mathrm{sym}_i(\theta^{\psi}_{r,m})$, on rappelle le corollaire de la proposition 2.8 de [Mi]

Lemme 2.8 . — *Pour tout entier $i > 0$, pour tout $j \in \mathbf{Z}/p\mathbf{Z}$, et pour tout caractère additif non trivial ψ de $\mathbf{Z}/p\mathbf{Z}$, on a la majoration*

$$\left|\mathcal{F}(\mathrm{sym}_i(\theta^{\psi}_{p,\_}),j;p)\right| \leq (i+1)p^{1/2}.$$

Nous aurons aussi recours au lemme d'analyse suivant, qui précise le comportement en moyenne de certaines fonctions arithmétiques (dont les fonctions diviseurs) à partir des propriétés de leur série de *Dirichlet* : c'est la méthode de *Selberg-Delange*. *Tenenbaum* lui a donné une forme très générale ([Te2] T.II Chap. 5.3 Thm. 3), dont nous présentons une version simplifiée.

Lemme 2.9 . — *Soient $\alpha \in \mathbf{C}$, $c_0 > 0$, $0 < \delta \leq 1$, $H > 0$. Soit $F(z) = F(\sigma + i\tau) = \sum_n a_n n^{-z}$ une série de Dirichlet à coefficients positifs. On suppose que la fonction*

$$G_\alpha(z) := F(z)\zeta(z)^{-\alpha},$$

est prolongeable en une fonction holomorphe dans le domaine

$$Re(z) = \sigma \geq 1 - c_0/(1+\max\{0,\log|\tau|\}),$$

et qu'elle satisfait dans ce domaine, à la majoration

$$|G_\alpha(z)| \leq H(1+|\tau|)^{1-\delta};$$

on dira alors que $F(z)$ a la propriété $\mathcal{P}(\alpha;c_0,\delta,H)$. On a alors, pour $x \to +\infty$, l'égalité

$$\sum_{n\leq x} a_n = x(\log x)^{\alpha-1}(G_\alpha(1) + O(HR(x))),$$

avec

$$R(x) = \exp(-c_1\log^{1/2} x) + \frac{1}{\log x}.$$

La constante positive c_1 et la constante implicite dans le symbole de Landau dépendent au plus de c_0, δ et α.

3 Preuve du Théorème 3.1

3.1 Découpage des variables .

Par une partition dyadique de l'intervalle $[1, P]$ en $O(\log P)$ sous-intervalles, de la forme $[P', 2P']$,on est conduit à majorer les sommes typiques

$$\sum_{p\sim P'} \sum_{\substack{1\leq m\leq P^\alpha \\ (m,p)=1}} \lambda_m \frac{Kl(1,m;p)}{2\sqrt{p}}.$$

- La contribution des $P' \leq P^{1-\varepsilon}$, est en $O(|\lambda(P^\alpha)|P^{1-\varepsilon})$ (2.3(1)).
- Dans les sommes restantes ($P^{1-\varepsilon} \leq P' \leq P/2$), on supprime la condition $(m,p) = 1$ au prix d'un terme d'erreur en $O(|\lambda(P^\alpha)|P^{1/2+\varepsilon})$ (2.3(3))

Pour simplifier, on fera la majoration pour $P' = P$, les autres termes fournissent la même majoration à un facteur P^ε près. Notre somme s'écrit alors

$$\begin{aligned}\sum_{p\sim P} \sum_{1\leq m\leq P^\alpha} \lambda_m \frac{Kl(1,m;p)}{2\sqrt{p}} &= \sum_{n\sim P} \sum_{1\leq m\leq P^\alpha} \lambda_m \frac{\Lambda(n)}{\log\ n} \frac{Kl(1,m;n)}{2\sqrt{n}} + O(|\lambda(P^\alpha)|P^{1/2+\varepsilon}) \\ &= \frac{1}{2\sqrt{P}} \sum_{n\sim P} \sum_{1\leq m\leq P^\alpha} \lambda_m \frac{\Lambda(n)}{\log\ n} \frac{\sqrt{P}}{\sqrt{n}} Kl(1,m;n) \\ &\quad +O(|\lambda(P^\alpha)|P^{1/2+\varepsilon}),\end{aligned}$$

le terme d'erreur provenant de la contribution des puissances ≥ 2 de nombres premiers.

On applique le Lemme 2.1 avec $J = 4$ sur les n. On découpe l'intervalle de sommation de chacune des 8 variables s_i et c_i, $1 \leq i \leq 4$ créées, en sous intervalles de la forme $[S_i, S_i(1+Y^{-1})]$, $[C_i, C_i(1+Y^{-1})]$. Par le Lemme 2.3(1), le terme d'erreur créé en rendant les 8 variables indépendantes, est en

$$O(\frac{|\lambda(P^\alpha)|P^{1+\varepsilon}}{Y}).$$

Finalement, on en est réduit à traiter $O(Y^8 \log P)$ sommes de la forme: $(j \leq 4)$

$$S(S_1 \dots S_j|C_1 \dots C_j) :=$$

$$\frac{1}{\sqrt{P}} \sum_{\substack{s_i\in[S_i,S_i(1+Y^{-1})] \\ c_i\in[C_i,C_i(1+Y^{-1})]}} \mu(s_1)\dots\mu(s_j) \frac{\log\ c_1}{\log(c_1\dots s_j)} \frac{\sqrt{P}}{\sqrt{c_1\dots s_j}} \sum_m \lambda_m Kl(1,m;s_1\dots c_j).$$

Pour chacune d'elles, nous allons obtenir une majoration de la forme

$$|S(S_1 \dots S_j|C_1 \dots C_j)| \ll_\varepsilon |\lambda(P^\alpha)|P^{1-\varepsilon}.$$

Notons maintenant,

$$S_i = P^{\sigma_i}\ C_i = P^{\gamma_i},$$

les exposants σ_i et γ_j vérifient les conditions suivantes:

$$j \leq\ 4\ , 0 \leq \sigma_1 \leq \ldots \leq \sigma_j \leq 1/4,\ 0 \leq \gamma_i,\ \sigma_1 + \ldots + \sigma_j + \gamma_1 + \ldots + \gamma_j = 1.$$

On va décomposer chacun des produits

$$S_1 \ldots S_j C_1 \ldots C_j = P$$

en deux blocs pour appliquer au mieux de nos intérêts les Lemmes 2.4 ou 2.5.

3.2 Sommes de type I .

Supposons par exemple que $\gamma_1 > 0$. Soit

- $Z > 0$ un paramètre réel à fixer;
- $f(c_1)$, une fonction $\mathcal{C}^\infty$, à support dans $[C_1(1 - Z^{-1}), C_1(1 + Y^{-1}) + C_1 Z^{-1}]$, qui vaut 1 sur l'intervalle $[C_1, C_1(1 + Y^{-1})]$;
- g, une fonction $\mathcal{C}^\infty$, à support dans $[P^{1-\gamma_1}/2, 3P^{1-\gamma_1}]$, qui vaut 1 sur $[P^{1-\gamma_1}, 2P^{1-\gamma_1}]$, de sorte que la somme $S(S_1 \ldots S_j | C_1 \ldots C_j)$ n'est pas changée quand on multiplie le terme intérieur par $g(c_2 \ldots s_1 \ldots s_j)$.
- on applique à la variable m une partition $\mathcal{C}^\infty$ de l'unité, en $O(\log P)$ fonctions h_i, $\mathcal{C}^\infty$, à support dans $[2^i, 2^{i+1}]$ telles que

$$\forall\ t \in \mathbf{R},\ h_i^{(\nu)}(t) \ll_\nu 2^{-i\nu}.$$

La somme $S(S_1 \ldots S_j | C_1 \ldots C_j)$ est somme de $O(\log P)$ termes de la forme

$$\frac{1}{P^{1/2}} \sum_{\substack{s_j \in [S_j, S_j(1+Y^{-1})] \\ c_i \in [C_i, C_i(1+Y^{-1})]}} \sum_m \lambda_m \mu(s_1) \ldots \mu(s_j) g(m, c_2 \ldots s_j, c_1) Kl(1, m; s_1 \ldots c_j),$$

avec

$$g(m, s, c_1) = \frac{\log\ c_1}{\log(c_1 s)} \frac{\sqrt{P}}{\sqrt{c_1 s}} f(c_1) g(s) h_i(m).$$

Les termes c_1 contenus dans les intervalles

$$[C_1(1 - Z^{-1}), C_1] \cup [C_1(1 + Y^{-1}), C_1(1 + Y^{-1}) + C_1 Z^{-1}],$$

contribuent, d'après le Lemme 1, par un $O(|\lambda(P^\alpha)| P^{1+\varepsilon} Z^{-1})$: on oublie donc la condition $c_1 \in [C_1, C_1(1 + Y^{-1})]$. Il ne reste plus qu'à appliquer le Lemme 2.5, en donnant aux paramètres $C,\ S,\ N,\ Z,\ R$ et M respectivement les valeurs C_1,

$C_2 \times \ldots \times S_j,\ P^\alpha,\ Z, 1$ et 1. En vérifiant que la fonction $g(m,s,c_1)$ satisfait les hypothèses du Lemme 2.5 on obtient:

$$S(S_1 \ldots S_j | C_1 \ldots C_j) \ll \frac{|\lambda(P^\alpha)| P^{1+\varepsilon}}{Z} \tag{3}$$
$$+ P^\varepsilon Z^4 \|\lambda(P^\alpha)\| (P^{3/2-\gamma} Z^{1/2} + P^{1-\gamma/2+\alpha/2} + P^{5/4-\gamma/4} + P^{1+\alpha/4}),$$

pour tout $\gamma \in \{\gamma_1, \ldots, \gamma_j\}$.

