

Astérisque

JEAN-PIERRE SERRE

Majorations de sommes exponentielles

Astérisque, tome 41-42 (1977), p. 111-126

<http://www.numdam.org/item?id=AST_1977__41-42__111_0>

© Société mathématique de France, 1977, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

MAJORATIONS DE SOMMES EXPONENTIELLES

par

Jean-Pierre SERRE

Les "sommages exponentielles" considérées ici sont celles qui sont liées à la géométrie algébrique sur un corps fini (cf. [15], sections L 05 et T 25). Les résultats récents de Deligne sur la conjecture de Weil ([6], [7]) permettent d'en donner de bonnes majorations, au moins dans certains cas : c'est ce que Deligne lui-même montre dans [8]. Dans ce qui suit, j'expose, sans démonstrations, quelques uns des résultats les plus frappants de [8].

1. Sommages exponentielles

Notations

Si $x \in \mathbb{C}$, et si m est un entier ≥ 1 , on pose

$$(1.1) \quad e_m(x) = \exp(2\pi i x/m) .$$

La lettre p désigne un nombre premier. Si $x \in \mathbb{Z}$, $e_p(x)$ appartient au groupe μ_p des racines p -ièmes de l'unité, et l'application $x \mapsto e_p(x)$ définit par passage au quotient un isomorphisme

$$(1.2) \quad e_p : \mathbb{Z}/p\mathbb{Z} \rightarrow \mu_p .$$

On note k un corps fini à $q = p^a$ éléments. Si $x \in k$, on pose

$$(1.3) \quad \text{Tr}_k(x) = \text{Tr}_{k/\mathbb{F}_p}(x) = x + x^p + \dots + x^{p^{a-1}}$$

et

$$(1.4) \quad \psi_k(x) = e_p(\text{Tr}_k(x)) ;$$

cela a un sens, puisque $\text{Tr}_k(x)$ appartient à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. L'application

$$\psi_k : k \rightarrow \mu_p$$

est un caractère du groupe additif de k , et tout caractère de ce groupe est de la forme

$$x \mapsto \psi_k(cx) ,$$

avec $c \in k$.

On choisit une clôture algébrique \bar{k} de k . Si $n \geq 1$, on note k_n la sous-extension de \bar{k} qui est de degré n sur k . On a :

$$(1.5) \quad \psi_{k_n}(x) = \psi_k(\text{Tr}_{k_n/k}(x)) = \psi_k(x + x^q + \dots + x^{q^{n-1}})$$

pour tout $x \in k_n$.

Définition des sommes S et S_n

Soit X une variété algébrique sur k , et f une "fonction régulière" sur X , autrement dit une section du faisceau structural \mathcal{O}_X . On pose :

$$(1.6) \quad S = S(X, f) = \sum_{x \in X(k)} \psi_k(f(x)) ;$$

la sommation porte sur tous les points x de X à valeurs dans k ; si x est un tel point, on a $f(x) \in k$, ce qui donne un sens à l'expression $\psi_k(f(x))$.

(Exemple : si X est l'espace affine de dimension r , on a $X(k) = k^r$, et f s'identifie à un polynôme en r variables x_1, \dots, x_r ; la somme exponentielle S est simplement :

$$(1.7) \quad S = \sum_{x_i \in k} \psi_k(f(x_1, \dots, x_r)) .$$

Nous reviendrons au n° 6 sur cet exemple.)

A côté de la somme S , qui est relative à k , il est commode d'introduire les

sommes

$$(1.8) \quad S_n = S_n(X, f) = \sum_{x \in X(k_n)} \psi_{k_n}(f(x)) \quad , \quad n \geq 1 .$$

On a $S_1 = S$.

Fonction L attachée à (X, f)

Soit t une indéterminée. On pose :

$$(1.9) \quad L(t) = L(X, f; t) = \exp\left(\sum_{n=1}^{\infty} S_n t^n / n\right) .$$

C'est une série formelle à coefficients dans le corps cyclotomique $\mathbb{Q}(\mu_p)$. On peut l'interpréter (cf. par exemple [1]) comme la fonction L d'Artin $L(X'/X; e_p)$ associée au revêtement $X' \rightarrow X$ de groupe de Galois $\mathbb{Z}/p\mathbb{Z}$ défini par l'équation

$$(1.10) \quad y^p - y = f(x) ,$$

et au caractère e_p de son groupe de Galois. On a :

$$(1.11) \quad L(t) = \prod_P (1 - \lambda(P) t^{\deg(P)})^{-1} ,$$

où P parcourt l'ensemble des points fermés du schéma X , et $\lambda(P)$ est donné par

$$(1.12) \quad \lambda(P) = \psi_{k(P)}(f(P)) ,$$

où $k(P)$ désigne le corps résiduel de l'anneau local \mathcal{O}_P ; on a

$$(1.13) \quad \deg(P) = [k(P):k] .$$

La formule (1.11) montre en particulier que les coefficients de $L(t)$ sont des entiers du corps $\mathbb{Q}(\mu_p)$.

