ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 43, Number 1, 2013

ON SOME EXPONENTIAL SUMS WITH EXPONENTIAL AND RATIONAL FUNCTIONS

IGOR E. SHPARLINSKI

ABSTRACT. We study exponential sums of the form

$$\sum_{x=1}^{t} {}^{*} \exp(2\pi i(a\vartheta^x/p + f(x)/t))$$

where ϑ is an integer of multiplicative order t modulo a prime p, $f(X)$ is rational function modulo t and Σ^* indicates that the poles of f are excluded. The case of $f(X) = bX$ is well studied and has been considered in a number of works. For $f(X) = b/X$ these sums have recently been estimated by Bourgain and the author. Here we consider the general case of an arbitrary rational function f.

1. Introduction. For a prime p we denote by $\mathbf{F}_p$ the finite field of p elements, which we assume to be represented by the set $\{0, 1, \dots, p-1\}$. For an integer t we denote by $\mathbf{Z}_t$ the residue ring modulo t and by $\mathbf{Z}_t^*$ the group of units of $\mathbf{Z}_t$.

Let $\vartheta \in \mathbf{F}_p^*$ be of multiplicative order $t \geq 1$. Furthermore, for an integer $m > 0$, we put

$$\mathbf{e}_m(z) = \exp(2\pi i z/m),$$

and define the exponential sums

$$S_p(a; f) = \sum_{x \in \mathcal{X}_f} \mathbf{e}_p(a\vartheta^x)\mathbf{e}_t(f(x))$$

where $f(X)$ is rational function over $\mathbf{Z}_t$ and $\mathcal{X}_f$ is the set of $x \in \mathbf{Z}_t$ for which the denominator of $f(X)$ is a unit of $\mathbf{Z}_t$.

2010 AMS *Mathematics subject classification.* Primary 11L07, 11T23.
Keywords and phrases. Exponential sums, uniform distribution.
During the preparation of this paper, the author was supported in part by ARC grant DP1092835.
Received by the editors on March 3, 2010, and in revised form on June 13, 2010.
DOI:10.1216/RMJ-2013-43-1-361

The case of $f(X) = bX$ (including $b = 0$) is well studied. In particular, the bound

$$\left|\sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^x)\mathbf{e}_t(bx)\right| \le p^{1/2}, \tag{1}$$

where $a, b \in \mathbf{Z}$ and $\gcd(a,p) = 1$, is a very special case of a much more general estimate of Korobov [**10**] of exponential sums with linear recurrence sequences.

Clearly the bound (1) becomes trivial for $t \le p^{1/2}$. For $b = 0$, a bound which is nontrivial already for $t \ge p^{3/7+\varepsilon}$ (with an arbitrary $\varepsilon > 0$) is given in [**12**]. In turn, the result of [**12**] has been improved by Heath-Brown and Konyagin [**7**] who lowered the threshold to $t \ge p^{1/3+\varepsilon}$. Konyagin [**9**] has further lowered it down to $t \ge p^{1/4+\varepsilon}$. Furthermore, in [**13**, Lemma 3.15] the result of [**7**] is extended to arbitrary b (which requires slightly more efforts and care than one usually expects for such generalizations), so (1) can now be replaced with

$$\left|\sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^x)\mathbf{e}_t(bx)\right| = \begin{cases} O(p^{1/2}), & \text{if } t \ge p^{2/3}, \\ O(p^{1/4}t^{3/8}), & \text{if } p^{2/3} > t \ge p^{1/2}, \\ O(p^{1/8}t^{5/8}), & \text{if } p^{1/2} > t \ge p^{1/3}, \end{cases} \tag{2}$$

where $a, b \in \mathbf{Z}$ and $\gcd(a,p) = 1$.

