Open Problems on Exponential and Character Sums

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

May 4, 2016

1 Introduction

This is a collection of mostly unrelated open questions, at various levels of difficulty, related to exponential and multiplicative character sums. One may certainly notice a large proportion of self-references in the bibliography. By no means should this be considered as an indication of anything else than the fact that the choice of problems reflects the taste and interests of the author. Thus it is not surprising that many (but not all) of the problems are related to some previous results of the author.

One can find the necessary background and a wealth of information about exponential and character sums in [95] (mainly in the context of finite fields) and in [85] (in a more general contexts), see also [91, 93, 117, 137].

Some of the problems below are likely to be very difficult, some may constitute a feasible long term project (such as doctoral thesis), some are not so hard and may be used by the beginners in this area as an entry point to gain some immediate "hands-on" experience with exponential and character sums. In particular, part of the motivation for writing this list of problems has been the frequent requests to the author to suggest a research problem on exponential sums.

One can also notice that most of the problems fall into two major categories. In one category we talk about obtaining new bounds of exponential

and character sums, while in the other category we seek new applications. Often problems from the first group are motivated by a problem from the second group. Besides in Section 3.14 we present some other problems, which, at least the first glance, have nothing to do with exponential or character sums.

As a general rule, the well known problems, which are described in the literature, are not presented. We have also avoided open ended problems of the form "*Improve the result of ...*" unless we are able to give some ideas about how it may be possible to achieve this.

2 Notation

For an integer $m \ge 1$, we denote

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

We always follow the convention that arithmetic operations in the arguments of $\mathbf{e}_m$ are performed modulo m.

We use (n/m) to denote the Jacobi symbol modulo an odd integer $m \ge 3$ (that is, the Legendre symbol in that case that $m = p$ is prime).

The letter p (possibly subscripted) always denotes a prime; k, m and n always denote integers (and so do K, M and N).

As usual, we say that $n \ge 2$ is y-smooth is all prime divisors p of n satisfy $p \le y$.

We use ε to denote a small positive parameter on which implied constants may depend.

Calligraphic letters, for example, $\mathcal{A} = (a_n)$, usually denote sets or sequences of integers.

For a prime power q, we use $\mathbb{F}_q$ to denote the finite field of q elements.

For an integer m, we use $\mathbb{Z}_m$ to denote the residue ring modulo m.

We use some standard notations for most common arithmetic functions. For $m \ge 2$ be an integer, we denote by:

- $P(m)$ the largest prime divisor of m,
- $\varphi(m)$ the Euler (totient) function of m,
- $\omega(m)$ the number of distinct prime divisors of m,

- $\tau(m)$ the number of positive integer divisors of m.

We also define $P(1) = \omega(1) = 0$ and $\tau(1) = \varphi(1) = 1$.
Letting $x \geq 0$ be a real number, we denote by:

- $\pi(x)$ the number of primes $p \leq x$,
- $\pi(x; q, a)$ the number of primes $p \leq x$ such that $p \equiv a \pmod{q}$.

We use the Vinogradov notation '$f(x) \ll g(x)$' which is equivalent to the Landau notation $f(x) = O(g(x))$, but easier to chain as, for example, $f(x) \ll g(x) = h(x)$. If convenient, we also write $g(x) \gg f(x)$ instead of $f(x) \ll g(x)$. We also write $f(x) \asymp g(x)$ if $f(x) \ll g(x) \ll f(x)$.

Finally, $\log x$ denotes the natural logarithm; we always assume the argument is large enough for the whole expression to make sense (as well as in the case of iterated logarithms).

3 Problems

3.1 Exponential functions

Problem 1. Obtain analogues of the results of J. Bourgain, A. A. Glibichuk and S. V. Konyagin [35] for multiplicative character sums

$$\sum_{x_1,\ldots,x_k \in \mathcal{X}} \chi(x_1 \ldots x_k + a) \qquad \text{and} \qquad \sum_{x=1}^{N} \chi(g^x + a)$$

with very small values of N relative to p, where $\mathcal{X} \subseteq \mathbb{Z}_p$, $\gcd(g, p) = 1$ and χ is a nonprincipal multiplicative character modulo p, see also [22, 23, 24, 25, 27, 28, 30, ?].

Problem 2. Obtain explicit forms, with all constants explicitly evaluated, of the results of J. Bourgain [22, 23, 24, 25, 27, 28], J. Bourgain and M.-C. Chang [30], J. Bourgain, A. A. Glibichuk and S. V. Konyagin [35] and several other similar results on short exponential sums with exponential functions

$$\sum_{x=1}^{N} \mathbf{e}_m(a_1 g_1^x + \ldots + a_k g_k^x), \qquad \text{and} \qquad \sum_{x=1}^{M} \sum_{y=1}^{N} \mathbf{e}_m(a g^x + b g^y + c g^{xy}),$$

where $a_1, \dots, a_k, a, b, c \in \mathbb{Z}$, $\gcd(gg_1 \dots g_k, m) = 1$, $M, N \in \mathbb{Z}$, and with the products

$$\sum_{x_1 \in \mathcal{X}_1} \dots \sum_{x_k \in \mathcal{X}_k} \mathbf{e}_m(ax_1 \dots x_k), \qquad a \in \mathbb{Z},$$

where $\mathcal{X}_1, \dots, \mathcal{X}_k \subseteq \mathbb{Z}_m^*$.

Comments: *J. Bourgain and M. Z. Garaev [?] and M.-C. Chang and C. Z. Yao [45] have recently obtained a series of very interesting results in this direction.*

Problem 3. Obtain stronger bounds for the sums of Problem 2 on average over prime moduli $m = p$.

Comments: *The ideas used in the proof of [91, Theorem 5.5] and of [5, Lemma 2.10] can possibly be of help.*

Problem 4. Use the method of [91, Chapter 5] to estimate exponential sums

$$\sum_{x=1}^{N} \mathbf{e}_m(ag^x), \qquad a \in \mathbb{Z},$$

where $\gcd(g, m) = 1$, for very small values of N relative to m, for "almost all" m.

Comments: *There are amazingly strong and general results of J. Bourgain and M.-C. Chang, see [24, 25, 30], which apply to very short and general sums and thus have significantly reduced the interest to this question. On the other hand, the method of [91, Chapter 5] may lead to more explicit and stronger bounds (but which hold only for "almost all" m rather than all m).*

Problem 5. Estimate exponential sums

$$\sum_{x=1}^{T} \mathbf{e}_p\left(ag^{x^2} + bg^x\right), \qquad a, b \in \mathbb{Z},$$

where T is a multiplicative order of g modulo p with $\gcd(g, p) = 1$.

Comments: *J. Bourgain [27] has obtained a nontrivial estimate for a large class of primes p, but in the general case there is no nontrivial bound (even if g is a primitive root modulo p). In the case of $b = 0$ these sums are estimated in [64], provided $T \ge p^{1/2+\varepsilon}$, see also [68, 96]. Bounds of similar sums with a composite denominator m can be found in [67].*

Problem 6. Estimate exponential sums

$$\sum_{x=1}^{N} \mathbf{e}_m\left(ag^{\lfloor f(x)\rfloor}\right), \qquad a \in \mathbb{Z},$$

where $f(X) \in \mathbb{R}[X]$ is a polynomial with real coefficients or some sufficiently smooth function.

Comments: *In the case of polynomials $f(X) \in \mathbb{Z}[X]$ with integers coefficients and prime $m = p$ such that $\ell^2 \mid p-1$ for another prime $\ell \ge p^{\varepsilon}$ (with arbitrary $\varepsilon > 0$) a nontrivial bound on the above sums are given by M.-C. Chang [41]. Also for $f(X) \in \mathbb{Z}[X]$ and prime $m = p$, in [122], a nontrivial bound is given "on average" over all primitive roots g modulo p. In fact in both [41] and [122] more general sums over arbitrary finite fields are estimated. The general case of polynomials, even for polynomials $f(X) \in \mathbb{Z}[X]$, probably requires some new ideas. On the other hand, the case of smooth and slowly growing functions $f(X)$ can probably be studied by the method of [16]. Results of these type have a natural interpretation of studying polynoially growinng sequences on orbits of the dynamical system generated by the map $u \to gu$ in the ring $\mathbb{Z}_m$, see [17, 69, 70] and references therein for various results of similar flavour in the settings of ergodic theory.*

Problem 7. Estimate incomplete exponential sums

$$\sum_{\substack{x=1\\ \gcd(x,T)=1}}^{N} \mathbf{e}_m\left(ag^{1/x}\right), \qquad a \in \mathbb{Z},$$

where T is a multiplicative order of g modulo m with $\gcd(g,m) = 1$.

Comments: *For a prime $m = p$ and $T \ge p^{\varepsilon}$ this has been done by J. Bourgain and I. E. Shparlinski [38], a more explicit estimate in the case of $T \ge p^{1/2+\varepsilon}$ is given in [125], see also [110, 129] for several more related results.*

Problem 8. Estimate complete exponential sums

$$\sum_{\substack{x=1\\ \gcd(x,T)=1}}^{T} \mathbf{e}_m\left(ag^{x} + bg^{1/x}\right), \qquad a, b \in \mathbb{Z},$$

where T is a multiplicative order of g modulo m with $\gcd(g,m) = 1$.

