Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

A NOTE ON SIGNS OF KLOOSTERMAN SUMS

Kaisa Matomäki

Tome 139
Fascicule 3

2011

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 287-295

Bull. Soc. math. France
139 (3), 2011, p. 287–295

A NOTE ON SIGNS OF KLOOSTERMAN SUMS

by Kaisa Matomäki

Abstract. — We prove that the sign of Kloosterman sums $\mathrm{Kl}(1,1;n)$ changes infinitely often as n runs through the square-free numbers with at most 15 prime factors. This improves on a previous result by Sivak-Fischler who obtained 18 instead of 15. Our improvement comes from introducing an elementary inequality which gives lower and upper bounds for the dot product of two sequences whose individual distributions are known.

Résumé (*Une note sur les signes des sommes de Kloosterman*). — On montre 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 15 facteurs premiers. Ceci améliore un résultat précédent de Sivak-Fischler qui avaient obtenu 18 à la place de 15. Notre amélioration provient de l'introduction d'une inégalité élémentaire donnant des bornes inférieures et supérieures pour le produit scalaire de deux suites dont les distributions propres sont connues.

Texte reçu le 16 décembre 2008, révisé le 20 novembre 2009, accepté le 15 décembre 2009.

Kaisa Matomäki, Department of Mathematics, University of Turku, 20014 Turku, Finland
• *E-mail :* ksmato@utu.fi

2000 Mathematics Subject Classification. — 11L05, 26D15.

Key words and phrases. — Kloosterman sums, rearrangement inequality, Sato-Tate conjecture.

The author was supported by the Finnish Cultural Foundation.

1. Introduction

The distribution of values of Kloosterman sums

$$\mathrm{Kl}(a,b;n) = \sum_{\substack{x \,(\mathrm{mod}\, n)\\ (x,n)=1}} e\left(\frac{ax+b\overline{x}}{n}\right)$$

is an important question in number theory. By the Estermann-Weil bound (see [1]) we have, for $32 \nmid n$,

$$|\,\mathrm{Kl}(a,b;n)| \leq 2^{\omega(n)}(a,b,n)^{1/2}n^{1/2}, \tag{1}$$

where $\omega(n)$ is the number of distinct prime divisors of n (for $32 \mid n$ the bound holds with an additional factor $\sqrt{2}$ on the right hand side). In particular

$$|\,\mathrm{Kl}(1,a;p)| \leq 2\sqrt{p}.$$

Since $\mathrm{Kl}(1,a;p)$ is real, this implies that there is an angle $\theta_{p,a} \in [0,\pi]$ such that

$$\cos\theta_{p,a} = \frac{\mathrm{Kl}(1,a;p)}{2\sqrt{p}}.$$

The distribution of the angles $\theta_{p,a}$ is related to the Sato-Tate measure μ_{ST} on $[0,\pi]$ defined by

$$d\mu_{ST} = \frac{2\sin^2\theta}{\pi}d\theta.$$

Indeed Katz has proved the following result concerning the vertical distribution (see [5, Example 13.6]).

THEOREM. — *The angles $\theta_{p,a}$ for $a = 1,\ldots,p-1$ are equidistributed with respect to the Sato-Tate measure as $p \to \infty$, i.e. we have*

$$\frac{1}{p-1}|\{1 \leq a < p | \alpha \leq \theta_{p,a} \leq \beta\}| \to \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta d\theta.$$

A corresponding horizontal result is expected to hold.

CONJECTURE. — *The angles $\theta_{p,a}$ for $p \sim X$ are equidistributed with respect to the Sato-Tate measure as $X \to \infty$, i.e. we have*

$$\frac{|\{X \leq p < 2X | \alpha \leq \theta_{p,a} \leq \beta\}|}{|\{X \leq p < 2X\}|} \to \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta d\theta.$$

However, it is not even known whether $\mathrm{Kl}(1,a;p)$ changes sign infinitely often. In this paper we prove the following approximation towards that.

THEOREM 1.1. — *There exist $X_0 \geq 1$ and $c_0 > 0$ such that, for $X \geq X_0$, we have*

$$|\{n \sim X| \operatorname{Kl}(1,1,n) > 0, \mu^2(n) = 1, \omega(n) \leq 15\}| \geq c_0 \frac{X}{\log X}$$

and

$$|\{n \sim X| \operatorname{Kl}(1,1,n) < 0, \mu^2(n) = 1, \omega(n) \leq 15\}| \geq c_0 \frac{X}{\log X}.$$

The first result of this type was obtained by Fouvry and Michel [3]. They showed the result with the condition $\omega(n) \leq 15$ replaced by assertion that all prime factors of n are larger than $n^{1/23.9}$ (which of course implies the above with 15 replaced by 23). Sivak-Fischler has improved 1/23.9 to 1/22.29 in [6] and showed the above theorem with 15 replaced by 18 in [7].