Généralisation

Les sommes exponentielles considérées ci-dessus sont de type additif : elles ne font intervenir que des caractères du groupe additif du corps fini k (ou k_n) .

Il y a lieu d'introduire également des sommes mixtes, du type

$$(1.14) \quad S = S(X, f, g) = \sum_{x \in X(k)} \psi_k(f(x)) \chi(g(x)) ,$$

où g est une fonction régulière inversible sur X , et χ un caractère du groupe

multiplicatif k^* . Les S_n sont alors définis par :

$$(1.15) \quad S_n = \sum_{x \in X(k_n)} \psi_{k_n}(f(x)) \chi_{(N_{k_n}/k)}(g(x)).$$

Tous les résultats des n° 2 et 3 restent valables.

2. Résultats généraux

On a tout d'abord :

THÉOREME 2.1 - La série $L(t)$ est une fonction rationnelle de t .

Cela peut se démontrer, soit par la méthode p-adique de Dwork ([9],[1]), soit par la méthode ℓ -adique ($\ell \neq p$) de Grothendieck [10] ; nous reviendrons là-dessus au n° 3.

On peut reformuler (2.1) en disant qu'il existe des nombres complexes α_i et β_j , en nombre fini, tels que

$$(2.2) \quad L(t) = \prod (1 - \beta_j t) / \prod (1 - \alpha_i t),$$

ou, ce qui revient au même,

$$(2.3) \quad S_n = \sum_i (\alpha_i)^n - \sum_j (\beta_j)^n \quad \text{pour tout } n \geq 1.$$

Bien entendu, on peut supposer que la famille $\{\alpha_i, \beta_j\}$ est réduite, c'est-à-dire qu'aucun α_i n'est égal à un β_j . Supposons que ce soit le cas. On montre facilement que les α_i et les β_j sont alors des entiers algébriques ; ces entiers jouissent de la propriété suivante :

THÉOREME 2.4 - Si ω est l'un des α_i, β_j , il existe un entier $r = r(\omega)$, appelé le poids de ω , tel que tous les conjugués de ω soient de valeur absolue (complexe) égale à $q^{r/2}$.

Ce résultat est conséquence d'un théorème de Deligne [7] sur les valeurs propres des endomorphismes de Frobenius ; voir [8], § 1 ainsi que (3.4) ci-après. D'après (2.3), on en déduit :

COROLLAIRE 2.5 - Soit r le plus grand des poids des α_i et des β_j . On a

$$(2.6) \quad |S_n| = \underline{O}(q^{nr/2}) \quad \text{quand } n \rightarrow \infty ,$$

et $|S_n|$ n'est $\underline{O}(q^{n\alpha})$ pour aucun $\alpha < r/2$.

Remarque 2.6. Le corollaire (2.5) a la curieuse conséquence suivante : si

$$|S_n| = \underline{O}(q^{n\alpha}) \quad \text{pour un nombre réel } \alpha ,$$

on a ipso facto $|S_n| = \underline{O}(q^{nr/2})$, où r est la partie entière de 2α . Ainsi, par exemple, dans le cas des sommes de Kloosterman à deux variables, Carlitz [3] a montré que $|S_n| = \underline{O}(q^{11n/8})$; comme la partie entière de $11/4$ est 2 , on en déduit, d'après ce qui précède, que $|S_n| = \underline{O}(q^n)$. (On a même $|S_n| \leq 3q^n$, cf. (5.6) .)