3.3 Sommes de type II .

On traite, ici, la somme $S(S_1 \ldots S_j | C_1 \ldots C_j)$ comme une somme de type II.

On applique le Lemme 2.4 en regroupant certains des σ_i et des γ_i; notons γ leur somme, s le produit des c_i et s_i correspondant et r le produit des termes restants, de sorte que $r \sim P^{1-\gamma}$ et $s \sim P^\gamma$; la somme se réécrit comme

$$S(S_1 \ldots S_j | C_1 \ldots C_j) = \frac{1}{\sqrt{P}} \sum_{\substack{s \sim P^\gamma \\ r \sim P^{1-\gamma}}} \beta_{r,s} \sum_m \lambda_m Kl(1, m; rs),$$

où $\beta_{r,s}$ est une fonction de r et s majorée par $\tau_8(m)\tau_8(n) \ll P^\varepsilon$. L'inégalité de *Cauchy-Schwarz*, le Lemme 2.4 et le Lemme 2.2 conduisent à la majoration

$$S(S_1 \ldots S_j | C_1 \ldots C_j) \ll \frac{1}{\sqrt{P}} \sum_r \Big(\sum_s |\beta_{r,s}|^2 \Big)^{1/2} \Big(\sum_s \Big| \sum_m \lambda_m Kl(1,m;rs) \Big|^2 \Big)^{1/2}$$

$$\ll \frac{1}{P^{1/2}} P^{\gamma/2+\varepsilon} \sum_r \|\lambda(P^\alpha)\| P^{\alpha/2} P^{\gamma+(1-\gamma)/2} (r^{\flat 1/8} r^{\sharp 1/12} (\frac{1}{r^{1/8}} + \frac{r^{1/8}}{P^{\gamma/4}}) + P^{\gamma/2-\alpha/2})$$

$$\ll \|\lambda(P^\alpha)\| P^{1+\alpha/2+\varepsilon} (P^{(\gamma-1)/8} + P^{(1-3\gamma)/8} + P^{(\gamma-\alpha)/2});$$

et ensuite à l'inégalité

$$S(S_1 \ldots S_j | C_1 \ldots C_j) \ll \|\lambda(P^\alpha)\| P^{1+\alpha/2+\varepsilon} (P^{(\gamma-1)/8} + P^{(1-3\gamma)/8} + P^{(\gamma-\alpha)/2}). \tag{4}$$

3.4 Conclusion .

La fin de la preuve est purement combinatoire:

on choisi $Y = Z = P^\varepsilon$.

Il s'agit de montrer que (ε a changé !, cf Notations)

$$S(S_1 \ldots S_j | C_1 \ldots C_j) \ll |\lambda(P^\alpha)| P^{1-\varepsilon} \tag{5}$$

sous les hypothèses

$$|\lambda(X)| \gg X^{\beta/2} \|\lambda(X)\|, \tag{6}$$

$$\beta > 16/17,\ 1/(2\beta) < \alpha < 1/(32(1-\beta)) \tag{7}$$

Note. — Pour alléger l'exposition, on omettra d'écrire les "ε" en remplaçant toutes les inégalités de la forme $a+\varepsilon \leq b$ (resp. $a \geq b+\varepsilon$) par l'écriture $a \prec b$ (resp $a \succ b$).

D'après (3) et (6), l'inégalité (5) est vérifiée dès que γ est l'un des γ_i et que

$$\gamma \succ \frac{1}{2} - \frac{\alpha\beta}{2} \tag{8}$$

$$\gamma \succ \alpha(1-\beta) \tag{9}$$

$$\gamma \succ 1 - 2\alpha\beta \tag{10}$$

$$\beta \succ \frac{1}{2} \tag{11}$$

Par (7) on remplace la condition (8), par la condition plus forte:

$$\gamma \succ \frac{1}{4} \tag{12}$$

et les conditions (9), (10) et (11) sont inutiles. Ainsi si un des $\gamma_i \succ 1/4$ on applique (3).

Si $\gamma_i \leq 1/4$, pour tout i, on utilise (4): d'après (4) et (6), l'inégalité (5) est vérifiée dès qu'on a simultanément les inégalités

$$\gamma \prec \alpha\beta \tag{13}$$

$$\gamma \succ \frac{1}{3} + \frac{4}{3}\alpha(1-\beta) \tag{14}$$

$$\gamma \prec 1 - 4\alpha(1-\beta) \tag{15}$$

Par (7), on remplace la condition (13), par la condition plus forte:

$$\gamma \leq \frac{1}{2} \tag{16}$$

et la condition (15) devient superflue. Enfin compte-tenu de (7) on voit que

$$\frac{1}{4} + \frac{1}{3} + \frac{4}{3}\alpha(1-\beta) \prec \frac{2}{3} - \frac{4}{3}\alpha(1-\beta). \tag{17}$$

Soit τ la plus grande des sommes formées de σ_i et de γ_j, inférieures à $\frac{1}{3}+\frac{4}{3}\alpha(1-\beta)$. D'après (17) n'importe lequel des $\gamma_{i'}$ ou $\sigma_{j'}$ qui ne participe pas à la somme τ vérifie

$$\frac{1}{3} + \frac{4}{3}\alpha(1-\beta) \prec \tau + \sigma \prec \frac{2}{3} - \frac{4}{3}\alpha(1-\beta);$$

on applique (4) avec $\gamma = \inf\{\tau+\sigma, 1-(\tau+\sigma)\} \leq \frac{1}{2}$, qui satisfait les conditions (16) et (14).

Il apparaît que, dans notre traitement des sommes de type I (Lemme 2.5), nous sommes essentiellement limités par les termes provenant des inégalités de type grand crible (voir [D-I]) et que la contribution des valeurs propres exceptionnelles du laplacien est minime, par conséquent la conjecture de *Selberg* pour les groupes de congruences n'apporterait pas d'amélioration à notre méthode.

4 Une généralisation de la Proposition de Fouvry, Iwaniec et Katz

Comme on l'a vu le traitement des sommes de type I repose sur la formule des traces de Kuznetzov, et faute d'une formule similaire impliquant les puissances symétriques des sommes de Kloosterman, on ne peut traiter les sommes de type I pour les fonctions sym_i $(i \geq 2)$. Pour les sommes de type II en revanche, le Lemme 2.4 se généralise pour les autres moments sous la forme du Théorème suivant, qui était implicitement démontré dans [F-I-K].

Soit $r = p_1 p_2 \dots p_k$ un entier *sans facteurs carrés*, on note pour $i = 1 \dots k$, $\hat{p}_i = r/p_i$.

Pour tout caractère additif modulo r, ψ, *d' ordre* n, on note, $Kl^{\psi}(l, m; r)$, la somme de *Kloosterman* relative à ce caractère:

$$Kl^{\psi}(l, m; r) = \sum_{\substack{x (\mathrm{mod}\ r) \\ (x,r)=1}} \psi(lx + m\overline{x});$$

si ψ est le caractère $\mathrm{e}(\frac{\cdot}{r})$ on l'écrira simplement $Kl(l, m; r)$. Si $(m, r) = 1$, la majoration de *Weil* 2.3(1), permet de définir l'angle de la somme de *Kloosterman* $\theta^{\psi}_{r,m}$ par la formule

$$\cos \theta^{\psi}_{r,m} = \frac{Kl^{\psi}(1, m; r)}{2^{\omega(r)} \sqrt{r}};$$

Par multiplicativité croisée cette formule se réecrit

$$\cos \theta^{\psi}_{r,m} = \cos \theta^{\psi_1}_{p_1, \overline{\hat{p}_1}^2 m} \dots \cos \theta^{\psi_k}_{p_k, \overline{\hat{p}_k}^2 m},$$

où ψ_i désigne le caractère mod p_i définit par $\psi_i(m) = \psi(\hat{p}_i m)$.

