

# Vérification de l'hypothèse $H_p(\chi)$ pour $p$ grand

E. Kowalski, Princeton University  
P. Michel, Université de Montpellier

Dans le texte qui précède, Merel a introduit l'hypothèse  $H_p(\chi)$ , pour  $p$  premier et  $\chi$  un caractère de Dirichlet primitif modulo  $p$ . Il s'agit d'un problème de non-annulation pour certaines fonctions  $L$  automorphes. Il a également fourni l'assertion élémentaire suivante qui est équivalente à  $H_p(\chi)$ :  
*Il existe  $u$  modulo  $p$ ,  $u \neq 0$ , tel que*

$$\sum_{\substack{x=-\bar{u} \\ x=u}} (\chi(x) - \chi(-1)\bar{\chi}(x)) \neq 0.$$

La somme est prise entre des représentants entiers quelconques de  $u$  et de  $-\bar{u}$ , où  $\bar{u}$  est l'inverse de  $u$  modulo  $p$ .

On voit que si  $\chi$  est quadratique et pair, l'expression en question est identiquement nulle. Nous montrons ici que réciproquement, si  $\chi$  n'est pas quadratique pair, et  $p$  assez grand ( $p > B$ , pour une constante absolue et effective  $B$ ), cette assertion est vraie, et donc  $H_p(\chi)$  l'est également. Dans la note [KM] nous établissons directement le théorème de non-annulation (sous une forme plus forte) et étudions le cas restant de  $\chi$  quadratique pair (c'est à dire la valeur centrale de la dérivée des fonctions  $L$  correspondantes).

## 1 Préliminaires

Dans tout ce qui suit,  $p$  est un nombre premier fixé et  $\chi \neq 1$  est un caractère modulo  $p$  également fixé. On étend comme d'habitude  $\chi$  à  $\mathbf{Z}/p\mathbf{Z}$  (et  $\mathbf{Z}$ ) en posant  $\chi(0) = 0$ .

La somme de Gauss associée à  $\chi$  est

$$\tau(\chi) = \sum_{a \bmod p} \chi(a) e\left(\frac{a}{p}\right) \tag{1}$$

et on a  $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p$ . On note  $W(\chi)$  le "signe" de la somme de Gauss, c'est à dire le nombre complexe de module 1 défini par  $W(\chi) = \tau(\chi)/\sqrt{p}$ . On a  $W(\chi)W(\bar{\chi}) = \chi(-1)$ ,  $W(\chi)^2W(\bar{\chi})^2 = 1$ . De plus, pour tout  $x$  modulo  $p$  on a

$$\chi(x) = \frac{1}{\tau(\bar{\chi})} \sum_{a \bmod p} \bar{\chi}(a) e\left(\frac{ax}{p}\right). \tag{2}$$

**Lemme 1.** *Le caractère  $\chi$  vérifie  $W(\chi)^2 = 1$  si et seulement si  $\chi$  est quadratique et pair.*

*Preuve.* En effet, soit  $\sigma_\alpha$ , pour  $\alpha \in (\mathbf{Z}/p\mathbf{Z})^\times$ , l'automorphisme du corps cyclotomique  $\mathbf{Q}(\mu_{p(p-1)})$  donné par  $e(1/p) \mapsto e(\alpha/p)$  et fixant  $e(1/(p-1))$ . La somme de Gauss, donc aussi  $W(\chi)^2$ , sont dans ce corps et on a

$$\sigma_\alpha(W(\chi)^2) = \frac{\sigma_\alpha(\tau(\chi)^2)}{p} = \bar{\chi}(\alpha)^2 W(\chi)^2$$

donc pour avoir  $W(\chi)^2 = 1$ , il faut que  $\chi(\alpha)^2 = 1$  pour tout  $\alpha \in \mathbf{Z}/p\mathbf{Z}$ ,  $\alpha \neq 0$ . Cela signifie que  $\chi$  is quadratique. Mais alors  $W(\chi)^2 = W(\chi)W(\bar{\chi}) = \chi(-1)$ , donc  $W(\chi)^2 = 1$  requiert aussi que  $\chi$  soit pair. La réciproque est évidente.  $\square$