3. Un critère cohomologique

Si l'on veut majorer explicitement les S_n par la méthode indiquée au n° 2 ci-dessus, il est nécessaire de connaître le nombre des α_i, β_j , ainsi que leurs poids. C'est là un problème non trivial, qui n'est résolu que dans des cas particuliers (cf. n°s 4,5,6). L'interprétation cohomologique de $L(t)$ due à Grothendieck [10] permet de dégager un cas favorable, celui où (X, f) est purement de poids r au sens de la définition (3.6) ci-dessous. Avant de donner cette définition, il est nécessaire de rappeler quelques uns des résultats de [10] et de [8] :

On fixe un nombre premier $\ell \neq p$, ainsi qu'un plongement de $\mathbb{Q}(\mu_p)$ dans une extension finie K_ℓ du corps ℓ -adique \mathbb{Q}_ℓ . Par "torsion" au moyen du revêtement $X' \rightarrow X$, on définit un certain faisceau ℓ -adique \mathcal{F}_ℓ , qui est localement libre de rang 1 sur K_ℓ . Si \bar{X} désigne la \bar{k} -variété déduite de X par extension du corps de base, on peut parler des groupes de cohomologie $H^i(\bar{X}; \mathcal{F}_\ell)$, ainsi que des groupes de cohomologie à supports propres $H_c^i(\bar{X}; \mathcal{F}_\ell)$. Ce sont des K_ℓ -espaces vectoriels de dimension finie ; ils sont nuls pour $i < 0$ et $i > \dim(X)$. Le morphisme de Frobenius F de \bar{X} opère de façon naturelle sur ces espaces ; notons $F|H^i$ et $F|H_c^i$ les K -endomorphismes ainsi définis. Le lien entre ces endomorphis-

mes et les sommes exponentielles S_n du n° 1 est fourni par la formule des traces

$$(3.1) \quad S_n = \sum_i (-1)^i \operatorname{Tr}(F^n | H_C^i) \quad , \quad \text{cf. [10],}$$

où S_n est interprété comme un élément de K_ℓ , via le plongement choisi de $\mathbb{Q}(\mu_p)$ dans K_ℓ ; si l'on note w_{ij} les valeurs propres de $F | H_C^i$ (dans une extension convenable de K_ℓ) , la formule (3.1) peut se récrire :

$$(3.2) \quad S_n = \sum_{i,j} (-1)^i (w_{ij})^n .$$

Elle équivaut aussi à :

$$(3.3) \quad L(t) = \prod_i \det(1 - t F | H_C^i)^{(-1)^{i+1}} .$$

Dans [7], Deligne montre que chacune des valeurs propres w_{ij} est un entier algébrique possédant un poids entier $r(i,j)$ au sens de (2.4), autrement dit tel que :

$$(3.4) \quad \text{tous les conjugués de } w_{ij} \text{ sont de valeur absolue } q^{r(i,j)/2} .$$

On a de plus

$$(3.5) \quad 0 \leq r(i,j) \leq i .$$

(3.6) Soit r un entier ≥ 0 . Nous dirons que (X,f) est purement de poids r si :

(3.6.1) X est non singulière et toutes ses composantes irréductibles sont de dimension r ;

$$(3.6.2) \quad H_C^i(\bar{X}; \mathcal{F}_\ell) = 0 \quad \text{pour tout } i \neq r ;$$

$$(3.6.3) \quad \text{l'homomorphisme canonique } H_C^r(\bar{X}; \mathcal{F}_\ell) \rightarrow H^r(\bar{X}; \mathcal{F}_\ell) \text{ est injectif.}$$

L'intérêt de ces conditions provient du résultat suivant, qui se déduit de (3.5) en utilisant la dualité de Poincaré (cf. [8], § 1) :

THÉOREME 3.7 - Si (3.6.1) et (3.6.3) sont vérifiées, toutes les valeurs propres de $F | H_C^r$ sont de poids r .

Posons

$$(3.8) \quad B = \dim. H_C^r(\bar{X}; \mathcal{F}_\ell) \quad , \quad \text{r-ième nombre de Betti de } \mathcal{F}_\ell .$$

Soient $\omega_1, \dots, \omega_B$ les valeurs propres de $F|_{H_C^r}$. Si l'on suppose (3.6.2) vérifié, on a, d'après (3.2) :

$$(3.9) \quad S_n = (-1)^r \sum_{i=1}^{i=B} (\omega_i)^n$$

et par suite

$$(3.10) \quad L(t) = \begin{cases} \prod (1 - \omega_i t) & \text{si } r \text{ est impair} \\ 1/\prod (1 - \omega_i t) & \text{si } r \text{ est pair.} \end{cases}$$

Vu (3.7), on en déduit (Deligne [8], § 1) :

THÉOREME 3.11 - Si (X, f) est purement de dimension r , et de nombre de Betti égal à B , on a

$$|S_n| \leq Bq^{nr/2} \quad \text{pour tout } n .$$

De plus, le cor. 2.5 montre que, si $B \neq 0$, l'exposant $r/2$ est "le meilleur possible" : on n'a $|S_n| = O(q^{n\alpha})$ pour aucun $\alpha < r/2$.

