PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 2, February 2008, Pages 419–425
S 0002-9939(07)08943-5
Article electronically published on November 2, 2007

ON THE DISTRIBUTION OF KLOOSTERMAN SUMS

IGOR E. SHPARLINSKI

(Communicated by Wen-Ching Winnie Li)

Abstract. For a prime p, we consider Kloosterman sums

$$K_p(a) = \sum_{x \in \mathbb{F}_p^*} \exp(2\pi i(x + ax^{-1})/p), \qquad a \in \mathbb{F}_p^*,$$

over a finite field of p elements. It is well known that due to results of Deligne, Katz and Sarnak, the distribution of the sums $K_p(a)$ when a runs through $\mathbb{F}_p^*$ is in accordance with the Sato–Tate conjecture. Here we show that the same holds where a runs through the sums $a = u + v$ for $u \in \mathcal{U}$, $v \in \mathcal{V}$ for any two sufficiently large sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$.

We also improve a recent bound on the nonlinearity of a Boolean function associated with the sequence of signs of Kloosterman sums.

1. Introduction

For a prime p we use $\mathbb{F}_p$ to denote the finite field of p elements.

For $a \in \mathbb{F}_p^*$ we consider the Kloosterman sum

$$K_p(a) = \sum_{x \in \mathbb{F}_p^*} \mathbf{e}_p(x + ax^{-1}),$$

where

$$\mathbf{e}_p(z) = \exp(2\pi iz/p)$$

(we identify $\mathbb{F}_p$ with the set $\{0, 1, \ldots, p-1\}$). Since for the complex conjugated sum we have

$$\overline{K_p(a)} = \sum_{x \in \mathbb{F}_p^*} \mathbf{e}_p(-x - ax^{-1}) = K_p(a),$$

the values of $K_p(a)$ are real.

According to the Weil bound, see [15],

$$|K_p(a)| \le 2\sqrt{p}, \qquad a \in \mathbb{F}_p^*.$$

Therefore, we can define the angles $\psi_p(a)$ by the relations

$$K_p(a) = 2\sqrt{p}\cos\psi_p(a) \qquad \text{and} \qquad 0 \le \psi_p(a) \le \pi.$$

Received by the editors August 20, 2006 and, in revised form, September 29, 2006.
2000 *Mathematics Subject Classification.* Primary 11L05, 11L40, 11T71.
During the preparation of this paper, the author was supported in part by ARC grant DP0556431.

The famous *Sato–Tate* conjecture asserts that for any fixed nonzero integer a, when p varies, the angles $\psi_p(a)$ are distributed according to the *Sato–Tate density*

$$\mu_{ST}(\alpha,\beta) = \frac{2}{\pi}\int_\alpha^\beta \sin^2\gamma\, d\gamma;$$

see [1, 6, 7, 8, 9, 11, 12, 14, 16, 17, 18] for various modifications and generalisations of this conjecture and further references.

It is also known that when a sufficiently large prime p is fixed and a runs through $\mathbb{F}_p^*$, then, as has been shown by Katz [11, Chapter 13], the work of Deligne on the *Weil conjecture* implies that the distribution of the sums $K_p(a)$ is in accordance with the Sato–Tate density; see also [12]. Furthermore, a quantitative form of this result is given by Niederreiter [18]. Namely, if $\mathcal{A}_p(\alpha,\beta)$ is the set of $a \in \mathbb{F}_p^*$ with $\alpha \le \psi_p(a) \le \beta$, then by the main result of Niederreiter [18], we have

$$\max_{0\le\alpha<\beta\le\pi} |\#\mathcal{A}_p(\alpha,\beta) - \mu_{ST}(\alpha,\beta)p| \ll p^{3/4}. \tag{1}$$

