Pure and Applied Mathematics Quarterly
Volume 2, Number 1
(*Special Issue: In honor of
John H. Coates, Part 1 of 2*)
179—197, 2006

Double Character Sums over Elliptic Curves and Finite Fields

William D. Banks, John B. Friedlander
Moubariz Z. Garaev and Igor E. Shparlinski

*Dedicated to John Coates on the occasion of
his sixtieth birthday*

Abstract: We estimate certain double character sums over points of an elliptic curve and in the multiplicative subgroup of a finite field. These bounds both improve and extend the scope of a series of previous results. We apply these results to estimate the related sums over primes, and to derive new uniformity of distribution results for the elliptic curve pseudorandom number power generator. We also mention some further applications, both to cryptography and to smooth number distribution.

1. Introduction

1.1. **Background.** For m a positive integer let $\mathbb{Z}_m$ denote the ring of integers modulo m, which we identify with the set $\{0, 1, \ldots, m-1\}$ and let $\mathbb{Z}_m^*$ denote the multiplicative group of invertible elements in $\mathbb{Z}_m$; then $\#\mathbb{Z}_m^* = \varphi(m)$ where φ is the Euler function. In case of a prime number p, then $\mathbb{Z}_p$ is a finite field which we sometimes denote by $\mathbb{F}_p$. Let $\mathbf{e}_p$ be the canonical additive character of $\mathbb{F}_p$ given by $\mathbf{e}_p(n) = \exp(2\pi i n/p)$ for all $n \in \mathbb{F}_p$. We use χ to denote an arbitrary multiplicative character, that is, a character of $\mathbb{F}_p^*$, which we extend to a map $\chi : \mathbb{F}_p \to \mathbb{C}$ by taking $\chi(0) = 0$.

There is a considerable literature devoted to bounds and applications thereof for sums of the form

$$\sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}} \alpha_u \beta_v \, \mathbf{e}_p(auv) \qquad \text{and} \qquad \sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}} \alpha_u \beta_v \, \chi(u+v),$$

Received June 8, 2005.
Subject Classification (2000) Primary 11L07, 11T23 Secondary 11G20.

where $a \in \mathbb{F}_p$, $\mathcal{U}$ and $\mathcal{V}$ are arbitrary subsets of $\mathbb{F}_p$, and $\{\alpha_u\}_{u\in\mathcal{U}}$ and $\{\beta_v\}_{v\in\mathcal{V}}$ are sequences of complex numbers supported on the sets $\mathcal{U}$ and $\mathcal{V}$ respectively; see for example [9, 15, 25, 26, 27, 36, 37, 39] (as well as Problem 14.a in Chapter 6 of [40]) and the references contained therein. These sums arise frequently in various number–theoretic constructions.

For a fixed element $\vartheta \in \mathbb{F}_p^*$ of multiplicative order t, double exponential sums of the form

$$\sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}} \alpha_u\beta_v\,\mathbf{e}_p(a\vartheta^{xy}), \tag{1}$$

where $\mathcal{U}$ and $\mathcal{V}$ are subsets of $\mathbb{Z}_t$, have also been considered in [20], and later (in full generality) in [1]. These sums too have interesting applications, sometimes, as for example in [6, 7], motivated by cryptographic considerations. In [1], an upper bound for the sums (1) played a crucial role in obtaining nontrivial upper bounds for the sums

$$\sum_{q\le N} \mathbf{e}_p(a\vartheta^q), \qquad a \in \mathbb{F}_p^*,$$

where the parameter q varies over prime numbers.

The main result of [20] has recently been improved in [21] and this has, when combined with the previous arguments, led to corresponding improvements in some of the results of [6, 7] and in some of the results of [1]. One of the advantages of the approach of [21] over that of [1, 20] is that it can also be applied to bound the corresponding multiplicative character sums and also to bound similar sums taken over points on an elliptic curve. In this paper we investigate these questions and also give some applications.

A word about notation. Throughout the paper, any implied constants in symbols O and $\ll$ may, where obvious, depend on the small positive parameter ε (whose value will change from one occurrence to the next), but are absolute otherwise.