Remarque - La majoration de $|S_n|$ fournie par (3.11) est de l'ordre de grandeur de la racine carrée de la majoration triviale $|S_n| \leq \text{Card.} X(k_n)$; d'un point de vue probabiliste, c'est ce que l'on pouvait espérer de mieux.

4. Exemple : sommes à une variable

On suppose que X est une courbe affine non singulière, absolument irréductible (par exemple la droite affine privée d'un nombre fini de points). On note \hat{X} la courbe projective correspondante, et X_∞ l'ensemble des points du schéma \hat{X} qui n'appartiennent pas à X ("points à l'infini"). Si $P \in X_\infty$, on note v_P la valuation correspondante du corps des fonctions rationnelles sur \hat{X} . Le revêtement étale $X' \rightarrow X$ défini par (1.10) se prolonge en un revêtement (en général ramifié) \hat{X}' de \hat{X} . On note \tilde{f} son conducteur. On a

$$(4.1) \quad \tilde{f} = \sum_{P \in X_\infty} n_P P ,$$

où l'entier n_P est défini de la manière suivante :

$$(4.2.1) \quad \text{si } \hat{X}' \rightarrow \hat{X} \text{ est non ramifié en } P, \text{ i.e. s'il existe une fonction}$$

rationnelle φ sur \hat{X} telle que $v_P(f - \varphi^D + \varphi) \geq 0$, on pose $n_P = 0$;

(4.2.2) sinon, on pose $n_P = 1 - \sup_{\varphi} v_P(f - \varphi^D + \varphi)$; on a $n_P \geq 2$.

THEOREME 4.3 - (i) Pour que (X, f) soit purement de poids 1 au sens de (3.6), il faut et il suffit que le revêtement $\hat{X}' \rightarrow \hat{X}$ soit ramifié en tous les points P de X_{∞} , i.e. que $n_P > 0$ pour tout $P \in X_{\infty}$.

(ii) Si (i) est vérifié, le nombre de Betti B correspondant, cf. (3.8), est donné par :

$$(4.4) \quad B = 2g - 2 + \deg(\tilde{f}) ,$$

où g est le genre de la courbe \hat{X} , et $\deg(\tilde{f}) = \sum n_P \deg(P)$.

Au langage près, ce résultat est dû à Weil [18] (voir aussi [1],[20] et [8], § 3). Vu (3.11), il entraîne (Weil, loc.cit.) :

COROLLAIRE 4.5 - Si (i) est vérifié, il existe des entiers algébriques $\omega_1, \dots, \omega_B$ de poids 1 tels que :

$$(4.6) \quad S_n = - \sum_{i=1}^{i=B} (\omega_i)^n , \quad L(t) = \prod_{i=1}^{i=B} (1 - \omega_i t) .$$

On a

$$(4.7) \quad |S_n| \leq B q^{n/2} \quad \text{pour tout } n .$$

Indiquons deux cas particuliers (on en trouvera d'autres dans [20]) :

Sommes de Kloosterman (cf. [4], [12], [13], [18], [20])

On prend pour X la droite affine privée de $\{0\}$, et pour f la fonction $x + c/x$, avec $c \in k^*$. Les sommes S_n s'écrivent

$$(4.8) \quad S_n = \sum_{x \in k_n^*} \varphi_{k_n}(x + c/x) = \sum_{\substack{xy=c \\ x, y \in k_n}} \varphi_{k_n}(x + y) .$$

On a $X_{\infty} = \{0, \infty\}$, et $n_0 = n_{\infty} = 2$. D'après (4.3), (X, f) est purement de poids 1, et $B = 0 - 2 + 4 = 2$. On a donc

$$(4.9) \quad S_n = - (\lambda^n + \mu^n) , \quad \text{avec } |\lambda| = |\mu| = q^{1/2} ,$$

d'où l'inégalité (due à Weil [18]) :

$$(4.10) \quad |S_n| \leq 2 q^{n/2} .$$

On peut montrer ([4], [8]) que

$$(4.11) \quad \lambda\mu = q, \quad \text{i.e.} \quad \mu = \bar{\lambda}.$$

Il en résulte que les S_n sont déterminés par $S_1 = S$. Signalons à ce sujet le problème suivant :

(4.12) Prenons $c = 1$, $q = p$, de sorte que $S = \sum e_p(x + 1/x)$ est un nombre réel compris entre $-2\sqrt{p}$ et $2\sqrt{p}$. Quelle est la distribution de S/\sqrt{p} dans le segment $[-2, 2]$ lorsque p varie ?