Comments: *Even the case of prime $m = p$ is of interest. Also, for a prime $m = p$, some bounds on average over $a, b \in \mathbb{F}_p$ are given in [119].*

3.2 Short character sums

Problem 9. Extend the Burgess bound, see [85, Theorems 12.6], in full generality, to the settings of arbirary finite fields.

Comments: *Very promising results in this direction have recently been obtained by J. Bourgain and M.-C. Chang [31], M.-C. Chang [42, 43] and S. V. Konyagin [90].*

Problem 10. For a prime p and integer $n \geq 2$, estimate character sums

$$\sum_{x=1}^{h} \chi(\alpha + x)$$

for $h \leq p^{1/2} \log p$, where χ is a multiplicative character of $\mathbb{F}_{p^n}$ α is such $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$.

Comments: *In [111] the above sums have been estimated as $O(np^{1/2} \log p)$ with an absolute implied constant has been used in [42]. Its any improvement with lead to new results in Problem 9.*

Problem 11. Prove that

$$\max_{0 \leq a < b \leq p-1} \left| \sum_{x=1}^{h} \left(\frac{(x+a)(x+b)}{p} \right) \right| = o(h)$$

for any $h \geq p^{\alpha}$ with some fixed $\alpha < 1/2$.

Comments: *V. Shoup [114] gives a factorization algorithm for polynomials over $\mathbb{F}_p$ of complexity $O(n^{2+o(1)}p^{1/2+o(1)})$ (where n is the degree of the polynomial $f(X) \in \mathbb{F}_p[X]$ to be factored), which is based on the Weil bound*

$$\max_{0 \leq a < b \leq p-1} \left| \sum_{x=1}^{h} \left(\frac{(x+a)(x+b)}{p} \right) \right| = O\left(p^{1/2} \log p\right).$$

Any improvement of this bound immediately leads to a better complexity estimate. Even obtaining such a bound only for "almost all" p is already of great interest.

Problem 12. Extend the result and method of A. A. Karatsuba [88] to double character sums modulo a composite.

Problem 13. Estimate sums with Jacobi symbols over the solutions to the congruence $xy \equiv a \pmod m$ in a given box, that is,

$$\sum_{\substack{xy \equiv a \pmod m \\ 1 \le x \le X, 1 \le y \le Y \\ y \equiv 1 \pmod 2}} \left(\frac{x}{y}\right), \qquad a \in \mathbb{Z},$$

for X and Y reasonably small compared to m.

Comments: *For very small m some results of this kind can be extracted from the work of G. Yu [140], see also [139] for applications of results of this kind to studying the distribution of Selmer groups of some families of elliptic curves.*

Problem 14. Assuming the *Generalised Riemann Hypothesis*, estimate the sums

$$S_m(\chi, N) = \sum_{n=1}^{N} \chi(n)$$

with a nontrivial multiplicative character χ modulo m.

Comments: *The bound $S_m(\chi, N) = N^{1/2} m^{o(1)}$ has been a part of folklore and in particular is quoted in [99, Bound (13.2)] as a consequence of the weaker Generalised Lindelöf Hypotheis. One can also derive it from [80, Theorem 2]. However, it is interesting to get an explicit expression for the term $m^{o(1)}$.*

3.3 Smooth numbers, S-units and primes

Problem 15. Estimate exponential and multiplicative character sums

$$\sum_{\substack{n \le x \\ n \text{ is } y\text{-smooth}}} \mathbf{e}_m\left(f(n)\right) \qquad \text{and} \qquad \sum_{\substack{n \le x \\ n \text{ is } y\text{-smooth}}} \chi(f(n))$$

with a polynomial $f(T) \in \mathbb{Z}[T]$, where $a \in \mathbb{Z}$ and χ is a multiplicative character modulo m.

Comments: *Several bounds for exponential sums over smooth numbers are given by É. Fouvry and G. Tenenbaum [62] and, more recently, by R. de la Bretèche and G. Tenenbaum [39]. Character sums in the case of a linear polynomial $f(T) = T - a$ are estimated [121]. The approach of [121] has also been used by K. Gong [78] for more general sums. The arguments of [39, 62] and [78, 121] are quite different and it is quite possible that combining them, or using them in different scenarious, one can obtain many new interesting results about exponential and character sums over y-smooth integers in wide ranges of the parameters m, x and y.*

Problem 16. For a set $\mathcal{S} = \{p_1, \ldots, p_s\}$ of s primes and an integer N we denote by $\mathcal{U}(\mathcal{S}, N)$ the set of integer S-units up to N, that is, the set of integers $u \le N$ composed out of primes from the set $\mathcal{S}$. Estimate character sums

$$U_k(\mathcal{S}, N) = \sum_{u_1, \ldots, u_k \in \mathcal{U}(\mathcal{S}, N)} \chi\left(a_1 u_1 + \ldots + a_k u_k\right), \qquad a_1, \ldots, a_k \in \mathbb{Z},$$

and

$$W_k(\mathcal{S}, N) = \sum_{u_1, \ldots, u_k \in \mathcal{U}(\mathcal{S}, N)} \chi\left(a_1 u_1 + \ldots + a_k u_k + 1\right), \qquad a_1, \ldots, a_k \in \mathbb{Z},$$

with a multiplicative character χ modulo m.

Comments: *In the case $s = k = 1$ the sums $W_k(\mathcal{S}, N)$ are estimated by E. Dobrowolski and K. S. Williams [55] and H. B. Yu [141] (in fact in this case the only generator p_1 need not be prime. Note that we ask for estimates which make use of larger values of s or k in a substantial way rather than merely reduce the question to the case $s = k = 1$. There should be a strong connection between estimates on $U_{k+1}(\mathcal{S}, N)$ and $W_k(\mathcal{S}, N)$.*

Problem 17. In the case of a positive solution to Problem 16 use its result together with the square sieve of D. R. Heath-Brown [81] to estimate the number of perfect squares of the form

$$u_1 + \ldots + u_k \qquad \text{and} \qquad \frac{w_1 - 1}{w_2 - 1}$$

where $u_1, \ldots, u_k, w_1, w_2 \in \mathcal{U}(\mathcal{S}, N)$ and similar.

Comments: *The question is related to some finiteness conjectures about the number of perfect squares and higher powers of the above and similar types made by P. Corvaja [53]. As for Problem 38, only sums with the Jacobi symbol modulo products of two distinct primes $m = p_1p_2$ are relevant.*

Problem 18. Make use of the Burgess bound, see [85, Theorems 12.6], in the argument of Z. Kh. Rakhmonov [112] in order to improve the bound [112] on the sums

$$\sum_{p \le N} \chi(p + a), \qquad a \in \mathbb{Z},$$

with an arbirary nontrivial multiplicative character χ modulo m, where $\gcd(a, m) = 1$. Obtain a result which is nontrivial for $N \ge m^{1-\alpha+\varepsilon}$ with some fixed $\alpha > 0$.

Comments: *Z. Kh. Rakhmonov [112] uses the Pólya–Vinogradov bound; accordingly, his estimate is nontrivial only for $N \ge m^{1+\varepsilon}$, see also a result of A. A. Karatsuba [87] for the case of prime modulus $m = p$ which is nontrivial starting with $N \ge p^{1/2+\varepsilon}$. For primitive characters such a result is given in [63], which is nontrivial for $N \ge m^{8/9+\varepsilon}$. Most certainly the method of [63] can be extended to all nontrivial characters but this has to be worked out in detail.*

3.4 Kloosterman sums

Problem 19. Obtain an explicit estimate of double Kloosterman sums

$$\sum_{k \in \mathcal{K}} \sum_{m \in \mathcal{M}} \alpha_k \beta_m \mathbf{e}_p \left(akm + bk^{-1}m^{-1}\right),$$

modulo a prime p, where $\mathcal{K} = [I, I + K]$ and $\mathcal{M} = [J, J + M]$ are intervals of lengths K and M, satisfying

$$KM \ge p^{1/2+\delta}$$

for a fixed $\delta > 0$, and α_k and β_m are some complex numbers with

$$|\alpha_k| \le 1, \ k \in \mathcal{K}, \qquad \text{and} \qquad |\beta_m| \le 1, \ m \in \mathcal{M}.$$

Comments: *A bound of such sum in the above range has been given by J. Bourgain [21, Theorem A.1] with some power saving $p^{-\eta}$ over the trivial bound, where $\eta > 0$ depends on δ, however the dependence of η on δ has not been made explicit.*

Problem 20. Estimate Kloosterman sums over squarefree and smooth numbers

$$\sum_{\substack{s\le N\\ s\,\text{squarefree}}} \mathbf{e}_m(as^{-1}+bs), \qquad \text{and} \qquad \sum_{\substack{s\le N\\ s\,y-\text{smooth}}} \mathbf{e}_m(as^{-1}+bs)$$

modulo an arbitrary integer m.