Combining results of Fouvry, Michel, Rivat, and Sárközy [9, Lemma 2.3] (with $r=1$) and of Niederreiter [18, Lemma 3], one can show that elements of $\mathcal{A}_p(\alpha,\beta)$ are uniformly distributed in the following sense. For any $\lambda \in \mathbb{F}_p^*$ and integer M with $1 \le M \le p-1$, we put

$$\mathcal{A}_p(\lambda, M; \alpha,\beta) = \{a \in \mathcal{A}_p(\alpha,\beta) \ : \ \lambda a \in [1, M]\}.$$

Then for $1 \le M \le p-1$, the following bound holds:

$$\max_{\lambda\in\mathbb{F}_p^*} \max_{0\le\alpha<\beta\le\pi} |\#\mathcal{A}_p(\lambda, M; \alpha,\beta) - \mu(\alpha,\beta)M| \ll M^{1/2}p^{1/4}(\log p)^{1/2}. \tag{2}$$

Fouvry, Michel, Rivat, and Sárközy [9] also remark that by combining a result of Fouvry and Michel [7] with the technique of Vaaler [20], one can show that

$$\max_{0\le\alpha<\beta\le\pi} |\#\mathcal{Q}_p(\alpha,\beta) - \mu_{ST}(\alpha,\beta)p| \ll p^{3/4},$$

where

$$\mathcal{Q}_p(\alpha,\beta) = \{a \in \mathbb{F}_p : \ a^2 \in \mathcal{A}_p(\alpha,\beta)\}.$$

The same bound can also be obtained immediately if one applies the result of Niederreiter [18, Lemma 3] to the bound of Michel [17, Corollary 2.4] (see also [7, Lemma 2.1]).

Here we show that the same type of distribution is preserved when a runs through the sums $a = u+v$ where $u \in \mathcal{U}$, $v \in \mathcal{V}$ for any two sufficiently large sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$. Namely, for any two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$, we put

$$\mathcal{W}_p(\mathcal{U},\mathcal{V};\alpha,\beta) = \{(u,v) \in \mathcal{U}\times\mathcal{V} \ : \ u+v \in \mathcal{A}_p(\alpha,\beta)\}.$$

In particular, we obtain an asymptotic formula for $\#\mathcal{W}_p(\mathcal{U},\mathcal{V};\alpha,\beta)$ which is nontrivial whenever

$$\#\mathcal{U}\#\mathcal{V} \ge p^{3/2+\varepsilon} \tag{3}$$

for any fixed $\varepsilon > 0$ and sufficiently large p.

Then, we also improve the upper bound of [19] on the *nonlinearity* of the Boolean function associated with the sequence of signs of Kloosterman sums; that is, for the function

$$f(a) = \begin{cases} 0, & \text{if } K(a) > 0 \text{ or } a = 0, \\ 1, & \text{if } K(a) < 0, \end{cases} \qquad a = 0, 1, \ldots, 2^{n-1}, \tag{4}$$

where n is defined by the inequalities

$$2^n \le p < 2^{n+1}.$$

Various pseudorandom properties of the function $f(a)$ have been studied by Fouvry, Michel, Rivat, and Sárközy [9]. Here we estimate one more characteristic of $f(a)$ of cryptographic interest, which in fact has already been considered in [19] whose result we now improve.

We denote by $\mathfrak{B}_n$ the n-dimensional Boolean cube $\mathfrak{B}_n = \{0,1\}^n$ and in a natural way identify its elements with the integers in the range $0 \le a \le 2^n - 1$ (and thus with a subset of $\mathbb{F}_p$).

We define the *Fourier coefficients* of $f(a)$ as

$$\widehat{f}(r) = 2^{-n} \sum_{a \in \mathfrak{B}_n} (-1)^{f(a)+\langle h,r\rangle}, \qquad r \in \mathfrak{B}_n,$$

where $\langle a, r\rangle$ denotes the inner product of $a, r \in \mathfrak{B}_n$. Furthermore, we recall that

$$N(f) = 2^{n-1} - 2^{n-1} \max_{r \in \mathfrak{B}_n} \left|\widehat{f}(r)\right|$$

is called the *nonlinearity* of f and is an important cryptographic characteristic; for example, see [5]. In particular, it is the smallest possible Hamming distance between the vector of values of f and the vector of values of a linear function in n variables over $\mathbb{F}_2$.