Théorème 4.1 . — *Pour tout entier s, soit f_s une fonction sur $\mathbf{Z}/s\mathbf{Z}$ à valeurs complexes dont le module est majoré par une fonction $f(s)$ croissante. Soit (λ_m) une suite de complexes et $i_1, \dots, i_k$ des entiers ≥ 1, et ψ un caractère de $\mathbf{Z}/r\mathbf{Z}$ d'ordre r, alors on a la majoration*

$$\mathcal{A} := \sum_{\substack{s \leq S \\ (r,s)=1}} \Big| \sum_{\substack{m \leq M \\ (m,r)=1}} f_s(m) \lambda_m \,\mathrm{sym}_{i_1}(\theta_{p_1, m\overline{s}^2 \overline{\hat{p}_1}^2}) \dots \mathrm{sym}_{i_k}(\theta_{p_k, m\overline{s}^2 \overline{\hat{p}_k}^2}) \Big|^2$$

$$\ll \ 4^k C(r)^{1/2}\|\lambda(M)\|^2 MS\log S f(S)^2 (\frac{1}{r^{1/4}}+\frac{r^{1/4}}{S^{1/2}}+\frac{S}{M}),$$

avec

$$C(r)=65^k\prod_{j=1}^{k}(i_j+1)^4.$$

De plus, la constante impliquée dans le symbole de Landau *est absolue.*

On notera que ce théorème est intéressant pour

$$r>1,\ S^2\geq r,\ M\geq S.$$

Preuve. — La preuve s'inspire de la démonstration du Théorème 2 de [F-I-K], rappelons la brièvement: on commence par faire un découpage dyadique sur la variable s, ce qui fournit $O(\log S)$ sommes du type ci-dessous, et on introduit un poids continu pour $s\in[S,4S]$

$$\omega(s)=\min\{s/S-1,1,4-s/S\}$$

alors par *Cauchy-Schwarz*,

$$\mathcal{A} \quad \ll \sum_{s,\ (s,r)=1}\omega(s)\sum_{b\ mod\ s}|f_s(b)|^2|\sum_{\substack{m\equiv b(s)\\(m,r)=1}}\lambda_m\,\mathrm{sym}_{i_1}(\theta_{p_1,m\overline{s}^2\overline{\hat{p}_1}^2})\ldots\mathrm{sym}_{i_k}(\theta_{p_k,m\overline{s}^2\overline{\hat{p}_k}^2})|^2$$

$$\ll Sf(S)^2\sum_{(s,r)=1}\omega(s)\sum_{\substack{m_1\equiv m_2(s)\\(m_1m_2,r)=1}}\lambda_{m_1}\overline{\lambda}_{m_2}\,\mathrm{sym}_{i_1}(\theta_{p_1,m_1\overline{s}^2\overline{\hat{p}_1}^2})\,\mathrm{sym}_{i_1}(\theta_{p_1,m_2\overline{s}^2\overline{\hat{p}_1}^2})\ldots$$

Les termes $m_1=m_2$ contribuent par

$$\Lambda Sf(S)^2\prod_{j=1}^{k}(i_j+1)^2,$$

où on a posé $\Lambda=\|\lambda(M)\|^2$. Pour les autres termes, on choisit comme nouvelle variable de sommation t, définie par

$$|m_1-m_2|=st,\quad 1\leq t\leq T=M/S,$$

ce qui nous mène par le même chemin que dans [F-I-K] à la majoration:

$$\mathcal{A}\leq\ Sf(S)^2\sum_{t\leq T}\mathcal{A}_t\quad+O(\Lambda Sf(S)^2\prod_{j=1\ldots k}(i_j+1)^2),$$

où,

$$\mathcal{A}_t=\sum_{\substack{(m_1-m_2,tr)=t\\(m_1m_2,r)=1}}\lambda_{m_1}\overline{\lambda}_{m_2}\omega(\frac{|m_1-m_2|}{t})$$

$$\mathrm{sym}_{i_1}(\theta_{p_1,m_1\overline{(m_1-m_2)/t}^2\overline{\hat{p}_1}^2})\,\mathrm{sym}_{i_1}(\theta_{p_1,m_2\overline{(m_1-m_2)/t}^2\overline{\hat{p}_1}^2})\ldots$$

L'inégalité de *Cauchy-Schwarz* donne

$$\mathcal{A}_t{}^2 \leq \Lambda(1+\frac{M}{rt}) \sum_{\substack{m_1\equiv m_2\ (t) \\ m_1\neq m_2\ (m_1m_2,r)=1}} |\lambda_{m_1}|^2 |V(m_1,m_2;r)|, \tag{18}$$

où l'on a posé pour tout caractère additif, ψ, mod r, d'ordre r,

$$V^{\psi}(m_1,m_2;r) = \sum_{\substack{z(tr),(z,r)=1 \\ (z-m_1,tr)=t \\ (z-m_2,tr)=t}} \prod_{j=1\ldots k} \operatorname{sym}_{i_j}(\theta^{\psi_j}_{p_j,m_1\overline{(m_1-z)/t}^2\overline{\hat{p}_j}^2}) \operatorname{sym}_{i_j}(\theta^{\psi_j}_{p_j,z\,\overline{(m_1-z)/t}^2\overline{\hat{p}_j}^2})$$
$$\times \quad \operatorname{sym}_{i_j}(\theta^{\psi_j}_{p_j,m_2\overline{(m_2-z)/t}^2\overline{\hat{p}_j}^2}) \operatorname{sym}_{i_j}(\theta^{\psi_j}_{p_j,z\,\overline{(m_2-z)/t}^2\overline{\hat{p}_j}^2}).$$

Proposition 4.2 . — *Si* $m_1 \equiv m_2$ *(mod* t*) et* $(r, m_1m_2) = 1$*, alors on a la majoration*

$$V^{\psi}(m_1,m_2;r) \ll C(r)(m_1-m_2,r)^{1/2}r^{1/2}.$$

Nous reportons la preuve de cette Proposition à la fin de cette section. D'après cette proposition et (18), on a

$$\mathcal{A}_t{}^2 \ll \Lambda^2(1+\frac{M}{rt}) \sum_{1\leq l\leq M/t} (l,r)^{1/2}(t,r)^{1/2}C(r)r^{1/2}$$

$$\mathcal{A}_t \ll \Lambda(1+\sqrt{\frac{M}{rt}})C(r)^{1/2}\tau(r)^{1/2}(t,r)^{1/4}\frac{M^{1/2}}{t^{1/2}}r^{1/4},$$

et finalement

$$\sum_t \mathcal{A}_t \ll C(r)^{1/2}\tau(r)^{3/2}\Lambda M(\frac{1}{r^{1/4}}+\frac{r^{1/4}}{S^{1/2}}),$$

ici on a eu recours aux inégalités classiques

$$\sum_{t\leq T}(t,r)^{1/2} \ll T\tau(r)\ ,\ \ et\ \sum_{t\leq T}\frac{(t,r)^{1/4}}{t} \ll \tau(r)\log T.$$

□

Preuve. — (de la Proposition 4.2) Si $r = r_1r_2$ (nécessairement $(r_1, r_2) = 1$), par le Théorème des restes chinois, on a l'égalité

$$V^{\psi}(m_1,m_2;r) = V^{\psi_1}(m_1,m_2;r_1)V^{\psi_2}(m_1,m_2;r_2),$$

où ψ_1 et ψ_2 sont deux caractères modulo r_1 et r_2 respectivement. On est donc ramené au cas $k = 1$, $r = p$, $i_1 = i$ (comme dorénavant, dans cette démonstration le caractère $\psi \pmod p$ est fixé, on ne l'écrira plus); si $p=2$ ou 3 ou que $p|m_1-m_2$ par sommation triviale on a,

$$V := V(m_1,m_2;p) \leq (i+1)^4 p.$$

Sinon, après le changement de variable $z = m_1 + (m_1-m_2)/(x-1)$, la somme V devient

$$\begin{aligned} V = \sum_{\substack{x (\mathrm{mod}\ p)\\ (x(x-1),p)=1}} & \mathrm{sym}_i(\theta_{p,m_1(x-1)^2})\,\mathrm{sym}_i(\theta_{p,(x-1)(m_1x-m_2)}) \\ \times\ & \mathrm{sym}_i(\theta_{p,m_2(\overline{x}-1)^2})\,\mathrm{sym}_i(\theta_{p,(\overline{x}-1)(m_2\overline{x}-m_1)}). \end{aligned}$$

La contribution du terme $x = m_2\overline{m}_1$ est $\leq (i+1)^4$, dès lors on peut supposer que dans la sommation, x vérifie la condition supplémentaire $(m_1x-m_2,p)=1$. Un peu de géométrie algébrique est nécessaire: reprenons les notations de l'appendice de [F-I-K], soit X_p l'ouvert de $\mathbf{P}^1\otimes\mathbf{F}_p$

$$X_p = Spec(\mathbf{F}_p[T,\frac{1}{T(T-1)(m_1T-m_2)}]) = \mathbf{P}^1\otimes\mathbf{F}_p - \{0,1,m_2/m_1,\infty\},$$

et on considère les 4 morphismes de $\mathbf{G}_m\otimes\mathbf{F}_p = \mathbf{P}^1\otimes\mathbf{F}_p - \{0,\infty\} \to X_p$:

$$\begin{aligned} f_1(T) &= m_1(T-1)^2 \\ f_2(T) &= (T-1)(m_1T-m_2) \\ f_3(T) &= m_2(T^{-1}-1)^2 \\ f_4(T) &= (T^{-1}-1)(m_2T^{-1}-m_1). \end{aligned}$$

On considère le $\overline{\mathbf{Q}}_l$-faisceau de *Kloosterman*, $\mathcal{K}l$ et on forme les quatres faisceaux lisses sur X_p

$$\mathcal{K}l_j := f_j^*(\mathcal{K}l),\ j=1\dots,4,$$

puis les faisceaux

$$\mathcal{K}l_j^i := \mathrm{Sym}_i(\mathcal{K}l_j),$$

obtenus par composition des représentations $\mathcal{K}l_j$ avec la représentation puissance symétrique i-ème de SL_2 (on rappelle qu'elle est irréductible de dimension $i+1$). Par définition, la trace du frobenius de $\mathcal{K}l_j^i$ en un point fermé x de X_p est $\mathrm{sym}_i(\theta_{p,f_j(x)})$, Si bien que la somme V est associée au faisceau

$$\mathcal{F}^i := \mathcal{K}l_1^i\otimes\mathcal{K}l_2^i\otimes\mathcal{K}l_3^i\otimes\mathcal{K}l_4^i,$$

qui est lisse sur X_p, de rang $(i+1)^4$ pur de poids 0. Par la formule des traces de *Lefschetz*, et les travaux de *Deligne* [D], il suffit donc de montrer que le groupe de monodromie géomérique associé, $G_{geom}(\mathcal{F}^i)$, agit irréductiblement, et de majorer $|\chi_c(X_p \otimes \overline{\mathbf{F}}_p, \mathcal{F}^i)|$.