Comments: *To estimate the sum over square free numbers one can use the inclusion principle in a very straight forward fashion. However we ask about a more an argument that goes beyond this approach. For a prime denominator $m = p$, a bound on Kloosterman sums over primes*

$$S_m(a,b) = \sum_{\substack{\ell\le N\\ \ell\,\text{prime}}} \mathbf{e}_m(a\ell^{-1}+b\ell),$$

has been given by É. Fouvry and Ph. Michel [60] and in a wider range (but in a less explicit form by J. Bourgain [21]. The result of M. Z. Garaev [71] has improved the result of [60] for $b = 0$. It has been shown in [61] that the method of M. Z. Garaev [71] also works for composite moduli m and can be further improved on average over m. Finally, R. C. Baker [4] obtained a fully explicit version of a result of [21] (for $b = 0$) and extended it from prime denominators to a much larger class of moduli, including all squarefree intgers. R. C. Baker [4] also improved the estimate of [61] about the bound of the sums $S_m(a,b)$ on average over m. These results together with the Vaughan identity [138] can be used to estimate the sums over smooth numbers.

Problem 21. Find nontrivial bounds of the sums

$$\sum_{\substack{\ell\le N\\ \ell\,\text{prime}}} \chi(a\ell^{-1}+b\ell), \qquad \text{and} \qquad \sum_{\substack{s\le N\\ s\,y-\text{smooth}}} \chi(as^{-1}+bs)$$

with nontrivial multiplicative characters modulo an arbitrary integer m.

Comments: *See the references in the comments to Problems 18 and 20.*

3.5 Combinatorial sequences

Problem 22. Let $\mathcal{P}_L$ be that set of all palindromes of length L, that is, the set of n for which the base $g \geq 2$ representation

$$n = \sum_{k=0}^{L-1} a_k(n) g^k,$$

where

$$a_k(n) \in \{0, 1, \ldots, g-1\}, \ k = 0, 1, \ldots, L-1, \qquad \text{and} \qquad a_{L-1}(n) \neq 0,$$

satisfies the symmetry condition:

$$a_k(n) = a_{L-1-k}(n), \qquad k = 0, 1, \ldots, L-1.$$

Estimate exponential and character sums

$$\sum_{n \in \mathcal{P}_L} \mathbf{e}_m(f(n)) \qquad \text{and} \qquad \sum_{n \in \mathcal{P}_L} \chi(n),$$

where $f(X) \in \mathbb{Z}[X]$ and χ is a multiplicative character modulo m.

Comments: *W. Banks, D. Hart and M. Sakata [8] have used bounds of twisted Kloosterman sums to estimate exponential sums with palindromes in the case $f(X) = X$, see also [10]. However, the method of [8] does not seem to apply to either exponential sums with more general polynomials or character sums. Even the case of prime $m = p$ is still open.*

Problem 23. Obtain nontrivial upper bounds on exponential and character sums with factorials modulo a prime p, such as

$$\sum_{n=1}^{N} \mathbf{e}_p(an!) \qquad \text{and} \qquad \sum_{n=1}^{N} \chi(n! + a), \qquad a \in \mathbb{Z},$$

where χ is a multiplicative character modulo p.

Comments: *Double exponential sums with $m!n!$ and single multiplicative character sums as above with $a = 0$ are estimated in [72] and [73], respectively.*

Problem 24. Estimate double exponential sums with binomial coefficients

$$\sum_{n=0}^{N}\sum_{m=0}^{n}\mathbf{e}_p\left(a\binom{n}{m}\right), \qquad a \in \mathbb{Z},$$

for $0 \le N < p$.

Comments: *Several estimates of single and double exponential and character sums with binomial coefficients and other combinatorial numbers are given by M. Z. Garaev, F. Luca and I. E. Shparlinski in [72, 73, 74, 75].*

Problem 25. Estimate exponential sums

$$\sum_{n=1}^{N}\sum_{k=0}^{n}\mathbf{e}_m\left(as(n,k)\right) \qquad \text{and} \qquad \sum_{n=1}^{N}\sum_{k=0}^{n}\mathbf{e}_m\left(aS(n,k)\right), \qquad a \in \mathbb{Z},$$

with Stirling numbers of the first and second kind, respectively.

Problem 26. Estimate exponential sums

$$\sum_{2\le n\le x}\mathbf{e}_n\left(aw_n\right) \qquad \text{and} \qquad \sum_{2\le n\le x}\mathbf{e}_{P(n)}\left(aw_n\right), \qquad a \in \mathbb{Z},$$

where $w_1 = 1$ and

$$w_n = \binom{2n-1}{n-1} = \frac{1}{2}\binom{2n}{n}, \qquad n \ge 2.$$

Comments: *This question has also been posed in [40].*

Problem 27. Obtain nontrivial upper bounds on exponential and character sums with n^n modulo an integer m, such as

$$\sum_{n=1}^{N}\mathbf{e}_m\left(an^n\right) \qquad \text{and} \qquad \sum_{n=1}^{N}\chi\left(n^n+a\right), \qquad a \in \mathbb{Z},$$

where χ is a multiplicative character modulo m.

Comments: *Probably the case of prime $m = p$ and the range $N = p-1$ is of most interest. In this case the bound $O\left(p^{48/25+o(1)}\right)$ of [3] on the number*

of solutions to the congruence $k^k \equiv n^n \pmod p$, $1 \le k, n < p$, *is equivalent to the estimate of the average values*

$$\frac{1}{p}\sum_{a=1}^{p}\left|\sum_{n=1}^{p-1}\mathbf{e}_m\left(an^n\right)\right|^2 \le p^{48/25+o(1)}$$

and

$$\frac{1}{p}\sum_{a=1}^{p}\left|\sum_{n=1}^{p-1}\chi\left(n^n+a\right)\right|^2 \le p^{48/25+o(1)}.$$

3.6 Polynomial discriminants

Problem 28. Estimate exponential and character sums

$$\sum_{\substack{\deg f=n,\ H(f)\le H\\ f\in\mathbb{Z}[X]\ \text{monic}}}\mathbf{e}_m\left(aD(f)\right) \qquad \text{and} \qquad \sum_{\substack{\deg f=n,\ H(f)\le H\\ f\in\mathbb{Z}[X]\ \text{monic}}}\chi\left(D(f)\right),$$

with $a \in \mathbb{Z}$ and nontrivial multiplicative characters χ modulo m over discriminants $D(f)$ of monic polynomials

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$$

of degree n and height $H(f) = \max\{|a_0|, \ldots, |a_{n-1}|\} \le H$.

Comments: *Certainly the determinant is a polynomials of degree* n *in the coefficients* $a_0, \ldots, a_{n-1}$. *So many general estimates for exponential and character sums with polynomials can be applied. For example, for a prime* $m = p$, *an immediate application of the Weil bound implies that for* $H \le p$ *each of the above sums is* $O(H^{n-1}p^{1/2}\log p)$. *Certainly only estimates which are better than such bounds and makes use some special properties of* $D(f)$ *are of interest. We also recall that if* $f \in \mathbb{F}_p[X]$ *is squarefree then by the Stickelberger theorem, see [18, Theorem 6.68]*

$$\left(\frac{D(f)}{p}\right) = (-1)^{n-s},$$

where $n = \deg f$ *and* s *is the number of distinct irreducible factors of* f. *Therefore if* χ *is the Legendre symbol then the corresponding sum is a polynomial analogue of the sum of Möbius function.*

Problem 29. Estimate double character sums

$$\sum_{n=1}^{N} \sum_{k=1}^{n-1} \chi\left(\Delta(n,k)\right),$$

for a nontrivial multiplicative character modulo m, where

$$\Delta(n,k) = (-1)^{n(n-1)/2}\left(n^n - (-1)^n k^k (n-k)^{n-k}\right)$$

is the discriminant of the trinomial $X^n + X^k + 1$.

Comments: *The question is of interest for even prime $m = p$, and especially for $m = p_1 p_2$ which is a product of two primes since in this case one can use the square sieve of D. R. Heath-Brown [81] to study the squarefree part of $\Delta(n,k)$, see [100, 124] for some related problems about the discriminants of trinomials. If such a bound is obtained then again the Stickelberger theorem, see the comments to Problem 28 can be used to extract some nontrivial information about factorisations of trinomials.*

3.7 Arithmetic functions

Problem 30. Estimate exponential sums with the divisor function

$$\sum_{n=1}^{N} \mathbf{e}_m(a\tau(n)), \qquad a \in \mathbb{Z},$$

for an odd $m \geq 3$.