1.2. **Double Sums over Elliptic Curves.** Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$, defined by an affine *Weierstraß equation* of the form

$$Y^2 = X^3 + AX + B$$

with coefficients $A, B \in \mathbb{F}_p$ and nonzero discriminant. It is well–known (see, for example, [3, 38]) that the set $\mathcal{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\mathcal{E}$, together with the point at infinity $\mathcal{O}$, forms an *abelian group* under an appropriate composition rule which is called *addition* and is denoted by $\oplus$. Given a point $Q \in \mathcal{E}(\mathbb{F}_p)$ and an integer $n \ge 1$, we write

$$nQ = \underbrace{Q \oplus Q \oplus \cdots \oplus Q}_{n \text{ copies}}$$

and extend this definition to all $n \in \mathbb{Z}$ using the group structure of $\mathcal{E}(\mathbb{F}_p)$. Let us also recall that the number of points on the curve satisfies the well–known *Hasse bound*:

$$|\#\mathcal{E}(\mathbb{F}_p) - p - 1| \le 2p^{1/2}.$$

For every point $Q \in \mathcal{E}(\mathbb{F}_p)$ such that $Q \neq \mathcal{O}$, we denote by $\mathbf{x}(Q)$ and $\mathbf{y}(Q)$, respectively, its affine components in $\mathbb{F}_p$; that is, $Q = (\mathbf{x}(Q), \mathbf{y}(Q))$.

Let $G \in \mathcal{E}(\mathbb{F}_p)$ be a point of order T; in other words, T is the cardinality of the cyclic group $\langle G \rangle$ generated by G in $\mathcal{E}(\mathbb{F}_p)$. Below, we estimate the sums

$$W_a(\mathcal{U}, \mathcal{V}) = \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \alpha_u \beta_v \, \mathbf{e}_p(a\mathbf{x}(uvG)), \qquad a \in \mathbb{F}_p^*, \tag{2}$$

where, as before, $\mathcal{U}$ and $\mathcal{V}$ are subsets of $\mathbb{Z}_T$. Using these bounds, we then give estimates for the sums

$$S_a(N) = \sum_{q \le N} \mathbf{e}_p(a\mathbf{x}(qG)), \qquad a \in \mathbb{F}_p^*, \tag{3}$$

where, as before, the parameter q varies over prime numbers. These bounds are uniform in a.

Recall that the group of m-torsion points $\mathcal{E}[m]$ is isomorphic to $\mathbb{Z}_m^2$ whenever $p \nmid m$. If m is a power of p, then $\mathcal{E}[m]$ is either isomorphic to $\mathbb{Z}_m$ or to $\langle \mathcal{O} \rangle$. In the latter case, the curve is said to be *supersingular*, otherwise it is called *nonsupersingular* or *ordinary*. In what follows, we consider only ordinary curves.

Throughout the paper, for all of our sums over points $Q \in \mathcal{E}$, instead of simply taking the $\mathbf{x}$–component, one can obtain completely analogous results by taking the $\mathbf{y}$–component or indeed replacing this by any nonconstant rational function in $\mathbf{x}(Q)$ and $\mathbf{y}(Q)$.

There are a number of other papers that address the problem of bounding exponential sums over certain sequences of points on an elliptic curve (see, for example, [24, 29, 32]). As far as we can see our results cannot be derived using the approaches of those papers. However, we do apply a bound from [32], which follows from a more general estimate in [29]. In turn, the main result of [29] relies on classical results of Bombieri [5].

1.3. Cryptographic Applications.

Besides being a natural number–theoretic question, the estimation of the exponential sums (2) has cryptographic meaning as well. Since its invention by Koblitz [28] and Miller [34], elliptic curve cryptography has proved to be of great practical and theoretical value, see [3, 4, 22]. However, compared to cryptographic constructions based on subgroups of the multiplicative group of a finite field, relatively few rigorous results are known for the cryptographic protocols on elliptic curves. Our bound of the sums (2) makes a step towards eliminating the disparity between these two types of constructions.

In particular, it implies, by the well–known Weyl criterion, various uniformity of distribution results for Diffie-Hellman triples on elliptic curves, namely the triples

$$(\mathbf{x}(uG), \mathbf{x}(vG), \mathbf{x}(uvG)) \ , \tag{4}$$

statements analogous to the results of [6, 7] (wherein one can see just how the proofs proceed and also find a detailed outline of the cryptographic significance of such results). Indeed, if the point $G \in \mathcal{E}(\mathbb{F}_p)$ is of order T then the corresponding exponential sums with the points (4), that is, the sums

$$\sum_{u=1}^{T} \sum_{v=1}^{T} \mathbf{e}_p(a\mathbf{x}(uG) + b\mathbf{x}(vG) + c\mathbf{x}(uvG)), \qquad a, b, c \in \mathbb{F}_p,$$

are of the form (2) if $c \neq 0$ (and of a simpler form studied in [29] if $c = 0$).