Sommes polynomiales (cf. [18], [20])

On prend pour X la droite affine, et pour f un polynôme de degré d non divisible par p . Les sommes S_n s'écrivent :

$$(4.13) \quad S_n = \sum_{x \in k_n} \psi_{k_n}(f(x)).$$

On a $X_\infty = \{\infty\}$, et $n_\infty = 1 + d$. D'après (4.3), (X, f) est purement de poids 1, et $B = 0 - 2 + 1 + d = d - 1$. On a donc

$$(4.14) \quad S_n = - \sum_{i=1}^{i=d-1} (\varphi_i)^n, \quad \text{avec} \quad |\varphi_i| = q^{1/2},$$

et

$$(4.15) \quad |S_n| \leq (d-1) q^{n/2}, \quad \text{cf. [18]}.$$

Noter le cas particulier $d = 1$, où $S_n = 0$ (relations d'orthogonalité des caractères !) ainsi que le cas $d = 2$, où S_n est une somme de Gauss quadratique.

(Je renvoie à [5], [8], [18], [19], [20] pour les propriétés des sommes de Gauss générales et des sommes de Jacobi ; ce sont des sommes de type "mixte", cf. (1.14) et (1.15).)

5. Exemple : sommes de Kloosterman généralisées

Soient r un entier ≥ 1 et c un élément de k^* . On prend pour X l'hyper-surface de l'espace affine de dimension $r + 1$ définie par l'équation

$$(5.1) \quad x_0 \dots x_r = c,$$

et l'on prend pour f la fonction $x_0 + \dots + x_r$. Les sommes S_n correspondantes

s'écrivent

$$(5.2) \quad S_n = \sum_{\substack{x_0 \dots x_r = c \\ x_i \in k_n}} \psi_{k_n}(x_0 + \dots + x_r) .$$

Ce sont des sommes de Kloosterman généralisées (cf. [3], [8], [14], [16], [17]) ; pour $r = 1$, on retrouve les sommes de Kloosterman usuelles (4.8).

THÉOREME 5.3 - Le couple (X, f) ci-dessus est purement de poids r , avec pour nombre de Betti $B = r + 1$.

Ce résultat est dû à Deligne ([8], § 7). Vu (3.11), il entraîne :

COROLLAIRE 5.4 - Il existe des entiers algébriques $\omega_0, \dots, \omega_r$ de poids r tels que

$$(5.5) \quad S_n = (-1)^r \sum_{i=0}^{i=r} (\omega_i)^n .$$

On a

$$(5.6) \quad |S_n| \leq (r+1)q^{nr/2} \quad \text{pour tout } n .$$

L'existence d'entiers algébriques $\omega_0, \dots, \omega_r$ tels que l'on ait la formule (5.5) a également été établie par Sperber [17], en utilisant une méthode p -adique.

Sperber démontre en outre (si $p > r + 3$) :

$$(5.7) \quad \omega_0 \dots \omega_r = q^{r(r+1)/2} \quad (\text{voir aussi Deligne, } \underline{\text{loc.cit.}}) .$$

(5.8) Si $|\cdot|_p$ désigne une valeur absolue p -adique sur $Q(\omega_0, \dots, \omega_r)$, on peut ordonner les ω_i de telle sorte que $\omega_i = q^i u_i$, avec $|u_i|_p = 1$ pour $i = 0, \dots, r$.

6. Exemple : sommes polynomiales à plusieurs variables

On prend pour X l'espace affine de dimension r ($r \geq 1$), et pour f un polynôme de degré d en r variables, à coefficients dans k . Les sommes S_n correspondantes s'écrivent :

$$(6.1) \quad S_n = \sum_{x_i \in k_n} \psi_{k_n}(f(x_1, \dots, x_r)) \quad , \quad \text{cf. (1.7).}$$

THÉOREME 6.2 - Supposons que le degré d de f ne soit pas divisible par p , et que la composante homogène f_d de f de degré d soit non singulière. Le couple (X, f) est alors purement de poids r , avec pour nombre de Betti $B = (d-1)^r$.