The estimates of [**7, 9, 12**] are completely explicit. In fact, Cochrane and Pinner [**5**] have even evaluated explicitly the constants hidden in the 'O'-symbols in (2). Less explicit results, that however are valid, in an amazingly wide range of $t \ge p^{\varepsilon}$ have been given by Bourgain, Glibichuk and Konyagin [**3**] for $b = 0$. In fact, it is easy to extend this estimate to arbitrary $b \in \mathbf{Z}$. Indeed, since

$$\begin{aligned} \left|\sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^x)\mathbf{e}_t(bx)\right| &= \frac{1}{t}\left|\sum_{y=1}^{t}\sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^{x+y})\mathbf{e}_t(b(x+y))\right| \\ &\le \frac{1}{t}\sum_{y=1}^{t}\left|\sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^{x+y})\mathbf{e}_t(bx)\right|, \end{aligned}$$

applying the Cauchy inequality and changing the order of summation, we derive

$$\left|\sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^x)\mathbf{e}_t(bx)\right|^2 \le \frac{1}{t}\sum_{x_1,x_2=1}^{t}\left|\sum_{y=1}^{t} \mathbf{e}_p(a(\vartheta^{x_1} - \vartheta^{x_2}))\vartheta^y)\right|.$$

Now [**3**, Theorem 6] implies that, for any $\varepsilon > 0$, there exists some $\delta > 0$ such that, for $t \geq p^{\varepsilon}$, we have

$$\left| \sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^x)\mathbf{e}_t(bx) \right| \leq tp^{-\delta}. \tag{3}$$

Furthermore, Bourgain [**2**] has obtained a nontrivial estimate for these sums already for $t \geq p^{c/\log\log p}$ with some absolute constant $c > 0$.

For nonlinear functions f, the only nontrivial bounds of $S_p(a, f)$ have been known for $f(X) = b/X$, $b \in \mathbf{Z}$. In [**4**] it is obtained for $t \geq p^{\varepsilon}$ with an arbitrary $\varepsilon > 0$, and then also in [**14**] only for $t \geq p^{1/2+\varepsilon}$ but in a more explicit form than in [**4**].

Here, in the case of prime t, we use a modification of the method of [**4, 14**] to estimate the sums $S_p(a; f)$ for an arbitrary rational function f.

It is crucial for our approach to have good estimates on the number of solutions to the congruences of the form

$$\sum_{j=1}^{m} a_j \vartheta^{x_j} \equiv 0 \pmod p, \quad x_1, \dots, x_m \in \mathbf{Z}_t. \tag{4}$$

We use the bound (3) to derive such estimates, and then estimate the sums $S_p(a; f)$ provided that $t \geq p^{\varepsilon}$ is prime. Furthermore, for large values of t, namely for prime $t \geq p^{2/3}$, we use the more explicit bound (1) (note that both bounds are used with $b = 0$).

In fact, our approach also works for composite t; however, the result is much weaker and the technical details are more involved.

Throughout the paper, any implied constants in symbols O, $\ll$ and $\gg$ may occasionally depend, where obvious, upon the real positive parameter ε, the integer parameter k and the degree of the function f, and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \leq cV$ holds with some constant $c > 0$.

2. Preparations. Here we obtain some estimates on the number of solutions to the congruence (4). Let us define

$$\sigma_t = \max_{a=1,\dots,p-1} \left| \sum_{x=1}^{t} \mathbf{e}_p(a\vartheta^x) \right|.$$

(Note that this quantity depends only upon t rather than on ϑ.)

Lemma 1. *For an integer $m \ge 2$ and arbitrary integers $a_1, \dots, a_m$ with $\gcd(a_1 \cdots a_m, p) = 1$, the congruence (4) has*

$$J = \frac{t^m}{p} + O(\sigma_t^{m-2} t)$$

solutions.

Proof. Using the identity

$$\frac{1}{p} \sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda v) = \begin{cases} 1 & \text{if } v \equiv 0 \pmod p, \\ 0 & \text{if } v \not\equiv 0 \pmod p, \end{cases}$$

we express N via exponential sums as follows:

$$J = \sum_{x_1,\dots,x_m \in \mathbf{Z}_t} \frac{1}{p} \sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(\lambda \sum_{j=1}^{m} a_j \vartheta^{x_j}\right) = \frac{1}{p} \sum_{\lambda=0}^{p-1} \prod_{j=1}^{m} \sum_{x_j \in \mathbf{Z}_t} \mathbf{e}_p(\lambda a_j \vartheta^{x_j}).$$

Separating the term t^m/p corresponding to $\lambda = 0$, we derive

$$\frac{J - t^m}{p} \ll \frac{1}{p} \sum_{\lambda=1}^{p-1} \prod_{j=1}^{m} \left| \sum_{x_j \in \mathbf{Z}_t} \mathbf{e}_p(\lambda a_j \vartheta^{x_j}) \right| \le \frac{\sigma_t^{m-2}}{p} \sum_{\lambda=1}^{p-1} \prod_{j=1}^{2} \left| \sum_{x_j \in \mathbf{Z}_t} \mathbf{e}_p(\lambda a_j \vartheta^{x_j}) \right|.$$