## 2 Réductions

On pose

$$b_\chi(a) = \bar{\chi}(a) - W(\bar{\chi})^2 \chi(a)$$

pour  $a \in \mathbf{Z}/p\mathbf{Z}$ , et

$$F(\chi, u) = \sum_{x=u}^{x=-\bar{u}} (\chi(x) - \chi(-1)\bar{\chi}(x))$$

pour  $u \in \mathbf{Z}/p\mathbf{Z}$ ,  $u \neq 0$ . Le problème à résoudre est de montrer que si  $F(\chi, \cdot)$  est identiquement nulle, alors  $\chi$  est quadratique et pair.

**Lemme 2.** *On a pour tout  $u \neq 0$*

$$F(\chi, u) = \frac{1}{\tau(\bar{\chi})} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} \left( e\left(\frac{au}{p}\right) - e\left(\frac{a(1-\bar{u})}{p}\right) \right).$$

*Preuve.* Soit

$$f(\chi, u) = \sum_{x=u}^{x=-\bar{u}} \chi(x);$$

on a  $F(\chi, u) = f(\chi, u) - \chi(-1)f(\bar{\chi}, u)$ .

On utilise (2) pour écrire  $\chi(x)$  en terme de caractères additifs. Choisissons le représentant  $u_1$  de  $u$  tel que  $0 < u_1 < p$ , et un représentant  $u_2 > u_1$  de  $-\bar{u}$ . Alors, (2) donne

$$f(\chi, u) = \frac{1}{\tau(\bar{\chi})} \sum_{a \neq 0} \bar{\chi}(a) \sum_{x=u_1}^{x=u_2} e\left(\frac{ax}{p}\right)$$

et la somme intérieure est une progression géométrique,

$$\sum_{x=u_1}^{x=u_2} e\left(\frac{ax}{p}\right) = e\left(\frac{au_1}{p}\right) \frac{1 - e\left(\frac{(u_2 - u_1 + 1)a}{p}\right)}{1 - e\left(\frac{a}{p}\right)}$$

d'où, réduisant  $u_1$  et  $u_2$  modulo  $p$  de nouveau

$$f(\chi, u) = \frac{1}{\tau(\bar{\chi})} \sum_{a \neq 0} \frac{\bar{\chi}(a)}{1 - e\left(\frac{a}{p}\right)} \left( e\left(\frac{au}{p}\right) - e\left(\frac{a(1-\bar{u})}{p}\right) \right). \quad (3)$$

Appliqué à  $\bar{\chi}$  au lieu de  $\chi$ , cela donne

$$\chi(-1)f(\bar{\chi}, u) = \frac{\chi(-1)}{\tau(\chi)} \sum_{a \neq 0} \frac{\chi(a)}{1 - e\left(\frac{a}{p}\right)} \left( e\left(\frac{au}{p}\right) - e\left(\frac{a(1-\bar{u})}{p}\right) \right). \quad (4)$$

Puisque  $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p$ ,

$$\frac{\chi(-1)}{\tau(\chi)} = \frac{\tau(\bar{\chi})}{p} = \frac{1}{\tau(\bar{\chi})} \frac{\tau(\bar{\chi})^2}{p} = \frac{1}{\tau(\bar{\chi})} W(\bar{\chi})^2$$

donc le lemme découle des deux formules (3) et (4) pour  $f(\chi, u)$  et  $f(\bar{\chi}, u)$ .  $\square$

Définissons

$$G(u) = \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} e\left(\frac{au}{p}\right) \quad (5)$$

$$H(u) = \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} e\left(\frac{a}{p}\right) e\left(\frac{-au}{p}\right). \quad (6)$$

Le lemme s'écrit donc

$$F(\chi, u) = G(u) - H(\bar{u}). \quad (7)$$

On va maintenant appliquer l'analyse de Fourier sur le groupe multiplicatif  $(\mathbf{Z}/p\mathbf{Z})^\times$ , considérant l'identité hypothétique  $F(\chi, \cdot) = 0$  comme une relation de "modularité" entre  $G$  et  $H$  que l'on analyse par "transformation de Mellin". Ce n'est que l'un de plusieurs choix possibles ici, d'autres solutions sont sans doute possibles.