(On dit que f_d est non singulière si son discriminant est $\neq 0$, i.e. si l'hy-persurface de l'espace projectif P_{r-1} définie par f_d est lisse.)

Le th. (6.2) est dû à Deligne ([6], 8.4 à 8.13). Il entraîne :

COROLLAIRE 6.3 - Sous les hypothèses de (6.2), on a

$$(6.4) \quad |S_n| \leq (d-1)^r q^{nr/2} .$$

On sait peu de choses en dehors du cas (6.2). Dans [8], Deligne déduit des majorations de Weil le résultat suivant :

THÉOREME 6.5 - Si f n'est pas de la forme $\varphi^p - \varphi + c$, avec $c \in k$ et

$$\varphi \in k[X_1, \dots, X_r] ,$$

on a

$$|S_n| \leq (d-1) q^{n(r-1/2)} .$$

(Noter que l'on ne gagne qu'un exposant $1/2$ par rapport à la majoration tri-viale $|S_n| \leq q^{nr}$.)

Même lorsque $r = 2$, on ignore dans quel cas le couple (X, f) est purement de poids r . Dans [2], Bombieri et Davenport démontrent :

THÉOREME 6.6 - On suppose que $k = F_p$, $r = 2$, $d = 3$ et que le polynôme f ne se ramène pas à un polynôme en une variable par un changement linéaire de coordonnées. On a alors

$$S_n = \sum_{i=1}^{i=B} \pm (\omega_i)^n ,$$

avec $B \leq 14$, et $|\omega_i| \leq p$ pour tout i . En particulier :

$$(6.7) \quad |S_n| \leq 14 p^n \quad \text{pour tout } n .$$

(Dans une note de bas de page, les auteurs disent que la majoration $B \leq 14$ peut être remplacée par $B \leq 4$, i.e. par la majoration de (6.2).)

Il serait intéressant de traiter des cas plus généraux. L'une des difficultés est que l'on a peu de renseignements sur les groupes de cohomologie $H_c^i(\bar{X}; \mathbb{Z}_\ell)$

attachés au polynôme f . On ignore même si $\dim. H_C^i(\bar{X}; \mathcal{F}_\ell)$ a une borne ne dépendant que de d et de r (mais pas de k , ni de f). Dans cette direction, le seul résultat général connu semble être le suivant (démontré par voie p -adique par Bombieri [1]) : si l'on pose

$$(6.8) \quad \chi_C = \sum_i (-1)^i \dim. H_C^i(\bar{X}; \mathcal{F}_\ell) = v_{t=\infty}(L(t)) ,$$

on a

$$(6.9) \quad 0 \leq (-1)^r \chi_C \leq d^r .$$

Malheureusement, cette majoration ne permet pas de borner chacun des termes

$$\dim. H_C^i(\bar{X}; \mathcal{F}_\ell) .$$

Appendice - Sommes exponentielles incomplètes

Soit m un entier ≥ 1 , et soit φ une fonction de $x = (x_1, \dots, x_r)$, avec $x_i \in \mathbf{Z}$; on suppose φ périodique de période m , i.e. telle que

$$(A.1) \quad \varphi(x) = \varphi(y) \quad \text{si } x_i \equiv y_i \pmod{m} \text{ pour tout } i .$$

Soient $a = (a_1, \dots, a_r)$ et $b = (b_1, \dots, b_r)$ deux familles d'entiers telles que $a_i < b_i$ pour tout i . Posons

$$(A.2) \quad S_{a,b}\varphi = \sum_{a_i \leq x_i < b_i} \varphi(x_1, \dots, x_r) .$$

Une telle somme est dite "incomplète" (par opposition aux sommes "complètes", où la sommation porte sur un système de représentants des $x_i \pmod{m}$, par exemple $0 \leq x_i < m$). Il existe une méthode standard (cf. [11], n° 14) qui permet de ramener la majoration des sommes incomplètes à celle des sommes complètes. Rappelons comment on procède :

Si $\lambda = (\lambda_1, \dots, \lambda_r)$ est un élément de $\mathbf{Z}/m\mathbf{Z} \times \dots \times \mathbf{Z}/m\mathbf{Z}$, posons

$$(A.3) \quad \psi_\lambda(x) = e_m(\sum \lambda_i x_i)$$

et

$$(A.4) \quad S_\lambda \varphi = \sum_{x \pmod{m}} \psi_\lambda(x) \varphi(x) .$$

Les sommes $S_\lambda \varphi$ sont des sommes "complètes" au sens ci-dessus.