A more concrete and less immediate application of our results is to the so-called *power generator* on elliptic curves, which, for a given point $G \in \mathcal{E}(\mathbb{F}_p)$ of order T and an integer $e \geq 2$ with $\gcd(e, T) = 1$, is defined as the sequence of points $U_n \in \mathcal{E}(\mathbb{F}_p)$ on the elliptic curve $\mathcal{E}$ generated by the rule

$$U_n = eU_{n-1}, \qquad n = 1, 2, \ldots, \tag{5}$$

where $U_0 = G$. Analogues of these sequences in residue rings and finite fields have been studied in detail in the cryptographic literature; see [10, 31, 35]. Recently, in the series of papers [13, 14, 16, 17, 18, 19, 30], several results about the distribution and period length of such sequences have been obtained, which also exhibit strong links with analytic number theory. Motivated by these works, in [32] the sequence (5) has been introduced. Clearly, this sequence is purely periodic with period t which is the multiplicative order of e modulo T. In particular, it has been shown in [32] that for any fixed integer $\nu \geq 1$,

$$\sum_{n=0}^{t-1} \mathbf{e}_p(a\mathbf{x}(U_n)) \ll t^{1-(3\nu+2)/2\nu(\nu+2)} T^{(\nu+1)/\nu(\nu+2)} p^{1/4(\nu+2)} \tag{6}$$

uniformly for $a \in \mathbb{F}_p^*$ (note that in [32] the roles of t and T are interchanged). The bound (6) immediately implies the uniformity of distribution of the sequence $\mathbf{x}(U_n)$ in wide range of parameters t, T and p. In this paper we are not able to improve the above results, however we obtain bounds of exponential sums (and thus the corresponding uniformity of distribution properties) in the range $n = 1, \ldots, N$ with $N < t$, while the approach of [32] does not apply to incomplete exponential sums.

1.4. **Double Sums with Multiplicative Characters.**

We also give bounds for the sums

$$W_a(\mathcal{U}, \mathcal{V}; \chi) = \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \alpha_u \beta_v \, \chi(\vartheta^{uv} + a), \qquad a \in \mathbb{F}_p^*, \tag{7}$$

where χ is a given nonprincipal multiplicative character. We then apply these bounds to estimate the sums

$$S_a(N;\chi) = \sum_{q \le N} \chi(\vartheta^q + a), \qquad a \in \mathbb{F}_p^*, \tag{8}$$

taken over prime numbers q. Our bounds are uniform both in a and in χ. In this case as well, bounds for the sums (7) and (8) do not appear to be accessible using the approach of [1].

2. Exponential Sums over Elliptic Curves

2.1. **Double Sums.** We need the following bound, which is taken from [32]:

Lemma 1. *Let $1 \le k_1 < \cdots < k_s \le L$ be fixed integers and let $c_1, \ldots, c_s$ be fixed elements of $\mathbb{F}_p$ with $c_s \ne 0$. If $\mathcal{E}$ is any ordinary elliptic curve defined over $\mathbb{F}_p$ then, for every $a \in \mathbb{F}_p^*$, we have*

$$\sum_{\substack{Q \in \mathcal{H} \\ Q \ne \mathcal{O}}} \mathbf{e}_p\left(a \sum_{i=1}^{s} c_i \mathbf{x}\left(k_i Q\right)\right) \ll sL^2 p^{1/2},$$

where $\mathcal{H}$ is an arbitrary subgroup of $\mathcal{E}(\mathbb{F}_p)$ such that $\#\mathcal{H}$ is coprime to the product $k_1 \cdots k_s$.

We also need the following well–known consequence of the sieve of Eratosthenes:

Lemma 2. *For any positive integers m, N, we have:*

$$\sum_{\substack{j=1 \\ \gcd(j,m)=1}}^{N} 1 = \frac{\varphi(m)}{m} N + O(2^{\omega(m)}),$$

where $\omega(m)$ is the number of distinct prime divisors of m.

Proof. Using the Möbius function μ to detect the coprimality condition and interchanging the order of summation, we obtain the Legendre formula:

$$\sum_{\substack{j=1 \\ \gcd(j,m)=1}}^{N} 1 = \sum_{d \,|\, m} \mu(d) \left\lfloor \frac{N}{d} \right\rfloor = N \sum_{d \,|\, m} \frac{\mu(d)}{d} + O\left(\sum_{d \,|\, m} |\mu(d)|\right)$$

from which the result follows at once. □

We are now ready to estimate the sums $W_a(\mathcal{U}, \mathcal{V})$ defined by (2).