Considérons sur X_p, le faisceau lisse, $\mathcal{F} = \mathcal{K}l_1 \oplus \mathcal{K}l_2 \oplus \mathcal{K}l_3 \oplus \mathcal{K}l_4$; en appendice de [F-I-K], *Katz* a montré (Lemme 3) en utilisant le critère de *Goursat-Kolchin-Ribet*, l'égalité

$$G_{geom}(\mathcal{F}) = SL_2 \times SL_2 \times SL_2 \times SL_2.$$

Comme $\mathrm{Sym}_i(\mathrm{std}_2) \otimes \mathrm{Sym}_i(\mathrm{std}_2) \otimes \mathrm{Sym}_i(\mathrm{std}_2) \otimes \mathrm{Sym}_i(\mathrm{std}_2)$ est une représentation irréductible de $G_{geom}(\mathcal{F}) = SL_2 \times SL_2 \times SL_2 \times SL_2$ de dimension $(i+1)^4$, $G_{geom}(\mathcal{F}^i)$ agit irréductiblement. D'autre part, d'après le Théorème 1 de cette appendice $|\chi_c(X_p \otimes \overline{\mathbf{F}}_p, \mathcal{F})| \leq 64$, on trouve donc à l'aide de la formule de *Grothendieck-Ogg-Shafarevitch*

$$|\chi_c(X_p \otimes \overline{\mathbf{F}}_p, \mathcal{F}^i)| \leq (i+1)^4 |\chi_c(X_p \otimes \overline{\mathbf{F}}_p, \mathcal{F})| \leq 64(i+1)^4;$$

et on a finalement

$$V \leq 64(i_1+1)^4 p^{1/2} + (i_1+1)^4 \leq 65(i_1+1)^4 p^{1/2};$$

cela conclut la preuve de la Proposition 4.2.

□

5 Première application

Nous montrons, dans cette section le Théorème 1.2

5.1 Extraction du terme principal .

On considère, pour k entier, la somme,

$$\sum_{m \leq M} \lambda_m \sum_{r \leq R} \sum_{\substack{s \leq S \\ (m,rs)=1}} \mu^2(rs) \left(\frac{Kl(1,m;rs)}{2^{\omega(rs)}\sqrt{rs}} \right)^k, \tag{19}$$

avec la convention que λ_m vaut constamment 1 si k est pair .

D'après le Lemme 2.7 (appliqué avec $j=0$), $\cos^k \theta_{p,m}$ vaut en moyenne

$$\alpha_{0,k} = \int_{[0,\pi]} \cos^k \theta \mu_{ST}(\theta) < 1$$

(on rappelle que les sym_i forment une famille orthonormale sur $[0,\pi]$ pour la mesure de *Sato–Tate*); l'objet du Théorème 1.2 est de faire apparaître cette quantité dans un terme principal de la somme (19).

On désignera par un indice

- $-_1$ un nombre dont tous les facteurs premiers sont $\leq \log^B x$, (B sera fixé par la suite).
- $-_2$ un nombre dont tous les facteurs premiers sont $> \log^B x$;

ainsi, tout nombre r se factorise de manière unique sous la forme $r = r_1 r_2$ (avec éventuellement $r_2 = 1$); on pose également $X = \exp(\log^{1/3} x)$. On rappelle qu'on se trouve sous les hypothèses suivantes:

$$R = x^\rho,\ S = x^{1-\rho},\ M = x^\lambda,\ 1/2 \leq \rho < 2/3,\ 1-\rho < \lambda \leq 1; \tag{20}$$

par une majoration triviale, on peut supposer que l'entier rs vérifie en plus la minoration $rs > X$.

On commence par faire , sur la variable r, le découpage suivant

$$\begin{aligned}\sum_{r\leq R}\sum_{\substack{s\leq S\\ rs>X}} \mu^2(rs) \sum_{\substack{m\\ (m,rs)=1}} \lambda_m \cos^k \theta_{rs,m} &= \sum_{r_1r_2\leq R}\dots\\ &= \sum_{r_1\leq X}\sum_{r_1r_2\leq R}\dots + \sum_{r_1>X}\sum_{r_1r_2\leq R}\dots\\ &= \Sigma_1 \quad + \quad \Sigma_2.\end{aligned}$$

La somme Σ_2 est majorée grâce au Lemme 2.6:

$$\Sigma_2 \leq |\lambda(M)|S|\{r\leq R; r_1 > X\}| \ll \|\lambda(M)\| M^{1/2} x \exp(-c_0(B)\frac{\log^{1/3} x}{\log_2 x}), \tag{21}$$

ce qui est admissible.

Reste Σ_1: par multiplicativité croisée, cette somme vaut

$$\sum_{r_2}\sum_{r_1}\sum_{s} \mu^2(r_1r_2s) \sum_{m\leq M} \lambda_m \Big(\frac{Kl(1, m\overline{r}_2^2; r_1 s)}{2^{\omega(r_1 s)}\sqrt{r_1 s}}\Big)^k \Big(\frac{Kl(1, m\overline{r_1 s}^2; r_2)}{2^{\omega(r_2)}\sqrt{r_2}}\Big)^k,$$

avec les conditions de sommations

$$\log^B x \leq r_2 \leq R,\ s\leq S,\ r_1 \leq X,\ r_1r_2 \leq R,\ r_1r_2s > X,\ (m, r_1r_2s) = 1. \tag{22}$$

On rappelle que si $p|r_2$, on note $\hat{p} = r_2/p$; on a les égalités

$$\Sigma_1 = \sum_{r_2}\sum_{r_1,s} \mu^2(r_1r_2s) \sum_m \lambda_m \cos^k(\theta_{r_1 s, m\overline{r}_2^2}) \prod_{p|r_2} (\alpha_{0,k} + \cos^k(\theta_{p, m\overline{r_1 s\hat{p}}^2}) - \alpha_{0,k})$$

d'où

$$\begin{aligned}\Sigma_1 = \quad & \sum_{r_2} \alpha_{0,k}^{\omega(r_2)} \sum_{r_1,s} \mu^2(r_1 s r_2) \sum_m \lambda_m \cos^k(\theta_{r_1 s, m\overline{r}_2^2})\\ & + O(\sum_{r_2} \mu^2(r_2) \sum_{\substack{d_2|r_2\\ d_2\neq 1}} \alpha_{0,k}^{\omega(r_2/d_2)} R_k(d_2)),\end{aligned} \tag{23}$$

et où $R_k(d_2)$ est un terme d'erreur et désigne la quantité

$$R_k(d_2) = \sum_{\substack{s' \le \min\{SX,\ x/r_2\} \\ (r_2,s')=1}} \mu^2(s')\tau(s')|\sum_m \lambda_m \cos^k(\theta_{s',m\overline{r}_2^2}) \prod_{p|d_2} (\cos^k(\theta_{p,m\overline{s'\hat{p}}^2}) - \alpha_{0,k})|.$$

D'après le Lemme 2.7, en notant $\omega = \omega(d_2)$, et $d_2 = p_1 \dots p_\omega$, on a

$$\prod_{p|d_2} \dots = \sum_{i_1=1}^{k} \dots \sum_{i_\omega=1}^{k} \alpha_{i_1,k} \dots \alpha_{i_\omega,k} \operatorname{sym}_{i_1}(\theta_{p_1,m\overline{s'\hat{p}_1}^2}) \dots \operatorname{sym}_{i_\omega}(\theta_{p_\omega,m\overline{s'\hat{p}_\omega}^2}),$$

et donc $R_k(d_2)$ est majoré par

$$\sum_{i_1=1}^{k} \dots \sum_{i_\omega=1}^{k} \alpha_{i_1,k} \dots \alpha_{i_\omega,k} \sum_{s'} \tau(s')|\sum_m \lambda_m \cos^k(\theta_{s',m\overline{r}_2^2}) \operatorname{sym}_{i_1}(\theta_{\dots}) \dots \operatorname{sym}_{i_\omega}(\theta_{\dots})|,$$