Comments: *One can use the fact that "typically" $\tau(n) = 2^k a$ for a small a and rather large k. Then one can try to use bounds of exponential sums with exponential function from [22, 23, 24, 25, 27, 28, 30, ?, 35, 91]. In fact the case of $m = p^k$ where p is fixed can be a good starting point where one can use the result of N. M. Korobov [92] for the relevant exponential sums.*

Problem 31. Estimate exponential and character sums with the largest squarefree divisor of n and with the squarefree part of n, that is,

$$\sum_{n=1}^{N} \mathbf{e}_m(aQ(n)) \qquad \text{and} \qquad \sum_{n=1}^{N} \mathbf{e}_m(aS(n)), \qquad a \in \mathbb{Z},$$

where

$$Q(n) = \prod_{p \mid n} p \qquad \text{and} \qquad S(n) = \min\{s \ : \ \sqrt{n/s} \in \mathbb{Z}\}.$$

Comments: *Bounds of character sums with these functions are given by H. Liu and W. Zhang [97], but the method of [97] does not apply to exponential sums. Exponential sums with $P(n)$ have been estimated in [7]; exponential and character sums with the Euler function are estimated in [2, 9, 13].*

Problem 32. For an integer $g > 1$ estimate exponential sums

$$\sum_{\substack{n=1\\ n \text{ composite}}}^{N} \mathbf{e}_n\left(a(g^{n-1}-1)\right), \qquad a \in \mathbb{Z}.$$

Comments: *This question has also been posed in [5] where one can also find estimates of some other related sums with fractions $(g^{n-1}-1)/n$ and alike.*

3.8 Beatty sequences

Problem 33. Extend the bounds of character sums with Beatty sequences $\lfloor \alpha n + \beta \rfloor$ of W. D. Banks and I. E. Shparlinski [11, 12] to composite moduli.

Problem 34. Obtain explicit versions of the bounds of character sums with Beatty sequences $\lfloor \alpha n + \beta \rfloor$ of W. D. Banks and I. E. Shparlinski [15] in the case when α is of approximation type 1.

Problem 35. Estimate character sums with Beatty sequences $\lfloor \alpha p + \beta \rfloor$ over primes $p \le x$.

Problem 36. Estimate character sums with Beatty sequences $\lfloor \alpha s + \beta \rfloor$ over y-smooth integers $s \le x$.

Problem 37. Estimate double character sums with Beatty sequences

$$\sum_{k \in \mathcal{K}} \sum_{m \in \mathcal{M}} \chi\left(\lfloor \alpha(k+m) + \beta \rfloor\right)$$

on sumsets, where χ is a multiplicative character modulo $m \ge 2$ and $\mathcal{K}$ and $\mathcal{M}$ are sufficiently dense sets of integers of the interval $[1, N]$. Even the case of $m = p$ and very large N is still open.

Problem 38. In the case of positive solutions to Problems 33 and 34 use their results together with the square sieve of D. R. Heath-Brown [81] in order to get a lower bound on the number of distinct quadratic fields of the form $\mathbb{Q}\left(\sqrt{\lfloor \alpha n + \beta \rfloor}\right)$, $n = 1, \ldots, N$.

Comments: *Only sums with the Jacobi symbol modulo products of two distinct primes $m = p_1p_2$ are relevant.*

Problem 39. Extend the bounds of multiplicative character sums with integer parts $\lfloor f(n) \rfloor$ of "smooth" functions of W. D. Banks and I. E. Shparlinski [16] to composite moduli.

Problem 40. Estimate multiplicative character sums with integer parts $\lfloor f(n) \rfloor$ of a polynomial $f(X) \in \mathbb{R}[X]$.

Problem 41. In the case of a positive solution to Problem 39 use its result together with the square sieve of D. R. Heath-Brown [81] in order to get a lower bound on the number of distinct quadratic fields of the form $\mathbb{Q}\left(\sqrt{\lfloor f(n) \rfloor}\right)$, $n = 1, \ldots, N$.

Comments: *As for Problem 38, only sums with the Jacobi symbol modulo products of two distinct primes $m = p_1p_2$ are relevant.*

3.9 Sparse polynomials

Problem 42. Obtain analogues of the result of T. Cochrane, C. Pinner and J. Rosenhouse [48] on exponential sums

$$\sum_{x=1}^{m} \mathbf{e}_m\left(a_1x^{k_1} + \ldots + a_sx^{k_s}\right), \qquad a_1, \ldots, a_s \in \mathbb{Z},$$

with sparse polynomials of large degree, containing only s monomials, modulo a composite $m \geq 2$.

Comments: *The result of T. Cochrane, C. Pinner and J. Rosenhouse [48] is a generalisation of the bound of S. V. Konyagin [89] which corresponds to the case $s = 1$. Extending the bound of [89] to composite moduli is already an interesting problem. The bound of [48] has been applied to various problems in number theory [10], computer science [130] and cryptography [131]. Several other bounds (stronger, but more restrictive on the class of polynomials to which they apply) on exponential sums with sparse polynomials can be found in [23, 29, 49, 116].*

Problem 43. Obtain analogues of the result of on bounds exponential sums with sparse polynomials (see Problem 42) for exponential sums along an along an algebraic curve

$$\sum_{f(x,y)\equiv 0 \pmod p} \mathbf{e}_p\left(a_1x^{k_1}y^{m_1} + \ldots + a_sx^{k_s}y^{m_s}\right), \qquad a_1, \ldots, a_s \in \mathbb{Z},$$

with a nontrivial polynomial f modulo a prime $p \geq 2$.

Comments: *In the case of dense polynomials in the exponent, such a bound is given in the celebrated work of E. Bombieri [20].*

Problem 44. Obtain bounds on exponential sums

$$\sum_{\substack{x=1\\ \gcd(g(x),m)=1}}^{m} \mathbf{e}_m\left(f(x)/g(x)\right),$$

with sparse rational functions $f(X)/g(X)$, where

$$f(X) = a_1X^{h_1} + \ldots + a_rX^{h_r} \qquad \text{and} \qquad g(X) = b_1X^{k_1} + \ldots + b_sX^{k_s},$$

which are better than general estimates of T. Cochrane and Z. Y. Zheng [50] depending only on the degrees of f and g, see also [51].

Problem 45. Use the bound of W. D. Banks, A. Harcharras and I. E. Shparlinski [6] on analogues of short Kloosterman sums with polynomials over finite fields to sharpen the Brun-Titchmarsh theorem over $\mathbb{F}_q[X]$, see [84].

Comments: *One may try to imitate the approach of J. B. Friedlander and H. Iwaniec [65].*

3.10 Analogues of Heilbronn sums

Problem 46. Estimate exponential sums with two types of Fermat quotients

$$\sum_{n\leq N} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j \frac{(n+j)^{p-1}-1}{p}\right)$$

and

$$\sum_{n\leq N} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j \frac{(n+j)^{p}-(n+j)}{p}\right).$$

where $\gcd(a_0, \ldots, a_{s-1}, p) = 1$.

Comments: *For $s = 1$, the first sums has been estimated by D. R. Heath-Brown [82] and D. R. Heath-Brown and S. V. Konyagin [83] and the second by A. Ostafe and I. E. Shparlinski [109]. For any s and $N \ge p^{1+\varepsilon}$ the first sum is also estimated in [109], but the case of $N \le p$ seems to be very difficult.*

Problem 47. Estimate exponential sums

$$\sum_{n \le N} \mathbf{e}_p\left(a\frac{n^{t_p(n)} - 1}{p}\right)$$

where $t_p(n)$ is the multiplicative order n modulo p.

Problem 48. Estimate multiplicative character sums

$$\sum_{\substack{n \le N \\ \gcd(n,p)=1}} \chi\left(\frac{n^{p-1} - 1}{p}\right) \qquad \text{and} \qquad \sum_{n \le N} \chi\left(\frac{n^p - n}{p}\right)$$

for $N \ge p^{1/2+\varepsilon}$, where χ is a multiplicative character modulo p.

Comments: *In [126] a nontrivial estimate on the first sum is given in the case of $N \ge p^{5/4+\varepsilon}$, see also [77]. M. C. Chang [44] has obtained an nontrivial estimate already for $N \ge p^{3/4+\varepsilon}$. The same approach also works for the second sum. However obtaining nontrivial estimates for $N \le p$ appears to be very difficult.*

Problem 49. Estimate multiplicative character sums

$$\sum_{n=1}^{p-1} \chi\left(n(n+1)\left(\frac{(n+1)^p - n^p - 1}{p}\right)\right),$$

where χ is a multiplicative character modulo a prime p.