Soit  $X$  le groupe des caractères multiplicatifs de  $\mathbf{Z}/p\mathbf{Z}$ . On définit la transformée  $\hat{f}$  d'une fonction  $f$  définie sur  $(\mathbf{Z}/p\mathbf{Z})^\times$

$$\hat{f}(\psi) = \sum_{u \neq 0} f(u)\psi(u). \quad (8)$$

Par (7), on a

$$\hat{F}(\chi, \psi) = \hat{G}(\psi) - \hat{H}(\bar{\psi}). \quad (9)$$

**Lemme 3.** *On a*

$$\hat{G}(\psi) = \tau(\psi) \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} \bar{\psi}(a) \quad (10)$$

$$\hat{H}(\psi) = \psi(-1)\tau(\psi) \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} e\left(\frac{a}{p}\right) \bar{\psi}(a). \quad (11)$$

*Preuve.* Cela découle immédiatement des définitions et de (2).  $\square$

L'équation (9) peut s'écrire

$$\hat{F}(\chi, \psi) = \tau(\psi) \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} \bar{\psi}(a) - \frac{p}{\tau(\psi)} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} e\left(\frac{a}{p}\right) \psi(a)$$

ou bien

$$\frac{\tau(\psi)}{p} \hat{F}(\chi, \psi) = \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} W(\psi)^2 \bar{\psi}(a) - \sum_{a \neq 0} \frac{b_\chi(\bar{a})}{1 - e\left(\frac{\bar{a}}{p}\right)} e\left(\frac{\bar{a}}{p}\right) \bar{\psi}(a). \quad (12)$$

**Lemme 4.** Soit  $f$  une fonction sur  $X$  de la forme

$$f(\psi) = \sum_{a \neq 0} c(a) W(\psi)^2 \bar{\psi}(a)$$

pour des nombres complexes  $c(a)$ . Alors pour tout  $b$  modulo  $p$ ,  $b \neq 0$ , on a

$$\frac{1}{p-1} \sum_{\psi \in X} \bar{\psi}(b) f(\psi) = \frac{1}{p} \sum_{a \neq 0} c(a) S(a, b; p)$$

où

$$S(a, b; p) = \sum_{x \neq 0} e\left(\frac{ax + b\bar{x}}{p}\right)$$

est la somme de Kloosterman.

*Preuve.* Il suffit d'appliquer le lemme suivant, bien connu, et d'inverser l'ordre de sommation.  $\square$

**Lemme 5.** Pour tout  $x$  modulo  $p$ ,  $x \neq 0$ , on a

$$\sum_{\psi \in X} W(\psi)^2 \bar{\psi}(x) = \frac{p-1}{p} S(1, x; p).$$

*Preuve.* On calcule, en développant le carré de la somme de Gauss:

$$\begin{aligned} \sum_{\psi \in X} W(\psi)^2 \bar{\psi}(x) &= \frac{1}{p} \sum_{\psi} \bar{\psi}(x) \sum_{y, z} \psi(y) \psi(z) e\left(\frac{y+z}{p}\right) \\ &= \frac{1}{p} \sum_{y, z} e\left(\frac{y+z}{p}\right) \sum_{\psi} \psi(\bar{x}yz) \\ &= \frac{p-1}{p} \sum_{yz=x} e\left(\frac{y+z}{p}\right) = \frac{p-1}{p} S(1, x, p). \end{aligned}$$

$\square$

Soit  $\hat{F}_1(\chi, \psi)$  le membre de gauche de (12). On calcule

$$\frac{1}{p-1} \sum_{\psi \in X} \psi(\bar{b}) \hat{F}_1(\chi, \psi)$$

et on obtient par le lemme et par orthogonalité des caractères, pour tout  $b \neq 0$

$$\frac{1}{p-1} \sum_{\psi \in X} \psi(\bar{b}) \hat{F}_1(\chi, \psi) = \frac{1}{p} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} S(a, b; p) - \frac{b_\chi(b)}{1 - e\left(\frac{b}{p}\right)} e\left(\frac{b}{p}\right). \quad (13)$$