(dans le Lemme 2.7, les $\alpha_{i,k}$ sont positifs ou nuls). Par application de l'inégalité de *Cauchy-Schwarz*, du Théorème 4.1, de (22) et compte tenu du fait que $d_2 \ge \log^B x$ (car $d_2 \ne 1$), on obtient la majoration:

$$\begin{aligned} R_k(d_2) \quad & \ll \|\lambda(M)\| M^{1/2} \frac{x}{r_2} \log^2 x \left(\frac{1}{\log^{B/8} x} + \frac{R^{1/8}}{S^{1/4}} + \frac{(XS)^{1/2}}{M^{1/2}}\right) \times \\ & \qquad (65^{1/4}.2)^\omega \sum_{i_1=1}^{k} \dots \sum_{i_\omega=1}^{k} \alpha_{i_1,k} \dots \alpha_{i_\omega,k} (i_1+1) \dots (i_\omega+1) \\ & \ll \|\lambda(M)\| M^{1/2} \frac{x}{r_2} (\log x)^{2-B/8} (65^{1/4}.2(1-\alpha_{0,k}))^\omega, \end{aligned}$$

d'après (20) et la relation

$$\sum_{i=0}^{k} (i+1)\alpha_{i,k} = 1.$$

On en déduit facilement que le deuxième terme de (23) est majoré par

$$\sum_{r_2} \mu^2(r_2) \sum_{\substack{d_2|r_2 \\ d_2 \ne 1}} \alpha_{0,k}^{\omega(r_2/d_2)} R_k(d_2) \ll \|\lambda(M)\| M^{1/2} \frac{x}{(\log x)^{B/8-1-65^{1/4}.4(1-\alpha_{0,k})}}. \tag{24}$$

5.2 Le cas k impair .

Cette manipulation est inutile si k est impair, en effet $\alpha_{0,k} = 0$: il n'est plus nécessaire de découper la variable r en $r = r_1 r_2$, le premier terme de (23) est nul, le second se réduit à $\sum_r \mu^2(r) R_k(r)$ et

$$R_k(r) \ll \|\lambda(M)\| M^{1/2} S\left(\frac{1}{R^{1/8}} + \frac{R^{1/8}}{S^{1/4}} + \frac{S^{1/2}}{M^{1/2}}\right)(2.65^{1/4})^{\omega(r)};$$

donc, d'après (20) on a montré la deuxième partie du Théorème.

5.3 Le cas k pair .

On suppose maintenant que k est pair (que l'on réécrit $2k$) et donc que $\lambda_m = 1$.

Traitons le premier terme de (23): on commence par relâcher la contrainte $(m, r_2) = 1$ en notant que

$$|\{m \leq M; (m, r_2) \neq 1\}| \leq \omega(r_2)\frac{M}{\log^B x},$$

ce qui est acceptable.

En développant en série de *Fourier* la somme sur m, on obtient:

$$= \frac{1}{r_1 s}\sum_{j=0}^{r_1 s-1}\mathcal{F}(\cos^{2k}(\theta_{r_1 s, \_\overline{r_2}^2}), j; r_1 s)\sum_{m\leq M}\mathrm{e}(\frac{jm}{r_1 s})$$

$$= \frac{M}{r_1 s}\mathcal{F}(\cos^{2k}(\theta_{r_1 s, \_\overline{r_2}^2}), 0; r_1 s) + \frac{1}{r_1 s}\sum_{j=1}^{r_1 s-1}\ldots,$$

Dans la définition de la transformée de *Fourier* ci-dessus, on impose — en dépit de l'égalité $Kl(1,0;p) = -1$!— $\cos^{2k}(\theta_{r_1 s, m\overline{r_2}^2}) = 0$ pour $(m, r_1 s) \neq 1$; de ce fait, la condition $(m, r_1 s) = 1$ disparaît dans la transformée de *Fourier*.

Le premier terme de Σ_1 se réécrit sous la forme

$$\sum_{r_2}\alpha_{0,2k}^{\omega(r_2)}\sum_{r_1,s}\mu^2(r_1 s r_2)\sum_m \cos^{2k}(\theta_{r_1 s, m\overline{r}_2^2})$$

$$= \sum_{r_2}\mu^2(r_2)\alpha_{0,2k}^{\omega(r_2)}(M\mathcal{TP}(r_2) + \mathcal{TE}(r_2)),$$

où $\mathcal{TP}(r_2)$ correspond au terme $j = 0$ du développement en série de *Fourier* et constitue le terme principal:

$$\mathcal{TP}(r_2) = \sum_{r_1 s}\frac{\mu^2(r_1 r_2 s)}{r_1 s}\mathcal{F}(\cos^{2k}(\theta_{r_1 s, \_\overline{r_2}^2}), 0; r_1 s);$$

alors que $\mathcal{TE}(r_2)$ correspond aux termes $\frac{1}{r_1 s}\sum_{j=1}^{r_1 s-1}\ldots$, et est un terme d'erreur:

$$\mathcal{TE}(r_2) = \sum_{r_1 s}\frac{\mu^2(r_1 r_2 s)}{r_1 s}\sum_{j=1}^{r_1 s-1}\mathcal{F}(\cos^{2k}(\theta_{r_1 s, \_\overline{r_2}^2}), j; r_1 s/d)\sum_{m=1}^{M}\mathrm{e}(\frac{-jm}{r_1 s}).$$

Majoration des termes d'erreurs .

Par application du Théorème des restes chinois, et des Lemmes 2.7 et 2.8 , on obtient la majoration (pour s' sans facteurs carrés)

$$|\mathcal{F}(\cos^{2k}(\theta_{s', \_\overline{r_2}^2}), j; s)| \leq c_k^{\omega(s')}(j, s')^{1/2}s'^{1/2},$$

avec $c_k \geq 1$ ne dépendant que de k; on trouve alors que $\mathcal{TE}(r_2)$ est majoré par

$$\begin{aligned}\mathcal{TE}(r_2) \quad &\ll \sum_{1\leq s'\leq 2SX} \frac{\tau(s')c_k^{\omega(s')}}{s'^{1/2}} \sum_{\substack{j=-(s'-1)/2\\ j\neq 0}}^{(s'-1)/2} (j,s')^{1/2}\frac{s'}{j} \\ &\ll SX \sum_{1\leq s'\leq 2SX} \frac{\tau^2(s')c_k^{\omega(s')}\log(s')}{s'^{1/2}} \\ &\ll S^{3/2+\epsilon}.\end{aligned}$$

et donc

$$\sum_{r_2} \alpha_{0,2k}^{\omega(r_2)} \mathcal{TE}(r_2) \ll_\epsilon R^{1+\epsilon}S^{3/2+\epsilon} \ll xM\frac{S^{1/2+\epsilon}}{M}. \tag{25}$$

Ce terme est donc admissible compte tenu de l'inégalité $M > S^{1+\epsilon}$.

Traitement du terme principal .

Le terme principal $\mathcal{TP}(r_2)$, est traité de manière analogue: par application du Théorème des restes chinois, et des Lemmes 2.7 et 2.8 (avec $j = 0$), on obtient l'égalité

$$\mathcal{F}(\cos^{2k}(\theta_{r_1 s, \overline{r_2}^2}), 0; r_1 s) = r_1 s \prod_{p|r_1 s} (\alpha_{0,2k} + R_p),$$

et donc

$$\mathcal{TP}(r_2) = \sum_{r_1,s} \mu^2(r_1 s r_2) \prod_{p|r_1 s} (\alpha_{0,2k} + R_p)$$

où R_p un terme d'erreur *ne dépendant que de p et non de r_2* vérifiant

$$|R_p| \leq (1-\alpha_{0,2k})p^{-1/2} + \alpha_{0,2k}p^{-1} \leq p^{-1/2}.$$

Remarquons également que

$$0 < p\alpha_{0,2k} + pR_p = \sum_{\substack{m \pmod p\\ (m,p)=1}} \cos^{2k}(\theta_{p,m}) < p. \tag{26}$$

En sommant la variable r_2, on forme le terme principal de (23)

$$\mathcal{TP} = M \sum_{r_1,r_2,s} \mu^2(r_1 r_2 s)\alpha_{0,2k}^{\omega(r_2)} \prod_{p|r_1 s} (\alpha_{0,2k} + R_p);$$

tenant compte de la définition de r_2 ($p|r_2 \Rightarrow p > \log^B x$), on voit que

$$|\alpha_{0,2k}^{\omega(r_2)} - \prod_{p|r_2}(\alpha_{0,2k} + R_p - \frac{1}{(2\sqrt{p})^{2k}})| \leq \frac{2^{\omega(r_2)}}{\log^{B/2} x},$$

et donc que $\mathcal{TP}$ se réécrit sous la forme :

$$\mathcal{TP} = M \sum_{\substack{r_1 \le X \\ r_1 r_2 s > X}} \mu^2(r_1 r_2 s) \prod_{p | r_1 r_2 s} (\alpha_{0,2k} + R_p) + O(M \frac{x}{(\log x)^{B/2-4}});$$

Par une nouvelle application du Lemme 2.6 et par une majoration triviale, on supprime, à un terme admissible près, les contraintes $r_1 \le X$ et $rs > X$, pour finalement obtenir une forme plus sympathique de $\mathcal{TP}$

$$\mathcal{TP} = M \sum_{\substack{r \le R \\ s \le S}} \mu^2(rs) \prod_{p|rs} (\alpha_{0,2k} + R_p) + O(M \frac{x}{(\log x)^{B/2-4}}). \tag{27}$$

5.4 Application de la méthode de Selberg-Delange .

On estime maintenant le terme principal $\mathcal{TP}$ grâce au lemme 2.9.