Theorem 3. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$, and let $G \in \mathcal{E}(\mathbb{F}_p)$ be a point of order T. Then, for all subsets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_T$ and all $a \in \mathbb{F}_p^*$, the following bound holds:*

$$W_a(\mathcal{U}, \mathcal{V}) \ll ABT^{5/6}(\#\mathcal{U}\#\mathcal{V})^{1/2}p^{1/12+\varepsilon},$$

where

$$A = \max_{u\in\mathcal{U}} |\alpha_u| \ , \ B = \max_{v\in\mathcal{V}} |\beta_v| \ ,$$

and the implied constant depends only on ε.

Proof. For each divisor $d \,|\, T$, we denote by $\mathcal{V}_d$ the set of elements $v \in \mathcal{V}$ such that $\gcd(v, T) = d$. Then,

$$|W_a(\mathcal{U}, \mathcal{V})| \le A \sum_{d\,|\,T} \sigma_d, \tag{9}$$

where

$$\sigma_d = \sum_{u\in\mathcal{U}} \left| \sum_{v\in\mathcal{V}_d} \beta_v \mathbf{e}_p\left(a\mathbf{x}(uvG)\right) \right| .$$

Let $\mathcal{K}$ be the set consisting of the $K = \lceil T^{1/3}p^{-1/6} \rceil$ smallest positive integers that are coprime to T. We may assume that $T > p^{1/2+\varepsilon}$ else the theorem is trivial. Hence, by Lemma 2 we see that

$$\max_{k\in\mathcal{K}} k \ll K \log\log p. \tag{10}$$

For every $v \in \mathcal{V}_d$, there are precisely K ways to express $v/d \equiv kz \pmod{T/d}$ with $k \in \mathcal{K}$ and $z \in \mathbb{Z}_{T/d}^*$ (since, for each $k \in \mathcal{K}$, the value of z is uniquely determined). In particular,

$$\begin{aligned}
\sigma_d &= \frac{1}{K} \sum_{u\in\mathcal{U}} \left| \sum_{z\in\mathbb{Z}_{T/d}^*} \sum_{\substack{k\in\mathcal{K} \\ dkz\in\mathcal{V}_d}} \beta_{dkz} \mathbf{e}_p\left(a\mathbf{x}(udkzG)\right) \right| \\
&\le \frac{1}{K} \sum_{u\in\mathcal{U}} \sum_{z\in\mathbb{Z}_{T/d}^*} \left| \sum_{\substack{k\in\mathcal{K} \\ dkz\in\mathcal{V}_d}} \beta_{dkz} \mathbf{e}_p\left(a\mathbf{x}(udkzG)\right) \right| ,
\end{aligned}$$

where we have written dkz rather than $dkz \pmod T$ for simplicity. Using Cauchy's inequality we derive that

$$\sigma_d^2 \le \frac{T\#\mathcal{U}}{dK^2} \sum_{u\in\mathcal{U}} \sum_{z\in\mathbb{Z}_{T/d}^*} \left| \sum_{\substack{k\in\mathcal{K} \\ dkz\in\mathcal{V}_d}} \beta_{dkz} \mathbf{e}_p\left(a\mathbf{x}(udkzG)\right) \right|^2 .$$

We now extend the summation over u to the full set $\mathbb{Z}_T$, obtaining

$$\begin{aligned}\sigma_d^2 &\le \frac{T\#\mathcal{U}}{dK^2}\sum_{u\in\mathbb{Z}_T}\sum_{z\in\mathbb{Z}_{T/d}^*}\left|\sum_{\substack{k\in\mathcal{K}\\ dkz\in\mathcal{V}_d}}\beta_{dkz}\mathbf{e}_p\left(a\mathbf{x}(udkzG)\right)\right|^2\\ &= \frac{T\#\mathcal{U}}{dK^2}\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k,m\in\mathcal{K}\\ dkz\in\mathcal{V}_d\\ dmz\in\mathcal{V}_d}}\beta_{dkz}\overline{\beta}_{dmz}\sum_{u\in\mathbb{Z}_T}\mathbf{e}_p\left(a\left(\mathbf{x}(udkzG)-\mathbf{x}(udmzG)\right)\right)\\ &\le \frac{B^2T\#\mathcal{U}}{dK^2}\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k,m\in\mathcal{K}\\ dkz\in\mathcal{V}_d\\ dmz\in\mathcal{V}_d}}\left|\sum_{u\in\mathbb{Z}_T}\mathbf{e}_p\left(a\left(\mathbf{x}(udkzG)-\mathbf{x}(udmzG)\right)\right)\right|.\end{aligned}$$