### 3 Fin de la preuve

On peut maintenant prouver la

**Proposition 1.** *Il existe une constante absolue  $P$  tel que si  $p > P$ , et  $\chi$  n'est pas quadratique pair, alors  $F(\chi, \cdot)$  n'est pas identiquement nulle.*

**Lemme 6.** *On a pour  $0 \leq x \leq \pi$*

$$\sqrt{\frac{2}{5}}(2\pi x) \leq |1 - e(x)| \leq 2\pi x.$$

**Lemme 7.** *Pour tout  $a \neq 0$ , on a*

$$\frac{1}{p} \left| \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} S(a, b; p) \right| \leq \frac{2\sqrt{10}}{\pi} \sqrt{p} \log(2(p-1)) \leq 2.02\sqrt{p} \log(2(p-1)).$$

*Preuve.* On a  $|b_\chi(a)| \leq 2$ , et de plus l'estimation de Weil pour les sommes de Kloosterman, pour tout  $ab \neq 0$

$$S(a, b; p) \leq 2\sqrt{p}$$

donc

$$\begin{aligned} \frac{1}{p} \left| \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} S(a, b; p) \right| &\leq \frac{4}{\sqrt{p}} \sum_{a \neq 0} \frac{1}{\left|1 - e\left(\frac{a}{p}\right)\right|} = \frac{8}{\sqrt{p}} \sum_{0 < a \leq \frac{p-1}{2}} \frac{1}{\left|1 - e\left(\frac{a}{p}\right)\right|} \\ &\leq \frac{2\sqrt{10}}{\pi} \sqrt{p} \sum_{0 < a \leq \frac{p-1}{2}} \frac{1}{a} \quad (\text{par le Lemme 6}) \\ &\leq \frac{2\sqrt{10}}{\pi} \sqrt{p} \log(2(p-1)). \end{aligned}$$

□

**Lemme 8.** *Supposons que  $\chi$  n'est pas quadratique. Soit  $\varepsilon > 0$  un réel fixé,  $A = p^{1/4+\varepsilon}$ . Alors*

$$\sum_{1 \leq a \leq A} |b_\chi(a)|^2 = 2A + O(A^{1-\delta})$$

pour un  $\delta = \delta(\varepsilon) > 0$ .

*Preuve.* Soit  $w = W(\chi)$ . On a

$$\begin{aligned} \sum_{a \leq A} |b_\chi(a)|^2 &= \sum_{a \leq A} (2 - w^2 \chi(a)^2 - \bar{w}^2 \bar{\chi}(a)^2) \\ &= 2A - w^2 \sum_{a \leq A} \chi(a)^2 - \bar{w}^2 \sum_{a \leq A} \bar{\chi}(a)^2 \end{aligned}$$

Comme  $\chi$  n'est pas quadratique,  $\chi^2$  est un caractère non-trivial. D'après Burgess [Bur], [FI], on a alors

$$\sum_{a \leq A} \chi(a)^2 \ll A^{1-\delta}, \quad \sum_{a \leq A} \bar{\chi}(a)^2 \ll A^{1-\delta}$$

pour un certain  $\delta = \delta(\varepsilon) > 0$ ; c'est là que l'hypothèse  $A = p^{1/4+\varepsilon}$  avec  $\varepsilon > 0$  intervient. □

Notons que si l'on admet l'hypothèse de Riemann pour les fonctions  $L$  de caractères de Dirichlet, on peut raffiner considérablement cette inégalité.