On commence par évaluer séparément la somme

$$\mathcal{S}_r(S) := \sum_{s \le S,\ (r,s)=1} \mu^2(s) \prod_{p|s} (\alpha_{0,2k} + R_p).$$

Soit, $F_r(z)$, la série de *Dirichlet*, à coefficients positifs (26)), définie par

$$F_r(z) = \prod_{p \nmid r} (1 + \frac{\alpha_{0,2k} + R_p}{p^z});$$

par (26) la série de *Dirichlet*

$$F_r(z) \prod_{p|r} (1 + \frac{\alpha_{0,2k} + R_p}{p^z})$$

vérifie la propriété $\mathcal{P}(\alpha_{0,2k}; c_0, \delta, H)$, pour certaines constantes $0 < c_0 < 1/2$, δ, H, qu'on n'explicitera pas, et, (cf les notations du Lemme 2.9), $G_{\alpha_{0,2k}}(z)$ ne s'annule pas au point 1. D'après (26), on a, pour tout $\eta > 0$ et pour $\Re e z > 1 - c_0$, la minoration

$$|\prod_{p|r} (1 + \frac{\alpha_{0,2k} + R_p}{p^z})| \gg_\eta (1+\eta)^{-\omega(r)},$$

Il s'ensuit que $F_r(z)$ vérifie également $\mathcal{P}(\alpha_{0,2k}; c_0, \delta, (1+\eta)^{\omega(r)} H')$ et par application du Lemme 2.9, on a

$$\mathcal{S}_r(S) = \frac{S}{(\log S)^{1-\alpha_{0,2k}}} (1 + O_k(\frac{(1+\eta)^{\omega(r)}}{\log S})) G_{\alpha_{0,2k}}(1) \prod_{p|r} (1 + \frac{\alpha_{0,2k} + R_p}{p})^{-1}.$$

Pour conclure, il reste à estimer la somme suivante, sur la variable r,

$$\sum_{r \le R} \mu^2(r) \prod_{p|r} (\alpha_{0,2k} + R_p)(1 + \frac{\alpha_{0,2k} + R_p}{p})^{-1}.$$

On le fait, grâce à une dernière application du Lemme 2.9, et on obtient

$$\mathcal{TP} = C_k MRS(\log R)^{\alpha_{0,2k}-1}(\log S)^{\alpha_{0,2k}-1}(1 + O_k(\frac{1}{\log^{1-2\eta} x})).$$

Il suffit de choisir B assez grand, puis de réunir (21), (23) , (24), (25), et cette dernière estimée. Cela achève la preuve du Théorème 1.2.

6 Seconde application

On va se contenter, ici, d'esquisser la preuve du Théorème 1.4.

Soient (λ_m) une suite de complexes, $x > 0$ un réel, et $\alpha,\ \beta$ des réels vérifiant les inégalités:

$$1/3 < \alpha \leq 1/2, \ \textit{et}\ \alpha < \beta.$$

Pour des raisons de densité, il suffit de prouver, pour tout $\epsilon > 0$, assez petit, l'égalité,

$$\sum_{\substack{p\leq x^{1-\alpha},\ q\leq x^{\alpha} \\ p\neq q}} \sum_{\substack{m\leq x^{\beta} \\ (m,pq)=1}} \lambda_m\ \mathrm{sym}_i(\theta_{p,\overline{q}^2m})\,\mathrm{sym}_j(\theta_{q,\overline{p}^2m}) = O_\epsilon(\|\lambda(M)\|x^{\beta/2+1-\epsilon}),$$

pour tout couple d'entiers $i, j \geq 0$ vérifiant $i + j > 0$.

On peut supposer que les variables p et q satisfont $p \sim x^{1-\alpha}/2,\ q \sim x^{\alpha}/2$ (on se ramène à ce cas par découpage).

- Si $i > 0$, on utilise le Théorème 4.1 en choisissant $r = p$, $s = q$, et $f_s(m) = \mathrm{sym}_j(\theta_{q,\overline{p}^2m})$.
- Si $i = 0$, $j > 0$, on applique *Cauchy-Schwarz* pour obtenir

  $$|\sum_m \lambda_m \sum_q \mathrm{sym}_j(\theta_{q,\overline{p}^2m})|^2 \leq \|\lambda(x^\beta)\|^2 \sum_{q_1,q_2} \sum_{\substack{m\leq x^\beta \\ (m,q_1q_2)=1}} \mathrm{sym}_j(\theta_{q_1,\overline{p}^2m})\,\mathrm{sym}_j(\theta_{q_2,\overline{p}^2m}).$$

  On traite trivialement le cas $q_1 = q_2$, autrement, on fait un développement en série de *Fourier*, sur la fonction de $\mathbf{Z}/q_1q_2\mathbf{Z}$, $\mathrm{sym}_j(\theta_{q_1,\overline{p}^2m})\,\mathrm{sym}_j(\theta_{q_2,\overline{p}^2m})$. Le théorème des restes chinois et le Lemme 2.8 permettent alors de montrer que

  $$\sum_m \lambda_m \sum_q \mathrm{sym}_j(\theta_{q,\overline{p}^2m}) \ll \|\lambda(x^\beta)\|x^{\alpha+\beta/2}(x^{-\alpha/2} + x^{(\alpha-\beta)/2}\log x);$$

  on conclut la preuve grâce à nos hypothèses.

7 APPENDICE: preuve du Lemme 2.4

On aura besoin du résultat général suivant qui est une généralisation facile au cas des fractions du lemme 2 p.38 de [H-B2] (nous n'en donnerons pas de démontration):

Lemme 7.1 . — *Soit* $P(\mathbf{x})$, $Q(\mathbf{x})$, $\in Z[x_1,\dots,x_n]$ *et* A *un sous-ensemble de* $(\mathbf{Z}/p\mathbf{Z})^n$, *qui ne contient pas les zeros de* $Q \pmod p$. *Pour tout caractère additif, d'ordre* p^f *modulo* p^f, ψ, *soit*

$$S^\psi = \sum_{\substack{\mathbf{x} \ mod \ p^f \\ \mathbf{x}\in A}} \psi(P(\mathbf{x})\overline{Q(\mathbf{x})}).$$

Pour plus de simplicité, on écrira pour $\mathbf{x}$ *défini modulo* p^f

$$F(\mathbf{x}) := \frac{P(\mathbf{x})}{Q(\mathbf{x})} := P(\mathbf{x})\overline{Q(\mathbf{x})}$$

et soit

$$B = \{\mathbf{x} \ mod(p^g):\ \mathbf{x}\in A,\ p^g \mid \nabla F(\mathbf{x})\ \}$$

(∇F *désigne le gradient de* F*), alors*

$$|S^\psi| \leq p^{nf/2}\sharp B \qquad (si\ f = 2g \geq 2)$$

$$|S^\psi| \leq p^{nf/2}\sum_{\mathbf{x}\in\ B} p^{(n-r(\mathbf{x}))/2} \quad (si\ f = 2g+1 \geq 3)$$

où $r(\mathbf{x})$ *est le rang de la forme quadratique* $Q_{\mathbf{x}}$ *sur* $\mathbf{F}_p$ *représentée par la matrice*

$$\left(\frac{1}{2}\frac{\partial^2 F}{\partial x_i \partial x_j}\right)_{i,j=1\dots n}$$

(si $p = 2$ *on pose* $r(\mathbf{x}) = 0$*).*

On commence par prouver le résultat intermédiaire suivant (cf la PROPOSITION de [F-I-K], mais ici r n'est plus sans facteurs carrés):

Proposition 7.2 . — *Soient* m_1, m_2, r, t, a *des entiers non nuls tels que:* $m_1 \equiv m_2 \pmod t$ *ie* $m_1 - m_2 = tk$ *et* $(r, am_1m_2) = 1$. *Alors, pour tout caractère additif modulo* r, *d'ordre* r, ψ, *posons*

$$V^\psi(m_1,m_2;r) := \sum_{\substack{z' (\mathrm{mod}\ tr) \\ (z'-m_1,ts)=t \\ (z'-m_2,tr)=t}} Kl^\psi(a\overline{\tfrac{m_1-z'}{t}}, m_1\overline{\tfrac{m_1-z'}{t}}; r) Kl^\psi(a\overline{\tfrac{m_1-z'}{t}}, z'\overline{\tfrac{m_1-z'}{t}}; r)$$

$$Kl^\psi(a\overline{\tfrac{m_2-z'}{t}}, m_2\overline{\tfrac{m_2-z'}{t}}; r) Kl^\psi(a\overline{\tfrac{m_2-z'}{t}}, z'\overline{\tfrac{m_2-z'}{t}}; r);$$

on a la majoration

$$V^{\psi}(m_1, m_2; r) \ll_{\epsilon} f_{k,t}(r) r^{5/2+\epsilon}$$

et f est la fonction multiplicative définie comme suit: si $p^f \| r$ on pose, pour toute la suite $t = p^{\alpha} t'$, $(t', p) = 1$, $k = p^{\beta} k'$, $(k', p) = 1$,et $g = [f/2]$, alors,

$$\begin{aligned} f_{k,t}(2^f) &= 2^{f/2} && \textit{puis si } p \neq 2 \\ f_{k,t}(p) &= (p, p^{\alpha+\beta})^{1/2} && \textit{si } f = 1 \\ f_{k,t}(p^f) &= p^{(f-2g)/2} && \textit{si } f \geq 2 \textit{ et } 3\alpha + \beta < g \\ f_{k,t}(p^f) &= p^{f/2} && \textit{si } f \geq 2 \textit{ et } 3\alpha + \beta \geq g \end{aligned}$$