Clearly, as u varies over the set $\mathbb{Z}_T$ the point $Q = udzG$ hits every point of the subgroup $\mathcal{H}_d = \langle dG\rangle$ precisely d times; thus,

$$\sigma_d^2 \le \frac{B^2T\#\mathcal{U}}{K^2}\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k,m\in\mathcal{K}\\ dkz\in\mathcal{V}_d\\ dmz\in\mathcal{V}_d}}\left|\sum_{Q\in\mathcal{H}_d}\mathbf{e}_p\left(a\left(\mathbf{x}(kQ)-\mathbf{x}(mQ)\right)\right)\right|.$$

If $k \ne m$ we use Lemma 1 together with (10) to estimate the innermost sum as $O(K^2p^{1/2}(\log\log p)^2)$ whereas, if $k = m$, the value of the sum is $\#\mathcal{H}_d = T/d$. This leads to the estimate:

$$\sigma_d^2 \ll B^2p^{1/2+\varepsilon}T\#\mathcal{U}\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k,m\in\mathcal{K}\\ dkz\in\mathcal{V}_d\\ dmz\in\mathcal{V}_d}}1 + \frac{B^2T^2\#\mathcal{U}}{dK^2}\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k\in\mathcal{K}\\ dkz\in\mathcal{V}_d}}1.$$

Clearly,

$$\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k\in\mathcal{K}\\ dkz\in\mathcal{V}_d}}1 = \sum_{k\in\mathcal{K}}\sum_{\substack{z\in\mathbb{Z}_{T/d}^*\\ dkz\in\mathcal{V}_d}}1 = K\#\mathcal{V}_d \le K\#\mathcal{V},$$

and also,

$$\sum_{z\in\mathbb{Z}_{T/d}^*}\sum_{\substack{k,m\in\mathcal{K}\\ dkz\in\mathcal{V}_d\\ dmz\in\mathcal{V}_d}}1 = \sum_{k,m\in\mathcal{K}}\sum_{\substack{z\in\mathbb{Z}_{T/d}^*\\ dkz\in\mathcal{V}_d\\ dmz\in\mathcal{V}_d}}1 \le K\sum_{k\in\mathcal{K}}\sum_{\substack{z\in\mathbb{Z}_{T/d}^*\\ dkz\in\mathcal{V}_d}}1 = K^2\#\mathcal{V}_d \le K^2\#\mathcal{V}.$$

Consequently,

$$\begin{aligned}\sigma_d^2 &\ll B^2TK^2p^{1/2+\varepsilon}\#\mathcal{U}\#\mathcal{V} + d^{-1}K^{-1}B^2T^2\#\mathcal{U}\#\mathcal{V}\\ &= B^2T\#\mathcal{U}\#\mathcal{V}(K^2p^{1/2+\varepsilon} + TK^{-1}).\end{aligned}$$

Recalling our choice of K which balances (up to p^ε) the two terms in the above bound we see that

$$\sigma_d \ll BT^{5/6}p^{1/12+\varepsilon}(\#\mathcal{U}\#\mathcal{V})^{1/2}.$$

Substituting this bound into (9) and using the fact that the number $\tau(T)$ of divisors d of T satisfies the bound $\tau(T) \ll T^\varepsilon \le p^\varepsilon$ (see for example Theorem 317 in [23]), we derive the stated estimate. □

In the case that $\mathcal{U}$ and $\mathcal{V}$ are dense subsets of $\mathbb{Z}_T$, in the sense that $\#\mathcal{U} = T^{1+o(1)}$ and $\#\mathcal{V} = T^{1+o(1)}$, the bound of Theorem 3 takes the form

$$W_a(\mathcal{U}, \mathcal{V}) \ll ABT^{11/6}p^{1/12+\varepsilon},$$

which is nontrivial provided that $T \ge p^{1/2+\varepsilon}$.

2.2. **Sums over Primes.** In this subsection, we apply the bound of Theorem 3 to estimate the sums $S_a(N)$ defined by (3).

As before let μ be the Möbius function. Let Λ denote the von Mangoldt function which we recall is defined for positive integers n by

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n > 1 \text{ is a power of a prime } p; \\ 0, & \text{otherwise} \end{cases}$$

with log being the natural logarithm.