Comments: *Despite a somewhat unattractive shape, these character sums appear naturally (at least for a quadratic character χ) in the study of the Shafarevich–Tate groups of the curves $Y^p = X^s(1 - X)$, see [94, 98].*

Problem 50. Estimate multiplicative character sums

$$\sum_{\substack{\ell \le N \\ \ell \ne p \text{ prime}}} \chi\left(\frac{\ell^{p-1} - 1}{p}\right) \qquad \text{and} \qquad \sum_{\substack{\ell \le N \\ \ell \text{ prime}}} \chi\left(\frac{\ell^p - \ell}{p}\right)$$

where χ is a multiplicative character modulo p, for $N \ge p^{1+\varepsilon}$,

Comments: *For $N \ge p^{3/2+\varepsilon}$ it is done in [44], see also [126, 127, 128], for some previous results via the Vaughan identity, see [85, Section 13.4], and estimates of bilinear character sums*

$$\sum_{\substack{m \le M \\ n \le N \\ \gcd(mn,p)=1}} \alpha_m \beta_n \chi\left(\frac{(mn)^{p-1}-1}{p}\right)$$

with arbitrary complex weights α_m and β_n, using the congruence

$$\frac{(mn)^{p-1}-1}{p} \equiv \frac{m^{p-1}-1}{p} + \frac{n^{p-1}-1}{p} \pmod p, \qquad \gcd(mn,p)=1.$$

3.11 Nonlinear recurrence sequences

Problem 51. For a given polynomial $f \in \mathbb{F}_q[X]$ and $u_0 \in \mathbb{F}_q$ we define the following sequence of elements of $\mathbb{F}_q$

$$u_n = f\left(u_{n-1}\right), \qquad n = 1, 2, \ldots.$$

Clearly this sequence eventually becomes periodic, that is, $u_{n+T} = u_n$ for some $T \ge 1$ whenever $n \ge N_0$. In fact, without loss of generality, one can assume that it is purely periodic, that is, $N_0 = 0$. Improve the bound of H. Niederreiter and A. Winterhof [105] on character sums

$$\sum_{n=1}^{N} \psi(au_n), \qquad a \in \mathbb{F}_q^*,$$

with a nontrivial additive character ψ of $\mathbb{F}_q$ and $N \le T$.

Comments: *The bound of [105] develops some ideas suggested in [136] and also improves the previous result of [101]; however it is still nontrivial only if T is very close to its largest possible value p. Even constructing some special (but general enough) families of polynomials for which such improvement is possible is of interest. In the multidimensional case (that is, for iterations of multivariate polynomials) such families are constructed in [107], see also [108]. Furthermore, A. Ostafe [106] has modified the construction of [107] in a way that the method of [103] applies to this constructions and*

has led to much better results "on average" over all initial values. Unfortunately the constructions of [106, 107, 108] do not work in the univariate case. This problem has close links with pseudorandom number generation, see [102, 104, 136] for these links and further references.

Problem 52. For a prime p, a primitive root g modulo p and an integer v_0, the following sequence of integers

$$v_n \equiv g^{v_{n-1}} \pmod{p}, \ 0 \le v_n \le p-1, \qquad n = 1, 2, \ldots.$$

As before we note that this sequence eventually becomes periodic with some period T and we also assume that it is purely periodic. Estimate exponential sums

$$\sum_{n=1}^{N} \mathbf{e}_p(av_n), \qquad a \in \mathbb{Z},$$

for $N \le T$.

3.12 Computational and algorithmic problems

Problem 53. Let us define the constants

$$A(n) = \sup_{m \ge 1} \max_{\gcd(a,m)=1} \left| \sum_{x=1}^{q} \mathbf{e}_m\left(ax^n\right) \right| m^{-1+1/n}.$$

Compute

$$A = \max_{n \ge 2} A(n).$$

Comments: *S. B. Stechkin [134] has given the bound*

$$A(n) = \exp\left(O(\ln \ln n)^2\right)$$

and conjectured that $A(n) = O(1)$. This conjecture is proved in [115] in the following stronger form $A(n) = 1 + O(n^{-1/4+o(1)})$, which is improved to

$$A(n) = 1 + O(n^{-1}\tau(n) \log n)$$

in [91, Theorem 6.7]. Thus the constant A is correctly defined, and recent explicit estimates of Gauss sums of [47], make it to be a feasible task (but it

may still require quite significant efforts). Problem 53 is also posed as [91, Question 6.9]. Finally, we recall that by [91, Theorem 6.8]

$$A(n) \ge 1 + n^{-1} \exp\left(0.43 \frac{\log n}{\log \log n}\right)$$

for infinitely many n.

Problem 54. Find an algorithm to evaluate or approximate Kloosterman sums

$$\sum_{x \in \mathbb{F}_q^*} \psi(x + ax^{-1}), \qquad a \in \mathbb{F}_q^*,$$

with an additive character ψ of $\mathbb{F}_q$ more efficiently than directly from the definition.

Comments: *This question has some connections with quantum computing, see [46]. Results of [120, 123] imply lower bounds on the complexity of computation of Kloosterman sum in some standard computational models.*

3.13 Exponential sums and cryptography

Problem 55. We recall that the *Very Smooth Hash* function, VSH, introduced by S. Contini, A. Lenstra and R. Steinfeld [52] works as follows. Let p_i denote the ith prime number and let

$$Q_k = \prod_{i=1}^{k} p_i$$

denote the product of the first k primes and set $R_k = Q_{k+1}$. Assume that integers k and n satisfy $Q_k < n \le R_k$. Let $\ell < 2^k$, the message length, be a positive integer whose k-bit representation (including all leading zeros) is $\ell = \lambda_1 \dots \lambda_k$ that is

$$\ell = \sum_{i=1}^{k} \lambda_i 2^{i-1}.$$

Then VSH takes an ℓ-bit message $m = \mu_1 \dots \mu_\ell$ (with some leading zeros appended, if necessary) and hashes it (in a very efficient way, via a simple iterative procedure) to

$$h_n(m) \equiv \prod_{i=1}^{k} p_i^{e_i} \pmod{n}, \qquad 0 \le h_n(m) < m,$$

where $L = \lceil \ell/k \rceil$, $\mu_s = 0$, for $\ell < s \le Lk$, $\mu_{Lk+i} = \lambda_i$, for $1 \le i \le k$, and

$$e_i = \sum_{j=0}^{L} \mu_{jk+i} 2^{L-j}, \qquad i = 1, \ldots, k.$$

It is important for cryptographic application to study the distribution of this function which lead to the problems of estimating exponential sums

$$\sum_{m \le M} \mathbf{e}_n(ah(m)), \quad a \in \mathbb{Z}_n,$$

on some reasonably small $M < 2^\ell$.

Comments: *Some number theoretic properties of this function have been studied in [19].*

3.14 Miscellania

Problem 56. Let (f_k) be the sequence of totients, that is, the increasing sequence of all values of the Euler function:

$$\{f_k \ : \ k = 1, 2, \ldots\} = \{\varphi(n) \ : \ n = 1, 2, \ldots\} \qquad \text{and} \qquad f_1 < f_2 < \ldots .$$

Study the distribution of the differences $d_k = f_{k+1} - f_k$.

Comments: *We certainly ask about the results which do not immediately follow from the known facts about the distribution of primes [85] and the counting results for the number of totients up to x, see [59].*

Problem 57. Given a polynomial

$$F(X) = \sum_{j=0}^{d} a_d X^d \in \mathbb{Z}[X], \qquad a_d \ne 0,$$

we define its *Mahler measure* $M(F)$ as

$$M(F) = |a_d| \prod_{F(\alpha)=0} \max\{1, |\alpha|\}$$

where the product is over all roots α of F taken with their multiplicities. We also define $\mathrm{rad}(F)$ as the product of all irreducible factors of F, ignoring multiplicities. Given three polynomials $f, g, h \in \mathbb{Z}[x]$ with

$$f + g = h$$

estimate $M(\mathrm{rad}(fgh))$ in terms of $\max\{M(f), M(g), M(h)\}$?

Comments: *The question is yet another example of many possible polynomial analogues of the abc-conjecture. However instead of the degree* $\deg F$ *as the measure of the size of* F*, see [133], it refers to* $M(F)$*.*

Problem 58. Obtain upper and lower bounds for the number of squarefree palindromes up to x.

Comments: *Using the standard inclusion-exclusion principle and known asymptotic formulas and estimates on the number of palindromes up to* x *in a given arithmetic progression, see [8, 10], is not enough, but just barely.*

Problem 59. Obtain an asymptotic formula for the number of "hyperbolic" squarefree numbers $s \le N$, that is, for the number of vectors of positive integers (n_1, n_2, n_3, n_4) with $n_1n_4 - n_2n_3 = 1$ for which $s = n_1^2 + n_2^2 + n_3^2 + n_4^2$ satisfies $s \le N$ and is squarefree. One can also address a similar question with smooth s or with s having only a fixed number of prime divisors.

Comments: *J. B. Friedlander and H. Iwaniec [66] obtained conditional lower and upper bounds of the right order of magnitude for a much harder question with primes* $p = n_1^2+n_2^2+n_3^2+n_4^2$*. The assumption in [66] is a conjecture on the distribution of rational primes in arithmetic progressions that interpolate between the Bombieri-Vinogradov theorem and Elliott–Hallberstam conjecture, see [85, Section 17.1]. However for squarefree* $s = n_1^2+n_2^2+n_3^2+n_4^2$ *one may expect an unconditional asymptotic formula with a power saving in the error term. It also seems that the method of [66] can work for* s *that are products of at most three primes.*

Problem 60. Consider a set of positive integers $\mathcal{A} = \{a_0 = 1, a_1, \dots, a_N\}$, where for $1 \le n \le N$ we have $a_n = a_r + a_s$ with some integers $r, s < n$. Obtain a good upper bound for

$$W_N(\mathcal{A}) = \omega\left(\prod_{\substack{1\le m,n\le N\\ a_n\ne a_m}} (a_n - a_m)\right).$$

Comments: *It is obvious that*

$$W_N(\mathcal{A}) \ll \frac{N^3}{\log N}.$$

The question is related to lower bounds on generic algorithms for computing orders of elements in generic groups, see [135].