Finally, by the Cauchy inequality

$$\begin{aligned} &\sum_{\lambda=1}^{p-1} \prod_{j=1}^{2} \left| \sum_{x_j \in \mathbf{Z}_t} \mathbf{e}_p(\lambda a_j \vartheta^{x_j}) \right| \\ &\qquad \le \sqrt{\sum_{\lambda=1}^{p-1} \left| \sum_{x_1 \in \mathbf{Z}_t} \mathbf{e}_p(\lambda a_1 \vartheta^{x_1}) \right|^2} \sqrt{\sum_{\lambda=1}^{p-1} \left| \sum_{x_2 \in \mathbf{Z}_t} \mathbf{e}_p(\lambda a_2 \vartheta^{x_2}) \right|^2} \\ &\qquad = \sum_{\lambda=1}^{p-1} \left| \sum_{x \in \mathbf{Z}_t} \mathbf{e}_p(\lambda \vartheta^{x}) \right|^2 \le \sum_{\lambda=0}^{p-1} \left| \sum_{x \in \mathbf{Z}_t} \mathbf{e}_p(\lambda \vartheta^{x}) \right|^2 = pt, \end{aligned}$$

and the result now follows. □

We now estimate the number of solutions of an inhomogeneous version of (4):

$$\sum_{j=1}^{m} a_j \vartheta^{x_j} + a_0 \equiv 0 \pmod p, \quad x_1, \dots, x_m \in \mathbf{Z}_t. \tag{5}$$

We also need a result about linear independence of rational functions with shifted arguments.

Lemma 2. *Assume that $f(X) \in \mathbf{Z}_t(X)$ is a rational function that is not a polynomial. Then, for all but $O(t^k)$ vectors $\mathbf{x} = (x_1, \dots, x_{2k}) \in \mathbf{Z}_t^{2k}$, the rational function*

$$F_{\mathbf{x}}(X) = \sum_{j=1}^{2k} (-1)^j f(x_j + X)$$

is not constant.

Proof. Write $f(X) = g(X)/h(X)$ with two relatively prime polynomials $g(X), h(X) \in \mathbf{Z}_t[X]$. Assume that, for some $c \in \mathbf{Z}_t$, we have $F_{\mathbf{x}}(Y) = c$ identically. Then

$$\sum_{j=1}^{2k} (-1)^j g(x_j + X) \prod_{\substack{i=1 \\ i \neq j}}^{2k} h(x_i + X) = c \prod_{i=1}^{2k} h(x_i + X). \tag{6}$$

Let $\mathcal{Z}$ be the set of zeros of $h(X)$. Since f is not a polynomial, we have $\mathcal{Z} \neq \varnothing$. We now define the difference set

$$\mathcal{W} = \{z_1 - z_2 : z_1, z_2 \in \mathcal{Z}\}$$

(note that $0 \in \mathcal{W}$).

Assume that there exist some elements x_ν such that $x_\nu - x_i \notin \mathcal{W}$ for all $i \neq \nu$, $1 \leq i \leq 2k$. Then, taking arbitrary $z \in \mathcal{Z}$ and specializing

X as $x = z - x_\nu$, we see that all terms in (6) vanish for $j \neq \nu$, and we obtain

$$(-1)^\nu g(z) \prod_{\substack{i=1\\ i\neq\nu}}^{2k} h(x_i - x_\nu + z) = 0$$

that contradicts either the co-primality of $g(X)$ and $h(X)$ or the choice of x_ν.