Several results about some measures of pseudorandomess of the sequence of signs of Kloosterman sums have recently been obtained by Fouvry, Michel, Rivat, and Sárközy [9]. Motivated by (and actually using) the results of [9], the bound

$$N(f) = 2^{n-1}\left(1 + O\left(2^{-n/24} n^{1/12}\right)\right)$$

obtained in [19]. Here again we use some results of [9], but in a slightly different way, and we improve this bound.

2. Distribution of elements of $\mathcal{A}_p(\alpha, \beta)$

For a sequence of N real numbers $\gamma_1, \ldots, \gamma_N \in [0,1)$ the *discrepancy* is defined by

$$D = \max_{0 \le \gamma \le 1} \left|\frac{T(\gamma, N)}{N} - \gamma\right|,$$

where $T(\gamma, N)$ is the number of $n \le N$ such that $\gamma_n \le \gamma$.

We also recall our agreement that the elements of $\mathbb{F}_p$ have canonical representation as integers of the interval $[0, p-1]$. Thus for any field element $c \in \mathbb{F}_p$, we interpret c/p as a rational number in the interval $[0,1]$. Hence, for $\lambda \in \mathbb{F}_p^*$ we can define the discrepancy $D_p(\lambda; \alpha, \beta)$ of the sequence

$$\frac{\lambda a}{p}, \quad a \in \mathcal{A}_p(\alpha, \beta).$$

Then the bound (2) implies that

$$\max_{1 \le M \le p-1} \max_{\lambda \in \mathbb{F}_p^*} \max_{0 \le \alpha < \beta \le \pi} |\#\mathcal{A}_p(\lambda, M; \alpha, \beta) - \mu(\alpha, \beta) M| \ll p^{3/4} (\log p)^{1/2},$$

which can be reformulated in the following form:

Lemma 1. *We have*

$$\max_{\lambda \in \mathbb{F}_p^*} \max_{0 \le \alpha < \beta \le \pi} D_p(\lambda; \alpha, \beta) \ll p^{-1/4} (\log p)^{1/2}.$$

Our main tool is a bound of exponential sums with elements of $\mathcal{A}_p(\alpha, \beta)$. For $\lambda \in \mathbb{F}_p^*$ we define

$$S_p(\lambda; \alpha, \beta) = \sum_{a \in \mathcal{A}_p(\alpha, \beta)} \mathbf{e}_p(\lambda a).$$

Lemma 2. *We have*

$$\max_{\lambda \in \mathbb{F}_p^*} \max_{0 \le \alpha < \beta \le \pi} |S_p(\lambda; \alpha, \beta)| \ll p^{3/4} (\log p)^{1/2}.$$

Proof. We recall that for any real smooth function $F(\gamma)$ defined on the interval $[0, 1]$ and any sequence of N real numbers $\gamma_1, \ldots, \gamma_N \in [0, 1]$ of discrepancy D, we have

$$\frac{1}{N} \sum_{n=1}^{N} F(\gamma_n) = \int_0^1 F(\gamma) d\,\gamma + O(D \max_{0 \le \gamma \le 1} |F'(\gamma)|);$$

see [13, Chapter 2, Theorem 5.4]. Writing

$$S_p(\lambda; \alpha, \beta) = \sum_{a \in \mathcal{A}_p(\alpha, \beta)} \cos\left(2\pi \frac{\lambda a}{p}\right) + i \sum_{a \in \mathcal{A}_p(\alpha, \beta)} \sin\left(2\pi \frac{\lambda a}{p}\right)$$

and applying Lemma 1, we obtain the desired bound. □

3. Sato–Tate conjecture for sum sets

Theorem 3. *For any two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$, we have*

$$\max_{0 \le \alpha < \beta \le \pi} |\#\mathcal{W}_p(\mathcal{U}, \mathcal{V}; \alpha, \beta) - \mu_{ST}(\alpha, \beta) \#\mathcal{U} \#\mathcal{V}| \le \sqrt{\#\mathcal{U} \#\mathcal{V}}\, p^{3/4} (\log p)^{1/2}.$$