Problem 61. For a positive integer $g \geq 2$, an arbitrary integer h and a polynomial $f(X) \in \mathbb{Z}[X]$ obtain lower and upper bounds on

$$\lambda(P_h(x)), \qquad \lambda(F_f(x)), \qquad \lambda(G_{g,h}(x)),$$

where

$$P_h(x) = \prod_{h<p\leq x} (p-h), \qquad F_f(x) = \prod_{\substack{n\leq x \\ f(n)\neq 0}} |f(n)|, \qquad G_{g,h}(x) = \prod_{n\leq x} \left(g^n - h\right),$$

and $\lambda(k)$ is the Carmichael function, that is

$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1), & \text{if } p \geq 3 \text{ or } \nu \leq 2; \\ 2^{\nu-2}, & \text{if } p = 2 \text{ and } \nu \geq 3; \end{cases}$$

and for an arbitrary integer $n \geq 2$,

$$\lambda(n) = \operatorname{lcm}\big(\lambda(p_1^{\nu_1}), \ldots, \lambda(p_k^{\nu_k})\big),$$

where $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$ is the prime factorization of n.

Comments: *Certainly the behaviour of $\lambda(P_h(x))$ and $\lambda(G_{g,h}(x))$ depends quite dramatically whether $h = 0$ or $h \neq 0$. A lower bound $\omega(P_h(x)) \gg x^{0.3596}$ is given in [14].*

Problem 62. Prove that any integer n can be represented as $n = m + s$ where m is squarefree and s is very smooth.

Comments: *The case when $s = 2^k$ corresponds to the conjecture of Erdős, which is shown by A. Granville and K. Soundararajan [79] to be related to the nonvanishing of $(a^p - a)/p$ modulo p). It is quite possible that a combination of [79, Proposition 3] with the results about nonvanishing Fermat quotient of [32, 132] may lead to a result with a rather smooth s.*

Problem 63. Design and efficient algorithm, that for given x and y generates a "random" y-smooth number $n \le x$, that is, the output is always y-smooth and any y-smooth number appears with probability close to $1/\psi(x,y)$ where as usual

$$\psi(x,y) = \#\{s \le x \ : \ s \text{ is } y\text{-smooth}\}.$$

Comments: *E. Bach [1] has proposed an algorithm to generate random factored integers, that is, an algorithm that outputs any integer $n \le x$ with probability close to $1/x$, and also outputs a full factorisation of n. A. T. Kalai [86] has improved this algorithm.*

Problem 64. We say that an integer s is k-digit smooth to base g (for a fixed integer $g \ge 2$) if it can be written as a product $s = s_1 \dots s_m$, where each factor s_i contains at most k nonzero digits in its g-ary expansion. Obtain upper and lower bounds on

$$\Omega_g(x,k) = \#\{s \le x \ : \ s \text{ is } k\text{-digit smooth to base } g\}.$$

Comments: *Perhaps one can derive a nontrivial upper bound $\Omega_g(x,k)$ via the Rankin method.*

Problem 65. We say that a monic polynomial $f \in \mathbb{Z}[X]$ is *degenerate* if for two distinct roots λ and μ of f the ratio λ/μ is a root of unity. Obtain an sharp upper bound on the number $D_n(H)$ of degenerate polynomials of degree n and of height at most H, that is,

$$D_n(H) = \#\{f(X) = X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X] \ : \\ f \text{ is degenerate}, \ |a_i| \le H, \ i = 1, \dots, n\}.$$

Comments: *Degenerate polynomials play an important role in the theory of linear recurrence sequences, see [58]. Trivially, we have $D_n(H) = O(H^{n-1})$. Indeed, for a fixed n there are $O(1)$ roots of unity that are ratios of two algebraic numbers of degree at most n, see [56, 113] for a more precise result. If $f(X) = X^n + a_1X^{n-1} + \dots + a_n$ is degenerate then $f(X)$ and $f(\rho X)$, where ρ is one of these possible roots of unity, have a common root. Hence the resultant*

$$R_\rho(a_1, \dots, a_n) = \mathrm{Res}(f(X), f(\rho X)).$$

vanishes. Clearly $R_\rho(a_1, \dots, a_n)$ is a non-zero polynomial as otherwise $f(X)$ and $f(\rho X)$ have a common root for any monic polynomial f of degree n. Thus the equation $R(a_1, \dots, a_n) = 0$ has $O(H^{n-1})$ integer solutions in variables $|a_1|, \dots, |a_n| \le H$.

Problem 66. Prove that for any $\varepsilon > 0$ there exists $\ell(\varepsilon)$ such that for any $u \in \mathbb{F}_p$, an arbitrary $\lambda \in \mathbb{F}_p$ can be represented as

$$\frac{1}{x_1} + \ldots + \frac{1}{x_{\ell(\varepsilon)}} \equiv \lambda \pmod{p}$$

with $u + 1 \le x_1, \ldots, x_{\ell(\varepsilon)} \le u + p^{\varepsilon}$.

Comments: *The question is a generalisation of the Erdős-Graham problem [57], that corresponds to $u = 0$ and has been solved in [118], see also [26, 54, 76]. It is possible that the recent results of Bourgain and Garaev [34] can be of some use but the problem seems to be very difficult and certainly requires more new ideas. Even the case of $\varepsilon = 1/2$ is already difficult.*

Acknowledgements

The author is very grateful to his colleagues and especially to his co-authors, for joint projects or just discussions on exponential and characters sums, number theory and mathematics in general. This list of problems is a tribute to the sacrificed beer and chalk.

Special thanks also go Bill Banks and Ke Gong for the careful reading of the preliminary version and many valuable comments.

References

[1] E. Bach, 'How to generate factored random numbers', *SIAM J. Comp.*, **17** (1988), 179–193.

[2] S. Balasuriya, I. E. Shparlinski and D. Sutantyo, 'Multiplicative character sums with the Euler function', *Studia Sci. Math. Hungarica*, **46** (2009), 223–229.

[3] A. Balog, K. A. Broughan and I. E. Shparlinski, 'On the number of solutions of exponential congruences', *Acta Arith.*, **148** (2011), 93–103.

[4] R. C. Baker, 'Kloosterman sums with prime variable', *Preprint*, 2011.

[5] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Uniform distribution of fractional parts related to pseudoprimes', *Canad. J. Math.*, **61** (2009), 481–502.

[6] W. D. Banks, A. Harcharras and I. E. Shparlinski, 'Short Kloosterman sums for polynomials over finite fields', *Canad. J. Math.*, **55** (2003), 225–246.

[7] W. D. Banks, G. Harman and I. E. Shparlinski, 'Distributional properties of the largest prime factor', *Michigan Math. J.*, **53** (2005), 665–681.

[8] W. D. Banks, D. Hart and M. Sakata, 'Almost all palindromes are composite', *Math. Res. Lett.*, **11** (2004), 853–868.

[9] W. Banks and I. E. Shparlinski, 'Congruences and exponential sums with the Euler function', *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Amer. Math. Soc., 2004, 49–60.

[10] W. D. Banks and I. Shparlinski, 'Prime divisors of palindromes', *Period. Math. Hungar.*, **51** (2005), 1–10.

[11] W. D. Banks and I. E. Shparlinski, 'Non-residues and primitive roots in Beatty sequences', *Bull. Austral. Math. Soc.*, **73** (2006), 433–443.

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

[13] W. Banks and I. E. Shparlinski, 'Congruences and rational exponential sums with the Euler function', *Rocky Mountain J. Math.*, **36** (2006), 1415–1426.

[14] W. D. Banks and I. E. Shparlinski, 'On values taken by the largest prime factor of shifted primes', *J. Aust. Math. Soc.*, **82** (2007), 133–147.

[15] W. D. Banks and I. E. Shparlinski, 'Character sums with Beatty sequences on Burgess-type intervals', *Analytic Number Theory – Essays in Honour of Klaus Roth*, Cambridge Univ. Press, Cambridge, 2009, 15-21.

[16] W. D. Banks and I. E. Shparlinski, 'Multiplicative character sums with twice-differentiable functions', *Quart. J. Math.*, **60** (2009), 401–411.

[17] V. Bergelson, A. Leibman and E. Lesigne, 'Intersective polynomials and the polynomial Szemeredi theorem', *Advances in Math.* , **219** (2008), 369–388.

[18] E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, NY, 1968.

[19] I. Blake and I. E. Shparlinski, 'Statistical distribution and collisions of the VSH', *J. Math. Cryptology*, 2007, v.1, 329–349.

[20] E. Bombieri, 'On exponential sums in finite fields', *Amer. J. Math.*, **88** (1966), 71–105.

[21] J. Bourgain, 'More on the sum-product phenomenon in prime fields and its applications', *Int. J. Number Theory*, **1** (2005), 1–32.

[22] J. Bourgain, 'Estimates on exponential sums related to Diffie-Hellman distributions', *Geom. and Funct. Anal.*, **15** (2005), 1–34.