Now assume that, for every $j = 1, \dots, 2k$, there exist $i \neq \nu$, $1 \le i \le 2k$ with $x_j - x_i \in \mathcal{W}$. We consider the graph $\mathcal{G}$ on $2k$ vertices where we connect the vertices i and j if and only if $x_j - x_i \in \mathcal{W}$. By our assumption, each connected component contains at least 2 vertices; thus, $\mathcal{G}$ has at most k connected components. Specializing x_j for any $j = 1, \dots, 2k$ leads to at most $(\#\mathcal{W})^{2k}$ possibilities for any elements x_i with i from the same component with j. So, for every such graph $\mathcal{G}$, there are at most $O(t^s)$ vectors $\mathbf{x} = (x_1, \dots, x_{2k}) \in \mathbf{Z}_t^{2k}$ which correspond to $\mathcal{G}$, where $s \le k$ is the number of connected components of $\mathcal{G}$. Since there are $O(1)$ possible graphs $\mathcal{G}$ on $2k$ vertices, the result follows. ◻

3. Main results. We start with the case of small values of t.

Theorem 3. *For any $\varepsilon > 0$, there exists some $\eta > 0$ such that for and $\vartheta \in \mathbf{F}_p^*$ of prime multiplicative order $t \ge p^\varepsilon$ and a rational function $f(X) \in \mathbf{Z}_t(X)$ that is not a polynomial, we have*

$$S_p(a; f) \ll tp^{-\eta}$$

where the implied constant depends only upon $\deg f$ *and ε.*

Proof. For any integer $k \ge 2$,

$$S_p(a; f)^k = \sum_{x_1, \dots, x_k \in \mathcal{X}_f} \mathbf{e}_p\left(a \sum_{j=1}^{k} \vartheta^{x_j}\right) \mathbf{e}_t\left(\sum_{j=1}^{k} f(x_j)\right).$$

Now, for each $u = 0, \dots, p-1$, we collect together the terms with

$$\vartheta^{x_1} + \dots + \vartheta^{x_k} \equiv u \pmod p,$$

getting

$$|S_p(a;f)|^k \le \sum_{u=0}^{p-1} \Bigg| \sum_{\substack{x_1,\dots,x_k\in\mathcal{X}_f \\ \vartheta^{x_1}+\dots+\vartheta^{x_k}\equiv u \pmod p}} \mathbf{e}_t\Big(\sum_{j=1}^{k} f(x_j)\Big)\Bigg|.$$

Next, by the Cauchy inequality, we derive

$$\begin{aligned}|S_p(a;f)|^{2k} &\le p\sum_{u=0}^{p-1} \Bigg| \sum_{\substack{x_1,\dots,x_k\in\mathcal{X}_f* \\ \vartheta^{x_1}+\dots+\vartheta^{x_k}\equiv u \pmod p}} \mathbf{e}_t\Big(\sum_{j=1}^{k} f(x_j)\Big)\Bigg|^2 \\ &= p\sum_{(x_1,\dots,x_{2k})\in\mathcal{W}_{f,k}} \mathbf{e}_t\Big(\sum_{j=1}^{2k}(-1)^j f(x_j)\Big),\end{aligned}$$

where the outside summation is taken over the set of vectors

$$\begin{aligned}\mathcal{W}_{f,k} = \{&(x_1,\dots,x_{2k}) \in (\mathcal{X}_f)^{2k} : \\ &\vartheta^{x_1}+\dots+\vartheta^{x_{2k-1}} \equiv \vartheta^{x_2}+\dots+\vartheta^{x_{2k}} \pmod p\}.\end{aligned}$$

Now, for $y \in \mathbf{Z}_t$, we have

$$\begin{aligned}&\sum_{(x_1,\dots,x_{2k})\in\mathcal{W}_{f,k}} \mathbf{e}_t\Big(\sum_{j=1}^{2k}(-1)^j f(x_j)\Big) \\ &\qquad = \sum_{(x_1+y,\dots,x_{2k}+y)\in\mathcal{W}_{f,k}} \mathbf{e}_t\Big(\sum_{j=1}^{2k}(-1)^j f(x_j+y)\Big).\end{aligned}$$

Since

$$\vartheta^{x_1+y}+\dots+\vartheta^{x_{2k-1}+y} \equiv \vartheta^{x_2+y}+\dots+\vartheta^{x_{2k}+y} \pmod p$$

is equivalent to

$$\vartheta^{x_1}+\dots+\vartheta^{x_{2k-1}} \equiv \vartheta^{x_2}+\dots+\vartheta^{x_{2k}} \pmod p,$$

averaging over all $y \in \mathbf{Z}_t$ and changing the order of summation, we obtain