Proof. Using the identity

$$\frac{1}{p} \sum_{\lambda \in \mathbb{F}_p} \mathbf{e}_p(\lambda c) = \begin{cases} 1 & \text{if } c = 0, \\ 0 & \text{if } c \in \mathbb{F}_p^*, \end{cases} \tag{5}$$

we write

$$\begin{aligned} \#\mathcal{W}_p(\mathcal{U}, \mathcal{V}; \alpha, \beta) &= \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \sum_{a \in \mathcal{A}_p(\alpha, \beta)} \frac{1}{p} \sum_{\lambda \in \mathbb{F}_p} \mathbf{e}_p\left(\lambda(u + v - a)\right) \\ &= \frac{1}{p} \sum_{\lambda \in \mathbb{F}_p} S_p(-\lambda; \alpha, \beta) \sum_{u \in \mathcal{U}} \mathbf{e}_p(\lambda u) \sum_{v \in \mathcal{V}} \mathbf{e}_p(\lambda v). \end{aligned}$$

Separating the term $\#\mathcal{A}_p(\alpha, \beta)\#\mathcal{U}\#\mathcal{V}/p$ corresponding to $\lambda = 0$, we derive

$$\#\mathcal{W}_p(\mathcal{U}, \mathcal{V}; \alpha, \beta) = \frac{\#\mathcal{A}_p(\alpha, \beta)\#\mathcal{U}\#\mathcal{V}}{p} + O\left(R\right), \tag{6}$$

where

$$R = \frac{1}{p} \sum_{\lambda \in \mathbb{F}_p^*} |S_p(-\lambda; \alpha, \beta)| \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(\lambda u) \right| \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(\lambda v) \right|.$$

Using Lemma 2 and the Cauchy inequality, we obtain

$$\begin{aligned} R &\le p^{-1/4}(\log p)^{1/2} \sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(\lambda u) \right| \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(\lambda v) \right| \\ &\le p^{-1/4}(\log p)^{1/2} \left(\sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(\lambda u) \right|^2 \right)^{1/2} \left(\sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(\lambda v) \right|^2 \right)^{1/2}. \end{aligned}$$

Furthermore, by (5) we see that

$$\sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(\lambda u) \right|^2 \le \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(\lambda u) \right|^2 = \sum_{\lambda \in \mathbb{F}_p} \sum_{u_1, u_2 \in \mathcal{U}} \mathbf{e}_p\left(\lambda(u_1 - u_2)\right) = p \# \mathcal{U}.$$

Similarly,

$$\sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(\lambda v) \right|^2 \le p \# \mathcal{V}.$$

Collecting the above estimates together, we obtain

$$R \le \sqrt{\# \mathcal{U} \# \mathcal{V}}\, p^{3/4} (\log p)^{1/2},$$

which after substitution in (6) and using (1) leads us to the bound

$$\begin{aligned} &|\# \mathcal{W}_p(\mathcal{U}, \mathcal{V}; \alpha, \beta) - \mu_{ST}(\alpha, \beta) \# \mathcal{U} \# \mathcal{V}| \\ &\qquad \ll \# \mathcal{U} \# \mathcal{V} p^{-1/4} + \sqrt{\# \mathcal{U} \# \mathcal{V}}\, p^{3/4} (\log p)^{1/2}. \end{aligned}$$

It remains to note that

$$\# \mathcal{U} \# \mathcal{V} p^{-1/4} \le \sqrt{\# \mathcal{U} \# \mathcal{V}}\, p^{3/4};$$

thus the first term never dominates. □

Clearly the asymptotic formula of Theorem 3 is nontrivial under condition (3).