2. The method described

Following [2] and [7] we consider the sum

$$\sum_n \frac{\operatorname{Kl}(1,1,n)}{\sqrt{n}} g\left(\frac{n}{X}\right) \mu^2(n) \Lambda_k(n) \left(\sum_{d|n} \lambda_d\right)^2,$$

where $g(y)$ is a smooth function supported in the interval $[1,2]$, $\Lambda_k = (\log)^k * \mu$ is the generalized von Mangoldt function and λ_d are Selberg sieve weights satisfying

$$(2) \qquad \begin{cases} \lambda_1 = 1 & \\ \lambda_d = 0 & \text{if } d > 2z \text{ or } \mu(d) = 0, \\ |\lambda_d| \leq 2^{\omega(d)+1} & \text{for all } d \in \mathbb{N}, \\ \lambda_d = \mu(d) \frac{\log^4(z/d)}{\log^4 z} + O_\eta\left(\frac{\log^3(z/d)}{\log^4 z}\right) & \text{for any } \eta > 0 \text{ and } d < z^{1-\eta}, \end{cases}$$

where the level $2z = 2X^{1/20}(\log X)^{-B}$ for some large positive constant B.

Recalling that $\Lambda_k(n)$ is supported on numbers with at most k distinct prime factors, Theorem 1.1 follows once we have proved the following propositions in which $\hat{g} = \int_1^2 g(x)dx$.

PROPOSITION 2.1. — *For every large enough X we have*

$$(3) \qquad \sum_n \frac{|\operatorname{Kl}(1,1,n)|}{\sqrt{n}} g\left(\frac{n}{X}\right) \mu^2(n) \Lambda_{15}(n) \left(\sum_{d|n} \lambda_d\right)^2 > 0.89 \cdot \hat{g} X (\log X)^{14}.$$

Proposition 2.2. — *For every large enough X there exist sieve weights λ_d satisfying* (2) *such that*

$$\left|\sum_n \frac{\mathrm{Kl}(1,1,n)}{\sqrt{n}} g\left(\frac{n}{X}\right)\mu^2(n)\Lambda_{15}(n)\left(\sum_{d|n}\lambda_d\right)^2\right| < 0.81\cdot \hat{g}X(\log X)^{14}.$$

In Section 4 we show how Proposition 2.2 follows from Sivak-Fischler's work [7]. In Section 3 we prove Proposition 2.1 still following Sivak-Fischler's arguments that go back to [3]. Our improvement comes from introducing the following lemma which might have other applications.

Lemma 2.3. — *Assume that the sequences $(a_m)_{m\le M}$ and $(b_m)_{m\le M}$ contained in $[0,1]$ become equidistributed with respect to some continuous measures μ_a and μ_b respectively when $M\to\infty$. Then*

$$(1+o(1))\int_0^1 xy_l(x)d\mu_a([0,x]) \le \frac{1}{M}\sum_{m=1}^M a_m b_m \le (1+o(1))\int_0^1 xy_u(x)d\mu_a([0,x])$$

where $y_l(x)$ is the smallest solution to the equation $\mu_b([y_l,1]) = \mu_a([0,x])$ and $y_u(x)$ is the largest solution to the equation $\mu_b([0,y_u]) = \mu_a([0,x])$.

Remark 2.4. — As will be clear from the proof, the bounds are best possible under the given assumptions. The lower bound can be used to replace the trivial bound

$$\frac{1}{M}\sum_{m=1}^M a_m b_m \ge (1+o(1))AB(1-\mu_a([0,A])-\mu_b([0,B])), \tag{4}$$

which holds for any $A,B\in[0,1]$.

Proof of Lemma 2.3. — Denote by $\bar{c}_n$ the sequence c_n arranged in increasing order. Then by the rearrangement inequality (see [4, Theorem 368]),

$$\frac{1}{M}\sum_{m=1}^M a_m b_m \ge \frac{1}{M}\sum_{m=1}^M \bar{a}_m\bar{b}_{M-m}.$$

Invoking the equidistribution of the sequence a_m, the right hand side is

$$\ge (1+o(1))\int_0^1 x\bar{b}_{M-\lceil M\mu([0,x])\rceil}d\mu_a([0,x]).$$

Now the lower bound follows from the equidistribution of b_n. The upper bound can be proved similarly since

$$\sum_{m=1}^M a_m b_m \le \sum_{m=1}^M \bar{a}_m\bar{b}_m$$