THÉOREME A.5 - Soit $M = \sup_{\lambda} |S_{\lambda}\varphi|$, et supposons que $b_i - a_i \leq m$ pour tout i .

On a alors

$$(A.6) \quad |S_{a,b}\varphi| \leq M(1 + \log m)^r.$$

(Lorsqu'on ne suppose pas que $b_i - a_i \leq m$ pour tout i , l'inégalité (A.6) reste vraie à condition de remplacer $1 + \log m$ par $\log m + \sup_i (b_i - a_i)/m$.)

Démonstration de (A.6)

Puisque φ est périodique de période m , on peut l'écrire comme combinaison linéaire des ψ_{λ} :

$$(A.7) \quad \varphi = \sum_{\lambda} c_{\lambda} \psi_{\lambda}$$

avec

$$(A.8) \quad c_{\lambda} = m^{-r} \sum_{x \pmod{m}} \psi_{\lambda}(-x)\varphi(x) = m^{-r} S_{-\lambda}\varphi.$$

On a donc $|c_{\lambda}| \leq m^{-r}M$ pour tout λ , et l'on en déduit:

$$(A.9) \quad |S_{a,b}\varphi| = \left| \sum_{\lambda} c_{\lambda} S_{a,b}\psi_{\lambda} \right| \leq m^{-r}M \sum_{\lambda} |S_{a,b}\psi_{\lambda}|.$$

On est donc ramené à montrer que

$$(A.10) \quad \sum_{\lambda} |S_{a,b}\psi_{\lambda}| \leq \prod_{i=1}^{i=r} (b_i - a_i + m \log m).$$

Comme $S_{a,b}\psi_{\lambda}$ est le produit des sommes à une variable

$$\sum_{a_i \leq x_i < b_i} e_m(\lambda_i x_i),$$

on voit que (A.10) équivaut à:

LEMME A.11 -
$$\sum_{\lambda=0}^{m-1} \left| \sum_{a \leq x < b} e_m(\lambda x) \right| \leq b - a + m \log m.$$

Le terme $\lambda = 0$ donne $b - a$. Il reste donc à prouver que

$$(A.12) \quad \sum_{\lambda=1}^{m-1} \left| \sum_{a \leq x < b} e_m(\lambda x) \right| \leq m \log m.$$

Posons $z_{\lambda} = e_m(\lambda) = \exp(2\pi i \lambda/m)$, $1 \leq \lambda \leq m-1$. On a

$$(A.13) \quad \sum_{a \leq x < b} e_m(\lambda x) = z_\lambda^a + z_\lambda^{a+1} + \dots + z_\lambda^{b-1} \\ = z_\lambda^a (1 - z_\lambda^{b-a}) / (1 - z_\lambda) .$$

Comme $|1 - z_\lambda| = 2 \sin(\pi\lambda/m)$, on en déduit :

$$\sum_{\lambda=1}^{m-1} \left| \sum_{a \leq x < b} e_m(\lambda x) \right| \leq \sum_{\lambda=1}^{m-1} 1/\sin(\pi\lambda/m) .$$

Tenant compte de l'inégalité $\sin(\pi x) \geq 2x$ (valable pour $0 \leq x \leq 1/2$), on obtient :

$$(A.14) \quad \sum_{\lambda=1}^{m-1} \left| \sum_{a \leq x < b} e_m(\lambda x) \right| \leq m \left(\sum_{1 \leq \lambda < \frac{m}{2}} 1/\lambda + \epsilon_m \right) ,$$

où $\epsilon_m = 0$ si m est impair, et $\epsilon_m = 1/m$ si m est pair. L'inégalité cherchée résulte alors de la majoration élémentaire :

$$(A.15) \quad \sum_{1 \leq \lambda < \frac{m}{2}} 1/\lambda + \epsilon_m < \log m .$$

Application

On prend maintenant $m = p$.

THÉORÈME A.16 - Soit $f(x) = f(x_1, \dots, x_r)$ un polynôme de degré $d \geq 2$, en r variables, à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. On suppose que d n'est pas divisible par p , et que la composante homogène de degré d de f est non singulière, cf. (6.2).