4. Nonlinearity

Theorem 4. *For the nonlinearity $N(f)$ of the Boolean function $f(h)$ given by* (4)*, we have*

$$N(f) = 2^{n-1} \left(1 + O\left(2^{-n/16} n^{1/8}\right)\right).$$

Proof. We estimate the Fourier coefficients $\widehat{f}(k)$ of f by using the result that for any integers M, h_1, h_2 with $0 \le M \le M + c_1 < M + c_2 < 2^n$ we have

$$\sum_{b=0}^{M-1} (-1)^{f(b+c_1)+f(b+c_2)} \ll M^{2/3} p^{1/6} (\log p)^{1/3} + p^{1/2} \log p,$$

which is a combination of [9, Lemma 2.3] with a special case $r = 2$ of [9, Lemma 4.4]. In fact, the above bound can be simplified as

$$\sum_{b=0}^{M-1} (-1)^{f(b+c_1)+f(b+c_2)} \ll M^{2/3} p^{1/6} (\log p)^{1/3} \tag{7}$$

(since for $M \le p^{1/2} \log p$ the bound (7) is trivial and for $M > p^{1/2} \log p$ we also have $M^{2/3} p^{1/6} (\log p)^{1/3} > p^{1/2} \log p$).

We now fix some $m \le n$ and write $a, r \in \mathfrak{B}_n$ as

$$a = b + 2^m c \qquad \text{and} \qquad r = s + 2^m t,$$

with $0 \le b, s < 2^m$ and $0 \le c, t < 2^{n-m}$. In particular

$$\langle a, r\rangle = \langle b, s\rangle + \langle c, t\rangle.$$

Therefore,

$$\begin{aligned} |\widehat{f}(r)| &= |\widehat{f}(s + 2^m t)| = \left|2^{-n} \sum_{b=0}^{2^m-1} \sum_{c=0}^{2^{n-m}-1} (-1)^{f(b+2^m c)+\langle b,s\rangle+\langle c,t\rangle}\right| \\ &\le 2^{-n} \sum_{b=0}^{2^m-1} \left| \sum_{c=0}^{2^{n-m}-1} (-1)^{f(b+2^m c)+\langle c,t\rangle}\right|. \end{aligned}$$

By the Cauchy inequality we obtain

$$\begin{aligned} |\widehat{f}(r)|^2 &\le 2^{m-2n} \sum_{b=0}^{2^m-1} \left| \sum_{j=0}^{2^{n-m}-1} (-1)^{f(b+2^m c)+\langle c,t\rangle}\right|^2 \\ &= 2^{m-2n} \sum_{b=0}^{2^m-1} \sum_{c_1,c_2=0}^{2^{n-m}-1} (-1)^{f(b+2^m c_1)+f(b+2^m c_2)+\langle c_1,t\rangle+\langle c_2,t\rangle} \\ &\le 2^{m-2n} \sum_{c_1,c_2=0}^{2^{n-m}-1} \left| \sum_{b=0}^{2^m-1} (-1)^{f(b+2^m c_1)+f(b+2^m c_2)}\right|. \end{aligned}$$

For 2^{n-m} choices of $c_1 = c_2$, the sums over b are equal to 2^m. For the other choices of c_1 and c_2 we can use the bound (7), getting

$$\begin{aligned} |\widehat{f}(r)|^2 &= O\left(2^{m-2n}\left(2^{n-m}2^m + 2^{2(n-m)}2^{2m/3}2^{n/6}n^{1/3}\right)\right) \\ &= O\left(2^{m-n} + 2^{n/6-m/3}n^{1/3}\right). \end{aligned}$$

We now define m by the inequalities $2^m \le 2^{7n/8}n^{1/4} < 2^{m+1}$, and after simple calculations conclude the proof. □

5. Comments

It seems very plausible that [17, Corollary 2.4] can be used to derive a nontrivial estimate for sums

$$T_p(\chi; \alpha, \beta) = \sum_{a \in \mathcal{A}_p(\alpha,\beta)} \chi(a),$$

with a nonprincipal multiplicative character χ of $\mathbb{F}_p^*$. In this case one can obtain a multiplicative analogue of our results and study the set

$$\mathcal{Z}_p(\mathcal{U}, \mathcal{V}; \alpha, \beta) = \{(u, v) \in \mathcal{U} \times \mathcal{V} \ : \ uv \in \mathcal{A}_p(\alpha, \beta)\}.$$

Multidimensional analogues of our results which involve joint distributions of Kloosterman sums can be obtained as well.