We decompose Λ by means of the Vaughan identity, given for example in Chapter 24 of [11], which we use in the following form:

Lemma 4. *For any complex-valued function $f(n)$ and any real numbers $U, V > 1$ with $UV \le N$, we have*

$$\sum_{n \le N} \Lambda(n) f(n) \ll \Sigma_1 + \Sigma_2 + \Sigma_3 + |\Sigma_4|,$$

where

$$\Sigma_1 = \left|\sum_{n\le U} \Lambda(n) f(n)\right|,$$

$$\Sigma_2 = (\log UV) \sum_{v\le UV} \left|\sum_{s\le N/v} f(sv)\right|,$$

$$\Sigma_3 = (\log N) \sum_{v\le V} \max_{w\ge 1} \left|\sum_{w\le s\le N/v} f(sv)\right|,$$

$$\Sigma_4 = \sum_{\substack{k\ell\le N\\ k>V,\ \ell>U}} \Lambda(\ell) \left|\sum_{d|k,\ d\le V} \mu(d)\right| f(k\ell).$$

We also need the following result which follows from Theorem 1 of [29] using the standard reduction of incomplete sums to complete ones (see, for example, [8]).

Lemma 5. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$ and let $G \in \mathcal{E}(\mathbb{F}_p)$ be a point of order T. Then, for real numbers $H_1 < H_2$ and any integer a not divisible by p, the following estimate holds:*

$$\sum_{H_1<n\le H_2} \mathbf{e}_p(a\mathbf{x}(nG)) \ll \left(\frac{H_2-H_1}{T}+1\right) p^{1/2}\log p.$$

We are now ready to prove:

Theorem 6. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$, and let $G \in \mathcal{E}(\mathbb{F}_p)$ be a point of order T. Then, for every $a \in \mathbb{F}_p^*$, we have*

$$\sum_{n\le N} \Lambda(n)\mathbf{e}_p(a\mathbf{x}(nG)) \ll \left(NT^{-1}p^{1/2} + N^{2/3}T^{5/9}p^{1/18}\right) N^{\varepsilon}$$

where the implied constant depends only on ε.

Proof. We remark that the bound of the theorem is trivial if $N \ll T^{5/3}p^{1/6}$; hence we can assume that $T^{5/3}p^{1/6} = o(N)$. In particular, $\log p \ll \log N$.

Let $U, V > 1$ with $UV \le N$ and apply Lemma 4 with the function $f(n) = \mathbf{e}_p(a\mathbf{x}(nG))$. By Chebyshev's bound we have

$$\Sigma_1 = \left|\sum_{n\le U} \Lambda(n) f(n)\right| \le \sum_{n\le U} \Lambda(n) \ll U. \tag{11}$$

Next, for any $v \ge 1$ the point vG has order $T/\gcd(v,T)$ in $\mathcal{E}(\mathbb{F}_p)$; thus Lemma 5 provides the bound

$$\begin{aligned}\Sigma_2 &= (\log UV) \sum_{v \le UV} \left| \sum_{s \le N/v} \mathbf{e}_p(a\mathbf{x}(svG)) \right| \\ &\ll \log N \sum_{v \le UV} \left(\frac{N \gcd(v,T)}{vT} + 1 \right) p^{1/2} \log p \\ &\le NT^{-1} p^{1/2} \log N \log p \sum_{v \le UV} \frac{\gcd(v,T)}{v} + UVp^{1/2} \log N \log p.\end{aligned}$$

Also,

$$\begin{aligned}\sum_{v \le UV} \frac{\gcd(v,T)}{v} &= \sum_{d \mid T} \sum_{\substack{v \le UV \\ \gcd(v,T)=d}} \frac{d}{v} \le \sum_{d \mid T} \sum_{\substack{v \le UV \\ d \mid v}} \frac{d}{v} \\ &= \sum_{d \mid T} \sum_{w \le UV/d} \frac{1}{w} \ll \sum_{d \mid T} \log UV \le \tau(T) \log N.\end{aligned}$$

Therefore, since $\log p \ll N^{\varepsilon}$, we derive the estimate

$$\Sigma_2 \ll \left(NT^{-1} p^{1/2} + UVp^{1/2} \right) N^{\varepsilon}. \tag{12}$$

Similarly we have

$$\Sigma_3 \ll \left(NT^{-1} p^{1/2} + Vp^{1/2} \right) N^{\varepsilon}. \tag{13}$$

We now turn to the estimate of Σ_4. For every positive integer k let

$$A(k) = \left| \sum_{d \mid k, \ d \le V} \mu(d) \right|.$$

Then, since $k, \ell \le N$,

$$A(k) \le \tau(k) \ll N^{\varepsilon} \qquad \text{and} \qquad \Lambda(\ell) \le \log \ell \ll N^{\varepsilon}. \tag{14}$$