$$
\begin{aligned}
|S_p(a;f)|^{2k} &\le \frac{p}{t}\left|\sum_{y\in\mathbf{Z}_t}\ \sum_{(x_1+y,\ldots,x_{2k}+y)\in\mathcal{W}_{f,k}} \mathbf{e}_t\left(\sum_{j=1}^{2k}(-1)^j f(x_j+y)\right)\right| \\
&\le \frac{p}{t} \sum_{\substack{x_1,\ldots,x_{2k}\in\mathbf{Z}_t\\ \vartheta^{x_1}+\ldots+\vartheta^{x_{2k-1}}\equiv\vartheta^{x_2}+\ldots+\vartheta^{x_{2k}} \pmod p}} \\
&\qquad\qquad \left|\sum_{y\in\mathbf{Z}_t}{}^{*}\mathbf{e}_t\left(\sum_{j=1}^{2k}(-1)^j f(x_j+y)\right)\right|,
\end{aligned}
$$

where Σ^* indicates that the poles of the function in the exponent are excluded.

For $O(t^k)$ vectors $\mathbf{x} = (x_1,\ldots,x_{2k}) \in \mathcal{W}_{f,k}$ such that the rational function $F_{\mathbf{x}}(X)$, given in Lemma 2, is constant, we estimate the sum over y trivially by t. Hence, we see that the total contribution from such vectors is $O(t^{k+1})$.

Now, for the remaining $(x_1,\ldots,x_{2k}) \in \mathcal{W}_{f,k}$, recalling that t is prime and using the Weil bound of exponential sums with rational function, (for example, in the form given in [**11**]), we estimate the sum over y by $O(t^{1/2})$. We see from Lemma 1 and bound (3) that, for a sufficiently large k, depending only upon ε,

$$
\#\mathcal{W}_{f,k} = \frac{t^{2k}}{p} + O(t^{2k-1}p^{-\delta(2k-2)}) \ll \frac{t^{2k}}{p}, \tag{7}
$$

where the implied constants depend only upon k.

Hence, we see that the total contribution from such vectors is

$$
O(\#\mathcal{W}_{f,k}t^{1/2}) = O(t^{2k+1/2}/p).
$$

Therefore,

$$
|S_p(a;f)|^{2k} \ll \frac{p}{t}(t^{k+1} + t^{2k+1/2}/p) \ll pt^k + t^{2k-1/2}. \tag{8}
$$

Finally, we also assume that k is such that $p \le t^{k-1}$, which after the substitution in (8), concludes the proof. □

We now obtain an explicit bound in the case of large values of t.

Theorem 4. *For any $\vartheta \in \mathbf{F}_p^*$ of prime multiplicative order $t \ge p^{2/3}$ and rational function $f(X) \in \mathbf{Z}_t(X)$, we have*

$$S_p(a; f) \ll t^{7/8}.$$

Proof. We assume that the rational function f is not a constant or linear polynomial modulo t as otherwise the result is immediate from (1).

We now proceed as in the proof of Theorem 3. In particular, we assume that the rational function f is non-constant modulo t as otherwise the result is immediate from (1). We choose $k = 2$ and, instead of (7), we use the bound

$$\#\mathcal{W}_{f,k} \ll \frac{t^4}{p} + pt,$$

which follows from the inequality (1) combined with Lemma 1. Furthermore, since $t \ge p^{2/3}$, these estimates simplify as

$$\#\mathcal{W}_{f,k} \ll \frac{t^4}{p}$$

which is a full analog of (7).

Since, by our assumption, f is not a constant or linear polynomial modulo t, we also remark that, for $x_1 \not\equiv x_2 \pmod t$, the rational function

$$F_{x_1,x_2}(Y) = f(x_2 + Y) - f(x_1 + Y) \in \mathbf{Z}_t[Y]$$

is not constant in $\mathbf{Z}_t$, provided that t is large enough.

Therefore, with $k = 2$ the bound (8) becomes

$$|S_p(a; f)|^4 \ll pt^2 + t^{7/2}. \tag{9}$$

Finally, since $t \ge p^{2/3}$, we have $pt^2 \le t^{7/2}$ and the result follows. □

It is also clear that, for intermediate values of $t \in [p^{1/4}, p^{2/3}]$, using (2) in full generality and also the results of [**9**] (rather than just (1) as in the proof of Theorem 4), one can get a series of other explicit estimates.