Also, as a curiosity, we mention that Theorem 3 can be combined with the techniques of [2, 3, 4] to study sets of elements of the *Beatty* sequence $\lfloor \vartheta m + \rho \rfloor$ (where $\vartheta > 0$ and ρ are real) which belong to $\mathcal{A}_p(\alpha, \beta)$; that is, sets of the form

$$\mathcal{B}_p(\vartheta, \rho, M; \alpha, \beta) = \{m \in [1, M] \ : \ \lfloor \vartheta m + \rho \rfloor \in \mathcal{A}_p(\alpha, \beta)\}.$$

References

[1] A. Adolphson, 'On the distribution of angles of Kloosterman sums', *J. Reine Angew. Math.* **395** (1989), 214–220. MR983069 (90k:11109)

[2] W. Banks and I. E. Shparlinski, 'Non-residues and primitive roots in Beatty sequences', *Bull. Aust. Math. Soc.* **73** (2006), 433–443. MR2230651 (2007a:11118)

[3] W. Banks and I. E. Shparlinski, 'Short character sums with Beatty sequences', *Math. Res. Lett.* **13** (2006), 539–547. MR2250489

[4] W. Banks and I. E. Shparlinski, 'Prime divisors in Beatty sequences', *J. Number Theory* **123** (2007), 413–425.

[5] C. Carlet and C. Ding, 'Highly nonlinear mappings', *J. Compl.*, **20** (2004), 205–244. MR2067428 (2006d:94043)

[6] C.-L. Chai and W.-C. W. Li, 'Character sums, automorphic forms, equidistribution, and Ramanujan graphs. I: The Kloosterman sum conjecture over function fields', *Forum Math.* **15** (2003), 679–699. MR2010030 (2005h:11136)

[7] É. Fouvry and P. Michel, 'Sommes de modules de sommes d'exponentielles', *Pacific J. Math.* **209** (2003), 261–288. MR1978371 (2004d:11072)

[8] É. Fouvry and P. Michel, 'Sur le changement de signe des sommes de Kloosterman', *Ann. Math.* (to appear).

[9] É. Fouvry, P. Michel, J. Rivat and A. Sárközy, 'On the pseudorandomness of the signs of Kloosterman sums', *J. Aust. Math. Soc.* **77** (2004), 425–436. MR2099811 (2005h:11165)

[10] H. Iwaniec and E. Kowalski, *Analytic number theory.* American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[11] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Princeton Univ. Press, Princeton, NJ, 1988. MR955052 (91a:11028)

[12] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc, Providence, RI, 1999. MR1659828 (2000b:11070)

[13] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New York-London-Sydney, 1974. MR0419394 (54:7415)

[14] G. Laumon, 'Exponential sums and l-adic cohomology: A survey', *Israel J. Math.* **120** (2000), 225–257. MR1815377 (2002m:11075)

[15] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997. MR1429394 (97i:11115)

[16] P. Michel, 'Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman, II', *Duke Math. J.* **92** (1998), 221–254. MR1612781 (99d:11094)

[17] P. Michel, 'Minoration de sommes d'exponentielles', *Duke Math. J.* **95** (1998), 227–240. MR1652005 (99i:11069)

[18] H. Niederreiter, 'The distribution of values of Kloosterman sums', *Arch. Math.* **56** (1991), 270–277. MR1091880 (92b:11057)

[19] I. E. Shparlinski, 'On the nonlinearity of the sequence of signs of Kloosterman sums', *Bull. Aust. Math. Soc.* **71** (2005), 405–409. MR2150929 (2006e:11115)

[20] J. Vaaler, 'Some extremal functions in Fourier analysis', *Bull. Amer. Math. Soc.* **12** (1985), 183–216. MR776471 (86g:42005)

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au