Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

CRIBLE ASYMPTOTIQUE ET SOMMES DE KLOOSTERMAN

Jimena Sivak-Fischler

Tome 137
Fascicule 1

2009

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 1-62

Bull. Soc. math. France
137 (1), 2009, p. 1–62

CRIBLE ASYMPTOTIQUE ET SOMMES DE KLOOSTERMAN

PAR JIMENA SIVAK-FISCHLER

RÉSUMÉ. — On montre à l'aide de méthodes de crible, de méthodes issues de la théorie des formes automorphes et de géométrie algébrique ainsi qu'à l'aide de la loi de Sato-Tate verticale que le signe des sommes de Kloosterman $\mathrm{Kl}(1,1;n)$ change une infinité de fois pour n parcourant les entiers sans facteur carré ayant au plus 18 facteurs premiers. Ceci améliore un résultat précédent de Fouvry et Michel qui avaient obtenu 23 à la place de 18.

ABSTRACT (*Asymptotic sieve and Kloosterman sums*). — We prove using sieve methods, methods coming from automorphic form theory and algebraic geometry, and Sato-Tate vertical law that the sign of Kloosterman sums $\mathrm{Kl}(1,1;n)$ changes infinitely often as n runs through the square-free integers with at most 18 prime factors. This improves on a previous result of Fouvry and Michel, who had obtained 23 instead of 18.

Texte reçu le 4 juillet 2006, révisé le 30 juin 2008, accepté le 12 septembre 2008

JIMENA SIVAK-FISCHLER, Équipe d'Arithmétique et de Géométrie Algébrique, Bâtiment 425, Université Paris-Sud, 91405 Orsay Cedex, France • *E-mail :* `Jimena.Sivak@math.u-psud.fr` • *Url :* `http://www.math.u-psud.fr/~sivak/`

Classification mathématique par sujets (2000). — 11N36 ; 11L05.

Mots clefs. — Crible asymptotique de Bombieri, sommes de Kloosterman, conjecture de Sato-Tate.

© Société Mathématique de France

1. Introduction

On définit la somme de Kloosterman $\mathrm{Kl}(a,b;n)$, pour $a,b,n \geq 1$ entiers, par la formule

$$\mathrm{Kl}(a,b;n) := \sum_{\substack{x \bmod n \\ (x,n)=1}} \exp\Big(2i\pi \frac{ax+b\overline{x}}{n}\Big)$$

où (x,n) est le pgcd de x et n, et $\overline{x}$ l'inverse de x modulo n. Ce sont des nombres réels, non nuls pour $n=p$ premier.

Ces sommes exponentielles s'avèrent d'une importance cruciale en théorie analytique des nombres mais leurs propriétés demeurent mystérieuses. Par exemple, la célèbre estimation $|\mathrm{Kl}(1,1;p)| \leq 2\sqrt{p}$ de A. Weil [10] permet d'écrire $|\mathrm{Kl}(1,1;p)| = 2\sqrt{p}\cos\theta_p$ où $\theta_p \in [0,\pi]$ pour p premier. On peut se demander comment varie θ_p, qui mesure les oscillations des sommes de Kloosterman en amplitude et en signe autour de la taille maximale. Katz a proposé la conjecture suivante (cf. [5] p.493) :

Conjecture 1.1 (Loi de Sato-Tate horizontale). — *Pour $p \to +\infty$, l'ensemble des angles θ_p est équiréparti sur $[0,\pi]$ suivant la mesure μ_{ST} de Sato-Tate définie sur $[0,\pi]$ par $\frac{2}{\pi}\sin^2\theta \mathrm{d}\theta$, i.e. pour tous $0 \leq \alpha < \beta \leq \pi$, on a pour $X \to +\infty$*

$$\frac{|\{X \leq p \leq 2X | \alpha \leq \theta_p \leq \beta\}|}{|\{X \leq p \leq 2X\}|} \longrightarrow \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \mathrm{d}\theta.$$

Cette conjecture reste complètement ouverte. A l'heure actuelle, on ne peut exclure que $\mathrm{Kl}(1,1;p) > 0$ pour tout p premier assez grand, ou que $|\mathrm{Kl}(1,1;p)| < p^c$ avec $c < 1/2$ pour tout p premier assez grand...

Dans cette direction, un résultat de Kuznietsov montre qu'il existe de nombreuses compensations entre les sommes de Kloosterman $\mathrm{Kl}(1,1;n)$ (cf. [6] théorème 3) :

Theorème 1.2. — *Si g est une fonction $C^\infty(\mathbb{R},\mathbb{R})$ à support inclus dans $[1,2]$, on a*

$$\sum_n g\Big(\frac{n}{X}\Big)\mathrm{Kl}^*(1,1;n) = o_g(X),$$

où $\mathrm{Kl}^*(1,1;n) := \frac{\mathrm{Kl}(1,1;n)}{\sqrt{n}}$.

On voudrait obtenir des résultats de changement de signe de $\mathrm{Kl}(1,1;n)$ sous certaines conditions multiplicatives sur n, par exemple pour n presque premier (i.e. ayant peu de facteurs premiers). Fouvry et Michel ont montré le résultat suivant à l'aide du crible asymptotique [2] :

Theorème 1.3. — *Il existe $X_0 > 0$ et $c_0 > 0$ tels que pour $X \geq X_0$, on ait les minorations*

$$|\{n \in [X, 2X] |\ \mathrm{Kl}^*(1,1;n) > 0,\ \mu^2(n) = 1, \omega(n) \leq 23\}| \geq c_0 \frac{X}{\log X}$$

et

$$|\{n \in [X, 2X] |\ \mathrm{Kl}^*(1,1;n) < 0,\ \mu^2(n) = 1, \omega(n) \leq 23\}| \geq c_0 \frac{X}{\log X},$$

où $\omega(n)$ désigne le nombre de facteurs premiers distincts de n.