7.1 Preuve de la Proposition 7.2 .

Preuve. — par multiplicativité, il suffit de prouver ce lemme pour $r = p^f$ avec $p \neq 2$ (si $p = 2$, on somme trivialement la variable z en appliquant la majoration de *Weil* 2.3(1). On pose alors

$$z' = m_1 - tz, \;\; m_2 = m_1 - tk$$

$$V^{\psi}(m_1, m_2; s) := \sum_{\substack{z (\mathrm{mod}\ p^f) \\ (z(z-k), p) = 1}} \; \sum_{\substack{x_1 \ldots x_4 \mathrm{mod}\ p^f \\ (x_1 x_2 x_3 x_4, p) = 1}} \psi(F(x_1, x_2, x_3, x_4, z))$$

où $F(x_1, x_2, x_3, x_4, z)$ est la fraction

$$\frac{ax_1}{z} + \frac{m_1}{zx_1} + \frac{ax_2}{z} + \frac{m_1 - tz}{zx_2} +$$

$$\frac{ax_3}{z-k} + \frac{m_1 - tk}{(z-k)x_3} + \frac{ax_4}{z-k} + \frac{m_1 - tz}{(z-k)x_4}$$

- Si $f = 1$ on tombe sous le coup de la proposition p.274 de [F-I-K].
- Si $f > 1$ on applique le lemme 7.1, alors

$$\nabla F = \begin{pmatrix} \frac{1}{z}(a - \frac{m_1}{x_1^2}) \\ \frac{1}{z}(a - \frac{m_1 - tz}{x_2^2}) \\ \frac{1}{z-k}(a - \frac{m_1 - tk}{x_3^2}) \\ \frac{1}{z-k}(a - \frac{m_1 - tz}{x_4^2}) \\ \frac{-ax_1}{z^2} - \frac{m_1}{z^2 x_1} - \frac{ax_2}{z^2} - \frac{m_1}{z^2 x_2} - \\ \frac{ax_3}{(z-k)^2} - \frac{m_1 - tk}{(z-k)^2 x_3} - \frac{ax_4}{(z-k)^2} - \frac{m_1 - tk}{(z-k)^2 x_4} \end{pmatrix}$$

On cherche donc le nombre de solutions mod p^g de l'équation

$$\nabla F = 0$$

c'est à dire les solutions du système:

$$ax_1^2 = m_1 \tag{28}$$

$$ax_2^2 = m_1 - tz \tag{29}$$

$$ax_3^2 = m_1 - tk \tag{30}$$

$$ax_4^2 = m_1 - tz \tag{31}$$

$$\frac{a}{z^2 x_2}(x_1 + x_2)^2 + \frac{a}{(z-k)^2 x_4}(x_3 + x_4)^2 = 0 \tag{32}$$

$$(\ z(z-k)x_1x_2x_3x_4, p\ ) = 1 \tag{33}$$

dont on déduit

$$a(x_1^2 - x_2^2) = tz \tag{34}$$

$$a(x_1^2 - x_3^2) = tk \tag{35}$$

Quitte à poser $z_1 = t'z$ et $k_1 = t'k$, on peut pour résoudre ce système, supposer que $t' = 1$. Nous ferons un usage abusif du fait suivant:

considérons l'équation

$$x^2 + ax + b = 0\ (p^g)$$

si $\Delta := a^2 - 4b \not\equiv 0 (\mathrm{mod}\ p)$ *cette équation a autant de solutions que celle modulo p, soit au plus* 2 *solutions.* On en déduit tout d'abord que notre système a en général au plus $O(p^g)$ solutions (mod p^g); ce n'est pas suffisant et dans la discussion suivante, on va affiner cette estimation.

Soit (x_1, x_2, x_3, x_4, z) une solution, alors

$$x_2 = \pm x_4$$

de plus $x_1^2 = x_2^2$ mod p^α mais pas mod $p^{\alpha+1}$

- Si $x_2 = x_4$, (32) devient

$$(z-k)^2(x_1 + x_2)^2 + z^2(x_3 + x_2)^2 = 0\ (\mathrm{mod}\ p^g) \tag{36}$$

- Si $x_2 = -x_4$, (32) devient

$$(z-k)^2(x_1 + x_2)^2 - z^2(x_3 - x_2)^2 = 0\ (\mathrm{mod}\ p^g) \tag{37}$$

Cas $(x_1 + x_2, p) = 1$ **.**
Dans ce cas, on a $(x_3 + x_4, p) = 1$ et on sépare encore en deux sous-cas:

- Si $x_2 = x_4$, alors si -1 n'est pas un carré mod p^g, il n'y a pas de solutions. Sinon de (36) on déduit

$$(z - k)(x_1 + x_2) = \bar{i}z(x_3 + x_2) \pmod{p^g} \tag{38}$$

où $\bar{i}$ est un racine de -1, puis on multiplie les deux membres par t, et par (34) et (35) on obtient

$$(x_3 - x_2)(x_3 + x_2)(x_1 + x_2) = \bar{i}(x_1 - x_2)(x_1 + x_2)(x_3 + x_2) \pmod{p^g}$$

il est alors permis de simplifier par $(x_3 + x_2)(x_1 + x_2)$ pour obtenir

$$x_2 = \frac{\bar{i}x_1 - x_3}{\bar{i} - 1}$$

et z est alors bien déterminé: si $\alpha = 0$ on utilise le lemme 2.3 , si $\alpha \geq 1$ on utilise (38) (on a en effet $x_1 = x_3$ mod p, et $\bar{i} \neq 1$). En conclusion, on a au plus $O(1)$ solutions.

- Si maintenant $x_2 = -x_4$, (37) devient:

$$(z - k)(x_1 + x_2) = \pm z(x_3 - x_2) \pmod{p^g}; \tag{39}$$

en faisant la même manipulation que précédemment, on en déduit que:

  - soit $x_2 = \frac{x_1 - x_3}{2}$, mais alors comme $(p, x_2) = 1$ on en tire $\alpha = \beta = 0$, et z est déterminé par (29).
  - soit $x_3 = -x_1 (\text{mod } p^g)$ mais ceci n'est possible que si

$$g \leq \alpha + \beta \leq 3\alpha + \beta$$

et on a alors $O(p^g)$ solutions.

Remarque. — le cas $(x_1 + x_2, p) = 1$ englobe complètement le cas $(t, p) = 1$.

Cas $x_1 + x_2 = 0 (\text{mod } p)$ **.**
La méthode est toute différente. Notons d'abord par (32) que

$$x_3 + x_4 = 0 (\text{mod } p)$$

et nécessairement $\alpha \geq 1$, ce qui permet d' utiliser ce lemme de développement limité:

Lemme 7.3 . — *Soient* $1 \leq \alpha \leq g$ *deux entiers et* $x_1, x_2, z \in \mathbf{Z}/p^g\mathbf{Z}$ *vérifiant* $(2x_1x_2, p) = 1$,

$$x_2^2 = x_1^2 - p^\alpha z \text{ et de plus } x_2 = x_1 (\mathrm{mod}\ p),$$

alors, il existe $B \in \mathbf{Z}/p^g\mathbf{Z}$ *tel que*

$$x_2 = x_1 - \frac{zp^\alpha}{2x_1} - \frac{z^2p^{2\alpha}}{8x_1^3} + Bp^{3\alpha} \ (\mathrm{mod}\ p^g)$$

Dans la suite, on suppose $g > 3\alpha + \beta$ dans le cas contraire on majore le nombre de solutions par $O(p^g)$.

- Si $x_2 = x_4$, par le lemme 7.3 on a

$$x_2 = -x_1 \ (\mathrm{mod}\ p), \quad x_2 = -x_1 + \tfrac{zp^\alpha}{2x_1} + Bp^{2\alpha},$$

$$x_3 = x_1 \ (\mathrm{mod}\ p), \quad x_3 = x_1 - \tfrac{kp^\alpha}{2x_1} + B'p^{2\alpha},$$

  et (36) devient

$$(40) \qquad \begin{array}{l} (z-k)^2(\frac{zp^\alpha}{2x_1} + Bp^{2\alpha})^2 = -z^2(\frac{(z-k)p^\alpha}{2x_1} + B'p^{2\alpha})^2 \ (\mathrm{mod}\ p^g) \\ (z-k)(\frac{z}{2x_1} + Bp^\alpha) = \bar{i}z(\frac{(z-k)}{2x_1} + B'p^\alpha) \ (\mathrm{mod}\ p^{g-2\alpha}). \end{array}$$

  Ce qui implique l'égalité

$$(z-k)\frac{z}{2x_1} = \bar{i}z\frac{(z-k)}{2x_1} (\mathrm{mod}\ p),$$

  qui est impossible.