Si $b_i - a_i \leq p$ pour tout i , on a

$$\left| \sum_{a_i \leq x_i < b_i} e_p(f(x_1, \dots, x_r)) \right| \leq (d-1)^r (1 + \log p)^r p^{r/2} .$$

Posons $\varphi(x) = e_p(f(x))$. On a, pour tout $\lambda \in (\mathbb{Z}/p\mathbb{Z})^r$,

$$S_\lambda \varphi = \sum_{x \pmod{p}} e_p(f(x) + \lambda_1 x_1 + \dots + \lambda_r x_r) ,$$

et le terme de degré d du polynôme $f(x) + \lambda_1 x_1 + \dots + \lambda_r x_r$ est le même que celui de $f(x)$. On peut donc appliquer (6.4) à ce polynôme, ce qui donne

$$|S_\lambda \varphi| \leq (d-1)^r p^{r/2} \text{ pour tout } \lambda ,$$

et (A.16) résulte de (A.6), puisque $M \leq (d-1)^r p^{r/2}$.

Remarque - On notera que, pour d fixé, on obtient une majoration en $O(p^{r/2 + \epsilon})$, pour tout $\epsilon > 0$, majoration qui est presque aussi bonne que celle de la somme "complète".

Bibliographie

- [1] E. BOMBIERI - On exponential sums in finite fields, Amer. J. of Math., 88 (1966), p. 71-105.
- [2] E. BOMBIERI et H. DAVENPORT - On two problems of Mordell, Amer. J. of Math., 88 (1966), p. 61-70.
- [3] L. CARLITZ - A note on multiple exponential sums, Pacific J. of Math., 15 (1965), p. 757-765.
- [4] L. CARLITZ - Kloosterman sums and finite field extensions, Acta Arith., 16 (1969/70), p. 179-193.
- [5] H. DAVENPORT et H. HASSE - Die Nullstellen der Kongruenzzetafunktionen im gewissen zyklischen Fällen, Journ. Crelle, 172 (1935), p. 151-182.
- [6] P. DELIGNE - La conjecture de Weil I, Publ. Math. IHES, 43 (1974), p. 273-307.
- [7] P. DELIGNE - La conjecture de Weil II, en préparation.
- [8] P. DELIGNE - Applications de la formule des traces aux sommes trigonométriques, à paraître dans SGA 4 $\frac{1}{2}$.
- [9] B. DWORK - On the zeta function of a hypersurface, Publ. Math. IHES, 12 (1962), p. 5-68.
- [10] A. GROTHENDIECK - Formule de Lefschetz et rationalité des fonctions L, Sémin. Bourbaki, exposé 279 (1964) (reproduit dans "Dix exposés sur la cohomologie des schémas", North-Holland, 1968).
- [11] L-K. HUA - Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie, Enz. der Math. Wiss., Zweite Aufl., Band I 2, Heft 13, Teil I, Teubner, Leipzig, 1959.
- [12] H.D. KLOOSTERMAN - Asymptotische Formeln für die Fourierkoeffizienten ganzer Modulformen, Abh. Math. Sem. Hamburg, 5 (1927), p. 338-352.
- [13] D.H. LEHMER et E. LEHMER - The cyclotomy of Kloosterman sums, Acta Arith., 12 (1966/67), p. 385-407.

- [14] D.H. LEHMER et E. LEHMER - The cyclotomy of hyper-Kloosterman sums, Acta Arith., 14 (1968), p. 89-111.
- [15] J. LEVEQUE (edit.) - Reviews in Number Theory, 6 vol., Amer. Math. Soc., 1974.
- [16] L.J. MORDELL - Some exponential sums, Proc. Steklov Inst. Math., 132 (1973), p. 29-34.
- [17] S. SPERBER - p-adic hypergeometric functions and their cohomology, Thèse, Univ. Pennsylvania, 1975.
- [18] A. WEIL - On some exponential sums, Proc. Nat. Acad. Sci. USA, 34 (1948), p. 204-207.
- [19] A. WEIL - Number of solutions of equations in finite fields, Bull. Amer. Math. Soc., 55 (1949), p. 497-508.
- [20] A. WEIL - Examples of L functions, App. V to "Basic Number Theory", 3rd edit., Springer, 1974.

Jean-Pierre SERRE
Collège de France
75231 PARIS CEDEX 05