Ceci démontre qu'une infinité d'entiers n (sans facteur carré avec au plus 23 facteurs premiers) sont tels que $\mathrm{Kl}(1,1;n) > 0$ (respectivement $\mathrm{Kl}(1,1;n) < 0$). Il y a donc une infinité de changements de signe des sommes de Kloosterman sur l'ensemble des n sans facteur carré ayant au plus 23 facteurs premiers.

Le résultat principal de cet article est

Theorème 1.4. — *Il existe $X_0 > 0$ et $c_0 > 0$ tels que pour $X \geq X_0$, on ait les minorations*

$$|\{n \in [X, 2X] |\ \mathrm{Kl}^*(1,1;n) > 0,\ \mu^2(n) = 1, \omega(n) \leq 18\}| \geq c_0 \frac{X}{\log X}$$

et

$$|\{n \in [X, 2X] |\ \mathrm{Kl}^*(1,1;n) < 0,\ \mu^2(n) = 1, \omega(n) \leq 18\}| \geq c_0 \frac{X}{\log X}.$$

Pour démontrer ce résultat, on utilise le crible asymptotique (introduit par Fouvry et Michel dans [2]), des résultats issus de la théorie des formes automorphes et de géométrie algébrique, comme dans [2], mais on introduit aussi la loi de Sato-Tate verticale dans la preuve, au lieu de majorer trivialement $\mathrm{Kl}^*(1,1;n)$.

On désigne par $H(\theta)$ pour $0 < \theta \leq 1$ la conjecture (voir [2])

Conjecture 1.5 ($H(\theta)$). — *Pour toute fonction $g \in C^\infty(\mathbb{R}, \mathbb{R})$ à support inclus dans $[1, 2]$, pour tout $\epsilon > 0$, tout $A \geq 0$ et tout $X \geq 2$, on a*

$$\sum_{d \leq X^{\theta - \epsilon}} \Big| \sum_{d|n} g\Big(\frac{n}{X}\Big) \mathrm{Kl}^*(1,1;n) \Big| = \mathrm{O}_{g,\epsilon,A}(X(\log X)^{-A}).$$

Il s'agit en fait d'un théorème pour $\theta \leq \frac{1}{2}$ (cf. [4], Proposition 2.4) issu de la théorie des formes automorphes, que l'on utilise dans la preuve des théorèmes 1.3 et 1.4.

Sous $H(1)$, Fouvry et Michel ont démontré (voir [2]) qu'on peut remplacer 23 par 3 dans le théorème 1.3. Il semble cependant que les méthodes introduites dans le présent texte ne suffisent pas à améliorer ce résultat.

Un résultat légèrement différent du théorème 1.4 a été démontré par l'auteur [8] :

Theorème 1.6. — *Il existe $X_0 > 0$ et $c_0 > 0$ tels que pour $X \geq X_0$ et pour $z = X^{\frac{1}{22.29}}$, on ait les minorations*

$$|\{n \in [X, 2X] |\ \mathrm{Kl}^*(1,1;n) > 0,\ p|n \Rightarrow p \geq z\}| \geq c_0 \frac{X}{\log X}$$

et

$$|\{n \in [X, 2X] |\ \mathrm{Kl}^*(1,1;n) < 0,\ p|n \Rightarrow p \geq z\}| \geq c_0 \frac{X}{\log X}.$$

Il s'agit d'une amélioration de [4] (Théorème 2) où 22.29 est remplacé par 23.9, mais qui contrairement aux théorèmes 1.3 et 1.4 donne le bon ordre de grandeur espéré. Pour montrer cela, on utilise un crible de Selberg modifié, le *crible étrange*.

Nous utiliserons les notations suivantes :

- p désigne dans la suite un nombre premier.
- $C_c^\infty([a,b])$ désigne l'ensemble des fonctions $\mathbb{R} \to \mathbb{R}$, indéfiniment dérivables, à support compact inclus dans $[a,b]$.
- g désigne une fonction positive appartenant à $C_c^\infty([1,2])$.
- La transformée de Mellin d'une fonction $f : \mathbb{R}_*^+ \to \mathbb{C}$, continue à support compact inclus dans $]0, +\infty[$, est définie pour tout $s \in \mathbb{C}$ par

$$\hat{f}(s) := \int_0^\infty f(t) t^{s-1} \mathrm{d}t$$

  et sa transformée de Mellin inverse est donnée, pour $\alpha > 0$ et $x \in \mathbb{R}_+^*$, par

$$f(x) = \int_{\Re x = \alpha} \hat{f}(s) x^{-s} \mathrm{d}s.$$

- Pour $n \geq 1$ et α, β réels, on désigne par $\mathfrak{B}(n, \alpha, \beta)$ le produit de n bandes du plan complexe

$$\mathfrak{B}(n, \alpha, \beta) := \{z = (z_1, \ldots, z_n) \in \mathbb{C}^n | \alpha \leq \Re z_i \leq \beta,\ i = 1, \ldots, n\}.$$

- On dit, pour $z \geq 2$ réel, que la suite réelle $(\lambda_d)_{d \geq 1}$ vérifie la condition $\mathrm{Sel}(z)$ (pour rappeler la construction des coefficients du crible de Selberg) si on a

$$\mathrm{Sel}(z) \quad \begin{cases} \lambda_1 = 1 \\ |\lambda_d| \leq 2 \times 2^{\omega(d)} \\ \lambda_d = 0 \text{ si } d > 2z \text{ ou } \mu(d) = 0. \end{cases}$$