Now, let Δ be fixed in the range $1/V < \Delta < 1/2$ and define the set

$$\Omega = \left\{ V(1+\Delta)^j : 0 \le j \le R \right\},$$

where

$$R = \left\lfloor \frac{\log(N/V)}{\log(1+\Delta)} \right\rfloor \ll \Delta^{-1} \log N.$$

Then,

$$\Sigma_4 = \sum_{\substack{k\ell \le N \\ k > V, \ell > U}} A(k)\, \Lambda(\ell)\, \mathbf{e}_p(a\mathbf{x}(k\ell G)) = \sum_{K \in \Omega} \sigma(K),$$

where

$$\sigma(K) = \sum_{\substack{K<k\le K(1+\Delta)\\ k<N/U}} \sum_{U<\ell\le N/k} A(k)\,\Lambda(\ell)\,\mathbf{e}_p(a\mathbf{x}(k\ell G)).$$

For any k in the range $K < k \le K(1+\Delta)$ we have $N/k = N/K + O(\Delta N/K)$. Since $\Delta K \ge \Delta V > 1$, it follows from (14) that

$$\sigma(K) = \widetilde{\sigma}(K) + O\left(\Delta^2 N^{1+\varepsilon}\right),$$

where

$$\widetilde{\sigma}(K) = \sum_{\substack{K<k\le K(1+\Delta)\\ k<N/U}} \sum_{U<\ell\le N/K} A(k)\,\Lambda(\ell)\,\mathbf{e}_p(a\mathbf{x}(k\ell G)).$$

Since Ω has at most $O(\Delta^{-1}\log N)$ elements, it follows that

$$\Sigma_4 = \sum_{K\in\Omega} \widetilde{\sigma}(K) + O\left(\Delta N^{1+\varepsilon}\right). \tag{15}$$

We now estimate each $\widetilde{\sigma}(K)$ using Theorem 3 together with (14), obtaining

$$\begin{aligned}\widetilde{\sigma}(K) &\ll N^{\varepsilon} T^{5/6} p^{1/12} \left(\Delta K \cdot (N/K)\right)^{1/2}\\ &= \Delta^{1/2} N^{1/2+\varepsilon} T^{5/6} p^{1/12}.\end{aligned}$$

Applying this estimate to (15), we have

$$\Sigma_4 \ll \left(\Delta^{-1/2} N^{1/2} T^{5/6} p^{1/12} + \Delta N\right) N^{\varepsilon}.$$

Combining the preceding result with (11), (12), and (13) we find that

$$\sum_{n\le N} \Lambda(n)\mathbf{e}_p(a\mathbf{x}(nG)) \ll (B_1 + B_2 + B_3 + B_4)N^{\varepsilon},$$

where

$$\begin{aligned}B_1 &= NT^{-1}p^{1/2},\\ B_2 &= UVp^{1/2},\\ B_3 &= \Delta^{-1/2}N^{1/2}T^{5/6}p^{1/12},\\ B_4 &= \Delta N.\end{aligned}$$

We now choose $U = V = N^{1/2}T^{-1/2}$, which balances the terms B_1 and B_2, and we choose $\Delta = N^{-1/3}T^{5/9}p^{1/18}$ to balance the terms B_3 and B_4. Thus,

$$B_1 = B_2 = NT^{-1}p^{1/2} \qquad \text{and} \qquad B_3 = B_4 = N^{2/3}T^{5/9}p^{1/18}.$$

With these choices, we remark that the condition $1/V < \Delta < 1/2$ is satisfied since $T^{5/3}p^{1/6} = o(N)$. The result follows. □

Using partial summation we immediately obtain the following corollary to Theorem 6.

Corollary 7. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$, and let $G \in \mathcal{E}(\mathbb{F}_p)$ be a point of order T. Then, for every $a \in \mathbb{F}_p^*$ we have*

$$\sum_{q \le N} \mathbf{e}_p(a\mathbf{x}(qG)) \ll \left(NT^{-1}p^{1/2} + N^{2/3}T^{5/9}p^{1/18}\right) N^{\varepsilon}$$

where the sum is taken over prime numbers $q \le N$ and the implied constant depends only on ε.

2.3. **Sums with the Power Generator.** We now apply Theorem 3 to estimate the incomplete exponential sums relevant to the sequence (5).