*Preuve de la proposition.* Soit  $\chi$  un caractère tel que  $F(\chi, \cdot) = 0$ . Alors, d'après (13), on a pour tout  $b \neq 0$  l'égalité

$$\frac{b_\chi(b)}{1 - e\left(\frac{b}{p}\right)} e\left(\frac{b}{p}\right) = \frac{1}{p} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} S(a, b; p). \quad (14)$$

L'idée est qu'une telle identité n'est pas possible car les deux membres ne sont pas du même ordre de grandeur. Le membre de droite, d'après le Lemme 8, est borné par

$$\frac{1}{p} \left| \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e\left(\frac{a}{p}\right)} S(a, b; p) \right| \leq 2.02\sqrt{p} \log(2(p-1)). \quad (15)$$

Par contre, si on prend simplement  $b = 1$  dans le membre de gauche, on a par le Lemme 6

$$\left| \frac{1 - W(\bar{\chi})^2}{1 - e\left(\frac{1}{p}\right)} e\left(\frac{1}{p}\right) \right| \geq \frac{p|1 - W(\bar{\chi})^2|}{2\pi}. \quad (16)$$

La difficulté est que  $W(\bar{\chi})^2$  pourrait être très proche de 1, de sorte que comparer (15) et (16) n'implique pas aussitôt une contradiction.

En particulier, bien entendu, si  $\chi$  est quadratique pair,  $W(\bar{\chi})^2 = 1$  et le membre de gauche est toujours nul, ainsi que celui de droite. Si  $\chi$  est quadratique impair,  $W(\bar{\chi})^2 = -1$  donc on obtient en comparant

$$\frac{p}{\pi} \leq 2.02\sqrt{p} \log(2(p-1))$$

qui est impossible dès que  $p \geq 3067$ .

Si  $\chi$  n'est pas quadratique, on peut encore appliquer le Lemme 8: celui implique que, si l'on fixe  $\varepsilon > 0$  quelconque, alors si  $p > P$  il existe  $b \leq A = p^{1/4+\varepsilon}$  tel que  $|b_\chi(b)| \geq \sqrt{2}$ . Procédant comme ci-dessus avec ce  $b$  dans (14) on trouve que cette égalité impliquerait

$$\frac{\sqrt{2}}{2\pi} p^{3/4-\varepsilon} \leq \frac{p|b_\chi(b)|}{2\pi b} \leq \left| \frac{b_\chi(b)}{1 - e\left(\frac{b}{p}\right)} e\left(\frac{b}{p}\right) \right| \leq 2.02\sqrt{p} \log(2(p-1)). \quad (17)$$

Cela est impossible pour  $p$  assez grand si  $\varepsilon$  a été choisi  $< 1/4$ . □

**Remarques.** Pour obtenir une constante explicite  $B$  telle que  $p > B$  est suffisant pour la validité de cet argument, il suffit d'avoir une forme explicite du lemme 8, ce qui revient à avoir une forme explicite de l'estimation de Burgess (ou, en fait, de n'importe quelle estimation de sommes de caractères

$$S(\chi, A) = \sum_{a \leq A} \chi(a)$$

meilleure que l'inégalité de Polya-Vinogradov

$$|S(\chi, A)| \leq 4\sqrt{p} \log(p)$$

car il faut trouver  $b < \sqrt{p}(\log p)^{-1}$  tel que  $b_\chi(b)$  ne soit pas trop petit.) Malheureusement, il ne semble pas que des constantes possibles aient été explicitées.

De plus, dans l'inégalité de Burgess, le  $\delta(\varepsilon)$  est en général très petit, d'autant plus que  $\varepsilon$  est petit; par exemple, pour  $\varepsilon = \frac{1}{16}$ , donc  $1/4 + \varepsilon = 5/16$ , on a  $\delta = 1/256$ . Cela signifie que si la constante implicite est mauvaise dans l'inégalité de Burgess, on aura le lemme seulement pour  $p$  très grand.

## Bibliographie

- [Bur] Burgess, D. A.: On character sums and  $L$ -series, II, Proc. London Math. Soc. (1963), 524–536.
- [FI] Friedlander, J. et Iwaniec, H.: A mean-value theorem for character sums, Michigan Math. J. 39 (1992), no. 1, 153–159.
- [KM] Kowalski, E. et Michel, P.: Un théorème de non-annulation et un autre théorème de non-annulation, préprint (1999).