Note that, taking $k = 4$ and $\ell = 8$ in [**14**, Theorem 3.1], in the case of $f(X) = b/X$ and $t = p^{1+o(1)}$ (that is, for t which is close to its largest possible value), we obtain the bound

$$|S_p(a; f)| \le t^{127/128+o(1)}, \qquad \gcd(a,p) = 1,$$

and, with an even larger exponent for smaller values of t, however, these bounds apply to composite t as well.

4. Remarks. We have already mentioned that, in principle, our method works for composite values of t. All necessary tools are provided by the result of Cochrane and Zheng [**6**], which can be used instead of the Weil bound. On the other hand, the approach of this work does not seem to extend to the sums of multiplicative characters

$$T_{p,\chi}(a; f) = \sum_{x=1}^{t} \chi(\vartheta^x + a)\mathbf{e}_t(f(x))$$

and some other related sums to which the method of [**14**] applies, see [**14**, Section 4] for an outline of such possible extensions.

Finally, we note that the proof of Theorem 3 does not apply to polynomials $f(X) \in \mathbf{Z}_t[X]$ as if $2k > \deg f$ then, the function $F_{x_1,\ldots,x_{2k}}(Y)$ may also vanish on some vectors $(x_1, \ldots, x_{2k})$ of the second type. However, in this case the approach of [**1**] applies, which is in fact an adaptation of the *Weyl method* (see [**8**, Section 8.2]). Indeed, squaring $|S_p(a; f)|$, we derive

$$\begin{aligned} |S_p(a; f)|^2 &= \sum_{x,y=1}^{t} \mathbf{e}_p(a(\vartheta^x - \vartheta^y))\mathbf{e}_t(f(x) - f(y)) \\ &= \sum_{x,y=1}^{t} \mathbf{e}_p(a(\vartheta^x - \vartheta^{x+y}))\mathbf{e}_t(f(x) - f(x+y)) \\ &= \sum_{y=1}^{t}\sum_{x=1}^{t} \mathbf{e}_p(a(1 - \vartheta^y)\vartheta^x)\mathbf{e}_t(f(x) - f(x+y)). \end{aligned}$$

The sum over x is of the same type as the initial sum, besides that, for every y, the polynomial $f(X) - f(X+y)$ is of lower degree than $f(X)$.

Thus, an inductive argument applies, see the proof of [**1**, Lemma 1], which corresponds to the case $t = p - 1$. For a large prime t this, however, leads to a much weaker bound than that of Theorem 4, but instead it works in many cases to which Theorem 4 does not apply.

Acknowledgments. The author is very grateful to the referee for the very careful reading of the manuscript and finding a gap in the initial argument.

REFERENCES

1. W.D. Banks and I.E. Shparlinski, *Exponential sums with polynomial values of the discrete logarithm*, Uniform Distrib. Theory **2** (2007), 67–72.

2. J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. Funct. Anal. **18** (2009), 1477–1502.

3. J. Bourgain, A.A. Glibichuk and S.V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. **73** (2006), 380–398.

4. J. Bourgain and I.E. Shparlinski, *Distribution of consecutive modular roots of an integer*, Acta Arith. **134** (2008), 83–91.

5. T. Cochrane and C. Pinner, *Explicit bounds on monomial and binomial exponential sums*, Quart. J. Math. **62** (2011), 323–349.

6. T. Cochrane and Z.Y. Zheng, *Exponential sums with rational function entries*, Acta Arith. **95** (2000), 67–95.

7. D.R. Heath-Brown and S.V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. **51** (2000), 221–235.

8. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.

9. S.V. Konyagin, *Bounds of exponential sums over subgroups and Gauss sums*, Moscow Lomonosov State Univ., Moscow, 2002 (in Russian).

10. N.M. Korobov, *The distribution of non-residues and of primitive roots in recurrence series*, Dokl. Akad. Nauk. **88** (1953), 603–606 (in Russian).

11. C.J. Moreno and O. Moreno, *Exponential sums and Goppa codes*, 1, Proc. Amer. Math. Soc. **111** (1991), 523–531.

12. I.E. Shparlinski, *On bounds of Gaussian sums*, Mat. Z. **50** (1991), 122–130 (in Russian).

13. ———, *Cryptographic applications of analytic number theory*, Birkhauser, New York, 2003.

14. ———, *Exponential sums with consecutive modular roots of an integer*, Quart. J. Math. **62** (2011), 207–213.

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
Email address: igor.shparlinski@mq.edu.au