[23] J. Bourgain, 'Mordell's exponential sum estimate revisited', *J. Amer. Math. Soc.*, **18** (2005), 477–499.

[24] J. Bourgain, 'Exponential sum estimates on subgroups of $\mathbb{Z}_q$, q arbitrary', *J. Anal. Math.*, **97** (2005), 317–355.

[25] J. Bourgain, 'Exponential sum estimates in finite commutative rings and applications', *J. d'Analyse Math.*, **101** (2007), 325–355.

[26] J. Bourgain, 'Some arithmetical applications of the sum-product theorems in finite fields', *Geometric aspects of functional analysis*, Lecture Notes in Math., vol. 1910, Springer-Verlag, Berlin, 2007, 99–116.

[27] J. Bourgain, 'On an exponential sum related to the Diffie-Hellman cryptosystem', *Intern. Math. Research Notices*, **2008** (2008), Article ID 61271, 1–15.

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

[29] J. Bourgain, 'Estimates of polynomial exponential sums', *Israel J. Math.*, **176** (2010), 221–240.

[30] J. Bourgain and M.-C. Chang, 'Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q$, where q is composite with few prime factors', *Geom. and Funct. Anal.*, **16** (2006), 327–366.

[31] J. Bourgain and M.-C. Chang, 'On a multilinear character sums of Burgess', *Comp. Rend. Acad. Sci. Paris*, **348** (2010), 115–120.

[32] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.*, **59** (2010), 313–328.

[33] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambridge Phil. Soc.*, **146** (2009), 1–21.

[34] J. Bourgain and M. Z. Garaev, 'Sumsets of reciprocals in prime fields and multilinear Kloosterman sums', *Izvestiya: Mathematics*, **78** (2014), 656–707.

[35] 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. Lond. Math. Soc.*, **73** (2006), 380–398.

[36] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2008** (2008), Article ID rnn090, 1–29.

[37] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Distribution of elements of cosets of small subgroups and applications', *Intern. Math. Research Notices*, (to appear).

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

[39] R. de la Bretèche and G. Tenenbaum, 'Sommes d'exponentielles friables d'arguments rationnels', *Funct. Approx. Comment. Math.* , **37** (2007), 31–38.

[40] K. A. Broughan, F. Luca and I. E. Shparlinski, 'Some divisibility properties of binomial coefficients and Wolstenholme's conjecture', *Integers*, **10** (2010), 485–495.

[41] M.-C. Chang, 'On a problem of Arnold on uniform distribution', *J. Funcional Analysis*, **242** (2007), 272–280.

[42] M.-C. Chang, 'On a question of Davenport and Lewis and new character sum bounds in finite fields', *Duke Math. J.*, **145** (2008), 409–442.

[43] M.-C. Chang, 'Burgess inequality in $\mathbb{F}_{p^2}$', *Geom. Funct. Anal.*, **19** (2009), 1001–1016.

[44] M.-C. Chang, 'Short character sums with Fermat quotients', *Acta Arith.*, **152** (2012), 23–38.

[45] M.-C. Chang and C. Z. Yao, 'An explicit bound on double exponential sums related to DiffieHellman distributions', *SIAM J. Discr. Math.*, **22** (2008), 348–359.

[46] A. M. Childs, L. J. Schulman and U. V. Vazirani, 'Quantum algorithms for hidden nonlinear structures', *Proc. 48th IEEE Symp. on Found. Comp. Sci.*, IEEE, 2007, 395–404.

[47] T. Cochrane and C. Pinner, 'Explicit bounds on monomial and binomial exponential sums', *Quart. J. Math..*, **62** (2011), 323–349.

[48] T. Cochrane, C. Pinner and J. Rosenhouse, 'Bounds on exponential sums and the polynomial Waring problem mod$p$', *J. London Math. Soc.*, **67** (2003), 319–336.

[49] T. Cochrane, C. Pinner and J. Rosenhouse, 'Sparse polynomial exponential sums', *Acta Arith.*, **108** (2003), 37–52.

[50] T. Cochrane and Z. Y. Zheng, 'Exponential sums with rational function entries', *Acta Arith.*, **95** (2000), 67–95.

[51] T. Cochrane and Z. Y. Zheng, 'A survey on pure and mixed exponential sums modulo prime powers', *Proc. Illinois Millennial Conf. on Number Theory, Vol.1*, A.K. Peters, Natick, MA, 2002, 271–300.

[52] S. Contini, A. K. Lenstra and R. Steinfeld, 'VSH, an efficient and provable collision-resistant hash function', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **4004** (2006), 165–182.

[53] P. Corvaja, 'Problems and results on integral points on ratonal surfaces', *Diophantine Geometry*, CRM Series, Vol. 4, Scuola Normale Superiore, Pisa, 2007, 123–141.

[54] E. S. Croot, 'Sums of the form $1/x_1^k + \ldots + 1/x_n^k$ modulo a prime', *Integers*, **4** (2004), A20, 1–6.

[55] E. Dobrowolski and K. S Williams, 'An upper bound for the sum $\sum_{n=a+1}^{a+H} f(n)$ for a certain class of functions f', *Proc. Amer. Math. Soc.*, **114** (1992), 29–35.

[56] P. Drungilas and A. Dubickas, 'On subfields of a field generated by two conjugate algebraic numbers', *Proc. Edinb. Math. Soc.*, **47** (2004), 119–123.

[57] P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Math. **28**, Univ. de Genéve, Genéve, 1980.

[58] G. Everest, A. van der Poorten, I. E. Shparlinski and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, **104**, Amer. Math. Soc., Providence, RI, 2003.

[59] K. Ford, 'The number of solutions of $\varphi(x) = m$', *Annals of Math.*, **150** (1999), 283–311.

[60] É. Fouvry and Ph. Michel, 'Sur certaines sommes d'exponentielles sur les nombres premiers', *Ann. Sci. École Norm. Sup. (4)*, **31** (1998), 93–130.

[61] É. Fouvry and I. E. Shparlinski, 'On a ternary quadratic form over primes', *Acta Arith.*, **150** (2011), 285–314.

[62] É. Fouvry and G. Tenenbaum, 'Entiers sans grand facteur premier en progressions arithmétiques', *Proc. London Math. Soc.*, **63** (1991), 449–494.

[63] J. B. Friedlander, K. Gong and I. E. Shparlinski, 'Character sums over shifted primes', *Matem. Zametki*, **88** (2010), 605–619 (in Russian).

[64] J. B. Friedlander, J. Hansen and I. E. Shparlinski, 'On character sums with exponential functions', *Mathematika*, **47** (2000), 75–85.

[65] J. B. Friedlander and H. Iwaniec, 'The Brun–Titchmarsh theorem', *Analytic Number Theory*, Lond. Math. Soc. Lecture Note Series **247**, 1997, 363–372.

[66] J. B. Friedlander and H. Iwaniec, 'Hyperbolic prime number theorem', *Acta Math.*, **202** (2009), 1–19.

[67] J. B. Friedlander, S. V. Konyagin and I. E. Shparlinski, 'Some doubly exponential sums over $\mathbb{Z}_m$', *Acta Arith.*, **105** (2002), 349–370.

[68] J. B. Friedlander, D. Lieman and I. E. Shparlinski, 'On the distribution of the RSA generator', *Proc. Intern. Conf. on Sequences and Their Applications (SETA'98), Singapore*, Springer-Verlag, London, 1999, 205-212.

[69] N. Frantzikinakis, 'Multiple recurrence and convergence for Hardy sequences of polynomial growth', *J. d'Analyse Math.*, **112** (2010), 79–135.

[70] H. Furstenberg, 'From the Erdős–Turán conjecture to ergodic theory — The contribution of combinatorial number theory to dynamics', *Paul Erdős and His Mathematics*, Springer-Verlag, Berlin, 2002, 261–277.

[71] M. Z. Garaev, 'An estimate of Kloosterman sums with prime numbers and application', *Matem. Zametki*, **88** (2010), 365–373, (in Russian).

[72] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Character sums and congruences with $n!$', *Trans. Amer. Math. Soc.*, **356** (2004), 5089–5102.

[73] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Exponential sums and congruences with factorials', *J. Reine Angew. Math.*, **584** (2005), 29–44.

[74] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Catalan and Apéry numbers in residue classes', *J. Combin. Theory, Ser. A*, **113** (2006), 851–865.

[75] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Exponential sums with Catalan numbers' *Indag. Math.*, **18** (2007), 23–37.

[76] A. Glibichuk, 'Combinational properties of sets of residues modulo a prime and the Erdős-Graham problem', *Math. Notes*, **79** (2006), 356–365 (Transl. from *Matem. Zametki*).

[77] D. Gomez and A. Winterhof, 'Multiplicative character sums of Fermat quotients and pseudorandom sequences', *Period. Math. Hungarica*, (to appear).

[78] K. Gong, 'On certain character sums over smooth numbers', *Glasnik Math.*, **44** (2009), 333–342.