- Si $x_2 = -x_4$, d'après le lemme 7.3, on a

$$x_2 = -x_1 \ (\mathrm{mod}\ p) \quad x_2 = -x_1 + y_2p^\alpha$$

$$x_3 = -x_1 \ (\mathrm{mod}\ p) \quad x_3 = -x_1 + y_3p^\alpha$$

  avec

$$y_2 = \frac{z}{2x_1} + \frac{z^2p^\alpha}{8x_1^3} + Bp^{2\alpha} \ (\mathrm{mod}\ p^{g-\alpha})$$

$$y_3 = \frac{k}{2x_1} + \frac{k^2p^\alpha}{8x_1^3} + B'p^{2\alpha+3\beta} \ (\mathrm{mod}\ p^{g-\alpha}),$$

  et (37) prend la forme suivante

$$(41) \qquad (z-k)^2y_2^2 = z^2(y_2 - y_3)^2 \ (p^{g-2\alpha}).$$

  Comme $y_2 \not\equiv 0 \ (\mathrm{mod}\ p)$ on a donc

$$(z-k)y_2 = \pm z(y_2 - y_3) \ (\mathrm{mod}\ p^{g-2\alpha})$$

– Si c'est le signe "−",on a alors

$$2z\frac{(z-k)}{2x_1} = 0 \pmod p$$

ce qui est impossible d'après (33).

– Si c'est le signe "+", on obtient $ky_2 = zy_3 \pmod{p^{g-2\alpha}}$, soit

$$k\frac{z^2}{8x_1^3} + Bp^{\alpha+\beta} = z\frac{k^2}{8x_1^3} + B'p^{\alpha+3\beta} \pmod{p^{g-3\alpha}}.$$

Si maintenant $\beta = 0$,le terme de moindre valuation fournit

$$z - k = 0 \pmod{p^\alpha}.$$

Si $\beta > 0$, le terme de moindre valuation est $k\frac{z^2}{8x_1^3}$ qui doit être nul $\pmod{p^{\inf(\alpha+\beta, 2\beta, g-3\alpha)}}$. Dans les deux cas on rencontre une absurdité du fait que $\alpha > 1$ et l'hypothèse $g > 3\alpha + \beta$.

Ceci démontre la proposition dans le cas où $f = 2g$ est pair. Si $f = 2g + 1$, la matrice héssienne calculée aux points solutions de l'équation $\nabla F = 0$ et vérifiant (33) vaut

$$\begin{pmatrix} \frac{2a}{zx_1} & 0 & 0 & 0 & 0 \\ 0 & \frac{2a}{zx_2} & 0 & 0 & \frac{t}{zx_2^2} \\ 0 & 0 & \frac{2a}{zx_2} & 0 & 0 \\ 0 & 0 & 0 & \frac{2a}{(z-k)x_4} & \frac{t}{zx_4^2} \\ 0 & \frac{t}{zx_2^2} & 0 & \frac{t}{zx_4^2} & \frac{-2ak(x_1+x_2)^2}{z^3(z-k)x_2} \end{pmatrix},$$

et son rang est minoré par 4. D' après le lemme 7.1 cela termine la démontration de la proposition 7.2.

□

7.2 Fin de la preuve .

Remarquons d'abord qu'il suffit de montrer l'inégalité (2) quand on impose la condition de sommation supplémentaire sur les s: $(r, s) = 1$. en effet, posons $rs = rr_1s_1$ avec $r_1s_1 = s, r_1 \mid r^\infty$, $(r, s_1) = 1$ alors

$$\sum_{1\leq s\leq S} |\sum_{m\leq M} \lambda_m Kl(1, m; rs)|^2 = \sum_{\substack{r_1|r^\infty \\ r_1\leq S}} \sum_{\substack{1\leq s_1\leq S/r_1 \\ (r_1,rr_1)=1}} |\sum_{m\leq M} \lambda_m Kl(1, m; r_1s_1s)|^2;$$

on applique (2), et on utilise la majoration facile

$$\sum_{\substack{r_1|r^\infty \\ r_1\leq S}} \frac{s_1^{\flat 1/4} r_1^{\sharp 1/6}}{r_1^{1/4-\epsilon}} = O_\epsilon(\log(R)s^\epsilon),$$

pour conclure.

Dès lors, il suffit de reprendre *verbatim* [F-I-K] à partir de la page 274 (9) (voir aussi le début de la preuve du Théorème 4.1).

Par la Proposition 7.2, on a la majoration:

$$\begin{aligned}
\mathcal{A}_t{}^2 &\ll \|\lambda\|(1+\frac{M}{tr})\sum_{m_1\equiv m_2 \pmod t}|\lambda_{m_1}\lambda_{m_2}V(m_1,m_2;r)| \\
&\ll \|\lambda\|(1+\frac{M}{tr})\sum_{m_1\equiv m_2 \pmod t}|\lambda_{m_1}|^2|V(m_1,m_2;r)| \\
&\ll \|\lambda\|^2(1+\frac{M}{tr})r^{5/2+\epsilon}(r^{1/2}+\sum_{1\le k\le L/t}f_{k,t}(r))
\end{aligned}$$

le premier terme de cette dernière expression est évalué comme dans [F-I-K]; quand au second, après sommation sur la variable t, on applique l'inégalité de *Cauchy-Schwarz*; ainsi, on aboutit à la majoration,

$$\sum_{1\le t\le T}\mathcal{A}_t \ll \|\lambda(M)\|Mr^{1+\epsilon}(r^{1/2}/S)+$$

$$\|\lambda\|r^{5/4+\epsilon}(\sum_{1\le t\le T}1+\frac{M}{tr})^{1/2}(\sum_{t\le T}\sum_{1\le k\le M/t}f_{k,t}(s))^{1/2};$$

on remplace le produit $1\le kt\le M$ par une variable m au prix d'un terme en M^ϵ, et on majore la fonction $f_{k,t}(s)$ par la fonction $f_{1,kt}(s)$. On obtient finalement (on rappelle la notation $g=[f/2]$):

$$\begin{aligned}
\sum_{1\le m\le M}\frac{f_m(r)}{r} \ll \quad & L^\epsilon r^{\flat 1/2}\times\prod_{\substack{p\le M\\ p\nmid r}}(\frac{1}{1-p^{-1}}) \\
& \times\prod_{p\|r}(\frac{1}{1-p^{-1/2}}) \\
& \times\prod_{\substack{p^f\|r\\ p\neq 2}}(\sum_{0\le n<g/3}\frac{1}{p^n}+p^g\sum_{g/3\le n}\frac{1}{p^n}) \\
\ll\ & (Mr)^\epsilon r^{\flat 1/2}r^{\sharp 1/3},
\end{aligned}$$

ce qui conclut la preuve du Lemme 2.4.

Bibliographie

[B-F-I] E. BOMBIERI, J.B. FRIEDLANDER et H. IWANIEC. — *Primes in arithmetic progressions to large moduli,* Acta Math. Vol. 156 (1986) 203-251.

[D-I] J.-M. DESHOUILLERS et H. IWANIEC. — *Kloosterman Sums and Fourier Coefficients of Cusp Forms*, Invent. math. 70 (1982), 219-288.

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

[D-F-I] W. DUKE, J. B. FRIEDLANDER et H. IWANIEC. — *Equidistribution of roots of quadratic congruences of prime moduli*, Ann. of Math, 141 (1995), 423-441.

[Du-I] W. DUKE et H. IWANIEC. — *A relation between cubic exponential and Kloosterman sums*, Contemp. Maths., vol 143, (1993) 255-258.

[F-I-K] E. FOUVRY, H. IWANIEC et N.M. KATZ. — *The divisor function over arithmetic progressions,* Acta. Arith. LXI.3 (1992).

[H-B] D.R. HEATH-BROWN. — *Prime number in short intervals and a generalized Vaughan identity,* Canad. J. Math., 34 (1982) 1365-1377.

[H-B2] D.R. HEATH-BROWN. — *The divisor function $d_3(n)$ in arithmetic progressions,* Acta Arith., XLVII (1986), 29-56.

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

[Ho] C. HOOLEY. — *On the distribution of the roots of polynomial congruences,* Mathematika 11 (1964), 39-49.

[Ku] N.V. KUZNETZOV. — *Petterson hypothesis for parabolic forms of weight zero and Linnik hypothesis,* Math. Sb. 111(153) (1980), 334-383.

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

[Sa] P. SARNAK. — *Some applications of modular forms,* Cambridge Tracts in Math. 99 (1990).

[Te1] G. TENENBAUM. — *Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné,* Compositio Math. 51 (1984), 243-263.

[Te2] G. TENENBAUM. — *Introduction à la théorie analytique et probabiliste des nombres,* Publ. Inst. Elie Cartan.

[We1] A. WEIL. — *On some exponential sums,* Proc. Nat. Acad. Sci. 34 (1948), 204-207.