[79] A. Granville and K. Soundararajan, 'A binary additive problem of Erdős and the order of 2 mod p^2', *The Ramanujan J.*, **2** (1998), 283–298.

[80] A. Granville and K. Soundararajan, 'Large character sums' *J. Amer. Math. Soc.*, **14** (2001), 365–397.

[81] D. R. Heath-Brown, 'The square sieve and consecutive squarefree numbers', *Math. Ann.*, **266** (1984), 251–259.

[82] R. Heath-Brown, 'An estimate for Heilbronn's exponential sum', *Analytic Number Theory: Proc. Conf. in honor of Heini Halberstam*, Birkhauser, Boston, 1996, 451–463.

[83] 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. Oxford*, **51** (2000), 221–235.

[84] C.-N. Hsu, 'The Brun-Titchmarsh theorem in function fields', *J. Number Theory*, **79** (1999), 67–82.

[85] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[86] A. T. Kalai, 'Generating random factored numbers, easily', *J. Crypto.*, **16** (2003), 287–289.

[87] A. A. Karatsuba, 'Sums of characters with prime numbers', *Izv. Akad. Nauk Ser. Mat.*, 34 (1970) 299–321.

[88] A. A. Karatsuba, 'The distribution of values of Dirichlet characters on additive sequences', *Doklady Acad. Sci. USSR*, **319** (1991), 543–545 (in Russian).

[89] S. V. Konyagin, 'On estimates of Gaussian sums and the Waring problem modulo a prime', *Trudy Matem. Inst. Acad. Nauk USSR*, Moscow, **198** (1992), 111–124 (in Russian).

[90] S. V. Konyagin, 'Bounds of character sums in finite fields', *Matem. Zametki*, **88** (2010), 529–542 (in Russian).

[91] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[92] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Matem. Sbornik*, **89** (1972), 654–670 (in Russian).

[93] N. M. Korobov, *Exponential sums and their applications*, Kluwer Acad. Publ., Dordrecht, 1992.

[94] B. Levitt and W. McCallum, 'Yet more elements in the Shafarevich-Tate group of the Jacobian of a Fermat curve', *Computational Arithmetic Geometry: AMS Special Session, San Francisco, CA, USA, April 29–30, 2006*, Contemporary Mathematics **463**, Amer. Math. Soc., Providence, RI, 2008, 83–90.

[95] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge Univ. Press, Cambridge, 1997.

[96] D. Lieman and I. E. Shparlinski 'On a new exponential sum', *Canad. Math. Bull.*, **44** (2001), 87–92.

[97] H. Liu and W. Zhang, 'On the squarefree and squarefull numbers', *J. Math. Kyoto Univ.*, **45** (2005), 247–255.

[98] W. G. McCallum and P. Tzermias, 'On Shafarevich-Tate groups and the arithmetic of Fermat curves', *Number Theory and Algebraic Geometry*, Lecture Note Ser., vol 303, Cambridge Univ. Press, Cambridge, 2003, 203226.

[99] H. L. Montgomery, *Topics in multiplicative number theory*, *Lect. Notes in Math.*, Springer-Verlag, Berlin, **227** (1971).

[100] A. Mukhopadhyay, M. R. Murty and K. Srinivas, 'Counting squarefree discriminants of trinomials under *abc*', *Proc. Amer. Math. Soc.*, **137** (2009), 3219–3226.

[101] H. Niederreiter and I. E. Shparlinski, 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', *Finite Fields and Their Appl.*, **5** (1999), 246–253.

[102] H. Niederreiter and I. E. Shparlinski, 'Recent advances in the theory of nonlinear pseudorandom number generators', *Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods, 2000*, Springer-Verlag, Berlin., 2002, 86–102.

[103] H. Niederreiter and I. E. Shparlinski, 'On the average distribution of inversive pseudorandom numbers', *Finite Fields and Their Appl.*, **8** (2002), 491–503.

[104] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2643** (2003), 6–17.

[105] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields Appl.*, **14** (2008), 59–64.

[106] A. Ostafe, 'Multivariate permutation polynomial systems and nonlinear pseudorandom number generators', *Finite Fields and Their Appl.* **16** (2010), 144–154.

[107] A. Ostafe and I. E. Shparlinski, 'On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators', *Math. Comp.*, **79** (2010), 501–511.

[108] A. Ostafe and I. E. Shparlinski, 'Pseudorandom numbers and hash functions from iterations of multivariate polynomials', *Cryptography and Communications*, **2** (2010), 49–67.

[109] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discr. Math.*, **25** (2011), 50–71.

[110] A. Ostafe and I. E. Shparlinski, 'Exponential sums over points of elliptic curves with reciprocals of primes', *Mathematika*, **58** (2012), 21–33.

[111] G. I. Perel'muter and I. E. Shparlinski, 'On the distribution of primitive roots in finite fields', *Uspechi Matem. Nauk*, **45**(1) (1990), 185–186 (in Russian).

[112] Z. Kh. Rakhmonov, 'On the distribution of values of Dirichlet characters and their applications', *Proc. Steklov Inst. Math.*, **207** (1995), 263–272.

[113] A. Schinzel, 'Around Pólya's theorem on the set of prime divisors of a linear recurrence', *Diophantine equations*, Tata Inst. Fund. Res. Stud. Math., vol. 20, Mumbai, 2008, 225–233.

[114] V. Shoup, 'On the determenistic complexity of factoring polynomials over finite fields', *Inform. Proc. Letters*, **33** (1990), 261–267.

[115] I. E. Shparlinski, 'On bounds of Gaussian sums', *Matem. Zametki*, **50** (1991), 122–130 (in Russian).

[116] I. E. Shparlinski, 'On exponential sums with sparse polynomials and rational functions', *J. Number Theory*, **60** (1996), 233–244.

[117] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, 1999.

[118] I. E. Shparlinski, 'On a question of Erdős and Graham', *Arch. Math. (Basel)*, **78** (2002), 445–448.

[119] I. E. Shparlinski, 'Exponential function analogue of Kloosterman sums', *Rocky Mountain J. Math.*, **34** (2004), 1497–1502.

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

[121] I. E. Shparlinski, 'Character sums over shifted smooth numbers', *Proc. Amer. Math. Soc.*, **135** (2007), 2699–2705.

[122] I. E. Shparlinski, 'On some dynamical systems in finite fields and residue rings', *Discr. and Cont. Dynam. Syst., Ser.A*, **17** (2007), 901–917.

[123] I. E. Shparlinski, 'On the distribution of Kloosterman sums', *Proc. Amer. Math. Soc.*, **136** (2008), 403–407.

[124] I. E. Shparlinski, 'On quadratic fields generated by discriminants of irreducible trinomials', *Proc. Amer. Math. Soc.*, **138** (2010), 125-132.

[125] I. E. Shparlinski, 'Exponential sums with consecutive modular roots of an integer', *Quart. J. Math.*, **62** (2011), 207–213.

[126] I. E. Shparlinski, 'Character sums with Fermat quotients', *Quart. J. Math.*, **62** (2011), 1031–1043.

[127] I. E. Shparlinski, 'Bounds of multiplicative character sums with Fermat quotients of primes', *Bull. Aust. Math. Soc.*, **83** (2011), 456–462.

[128] I. E. Shparlinski, 'Fermat quotients: Exponential sums, value set and primitive roots', *Bull. Lond. Math. Soc.*, **43** (2011), 1228–1238.

[129] I. E. Shparlinski, 'On some exponential sums with exponential and rational functions', *Rocky Mountain J. Math.*, (to appear).

[130] I. E. Shparlinski and A. Winterhof, 'Noisy interpolation of sparse polynomials in finite fields', *Appl. Algebra in Engin., Commun. and Computing*, **16** (2005), 307–317.

[131] I. E. Shparlinski and A. Winterhof, 'A hidden number problem in small subgroups', *Math. Comp.*, **74** (2005), 2073–2080.

[132] Y. N. Shteinikov, 'Divisibility of Fermat quotients', *Mat. Zametki*, **92** (2012), 116–122 (in Russian).

[133] N. Snyder, 'An alternate proof of Mason's theorem', *Elemente der Mathematik*, **55** (2000), 93–94.

[134] S. B. Stechkin, 'An estimate for Gaussian sums', *Matem. Zametki*, **17** (1975), 342–349 (in Russian).

[135] D. C. Terr, 'A modification of Shanks' baby-step giant-step algorithm', *Math. Comp.*, **69** (2000), 767–773.

[136] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2007, 135–166.

[137] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge Univ. Press, Cambridge, 1981.

[138] R. C. Vaughan, 'A new iterative method for Waring's problem', *Acta Math.*, **162** (1989), 1–71.

[139] M. Xiong and A. Zaharescu, 'Distribution of Selmer groups of quadratic twists of a family of elliptic curves', *Advances Math.*, **219** (2008), 523–553.

[140] G. Yu, 'Rank 0 quadratic twists of a family of elliptic curves', *Compos. Math.*, **135** (2003), 331–356.

[141] H. B. Yu, 'Estimates of character sums with exponential function', *Acta Arith.*, **97** (2001), 211–218.