Theorem 8. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$. Suppose that $G \in \mathcal{E}(\mathbb{F}_p)$ is a point of order T and e is an integer with $\gcd(e,T) = 1$ of multiplicative order t modulo T. Then, for $1 \le N \le t$ and every $a \in \mathbb{F}_p^*$, we have*

$$\sum_{n=0}^{N-1} \mathbf{e}_p(a\mathbf{x}(U_n)) \ll T^{5/9}N^{1/3}p^{1/18+\varepsilon},$$

where the implied constant depends only on ε.

Proof. For any positive integer $K \le t$ we have

$$\begin{aligned}\sum_{n=0}^{N-1} \mathbf{e}_p(a\mathbf{x}(U_n)) &= \frac{1}{K}\sum_{k=0}^{K-1}\sum_{n=0}^{N-1} \mathbf{e}_p(a\mathbf{x}(U_{k+n})) + O(K)\\ &= \frac{1}{K}\sum_{k=0}^{K-1}\sum_{n=0}^{N-1} \mathbf{e}_p(a\mathbf{x}(e^{k+n}G)) + O(K)\\ &= \frac{1}{K}\sum_{k=0}^{K-1}\sum_{n=0}^{N-1} \mathbf{e}_p(a\mathbf{x}(e^{k}e^{n}G)) + O(K).\end{aligned}$$

Using Theorem 3 to estimate the above double sum we derive

$$\sum_{n=0}^{N-1} \mathbf{e}_p(a\mathbf{x}(U_n)) \ll K^{-1}T^{5/6}(KN)^{1/2}p^{1/12+\varepsilon} + K$$

and optimising the choice of K as $K = \lceil T^{5/9}N^{1/3}p^{1/18}\rceil$ we obtain the desired result (clearly, we can assume that for the above choice we have $K \le t$, otherwise the bound is trivial). □

It is easy to check that if, for example, $T = p^{1+o(1)}$ then the bound of Theorem 8 is nontrivial for $t \ge N \ge p^{11/12+\varepsilon}$ and so, by the well-known Weyl criterion, the sequence $\{U_n,\ 0 \le n \le N-1\}$ is uniformly distributed in this range of the parameters .

3. Multiplicative Character Sums

3.1. **Double Sums.** Here, instead of Lemma 1, we use the classical *Weil bound* for multiplicative character sums; see Chapter 5 of [33].

Lemma 9. *Let $f(X) \in \mathbb{F}_p(X)$ be a nonconstant rational function of degree at most L which has no multiple roots nor multiple poles. Let χ be a nonprincipal character of $\mathbb{F}_p^*$. Then we have*

$$\sum_{\lambda \in \mathcal{H}}{}^{*} \chi\left(f(\lambda)\right) \ll L p^{1/2},$$

where $\mathcal{H}$ is an arbitrary subgroup of $\mathbb{F}_p^*$, and Σ^* indicates that the poles of f are excluded from the summation.

Theorem 10. *Let χ be a nonprincipal multiplicative character of $\mathbb{F}_p^*$, and let ϑ be an element of multiplicative order T in $\mathbb{F}_p^*$. Then, for all subsets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_T$ and all $a \in \mathbb{F}_p^*$ the following bound holds:*

$$W_a(\mathcal{U}, \mathcal{V}; \chi) \ll ABT^{3/4}(\#\mathcal{U}\#\mathcal{V})^{1/2} p^{1/8+\varepsilon}.$$

where

$$A = \max_{u \in \mathcal{U}} |\alpha_u| \ , \ B = \max_{v \in \mathcal{V}} |\beta_v| \ ,$$

and the implied constant depends only on ε.

Proof. The proof is analogous to that of Theorem 3. Here we choose K slightly differently as $K = \lceil T^{1/2} p^{-1/4} \rceil$. We have the following analogue of (9):

$$|W_a(\mathcal{U}, \mathcal{V}; \chi)| \le A \sum_{d \,|\, T} \widetilde{\sigma}_d, \tag{16}$$

where

$$\widetilde{\sigma}_d = \sum_{u \in \mathcal{U}} \left| \sum_{v \in \mathcal{V}_d} \beta_v \chi\left(\vartheta^{uv} + a\right) \right| .$$

Arguing as before, we eventually arrive at the inequality:

$$\widetilde{\sigma}_d^2 \ll \frac{B^2 T \#\mathcal{U}}{K^2} \sum_{z \in \mathbb{Z}_{T/d}^*} \sum_{\substack{k,m \in \mathcal{K} \\ dkz \in \mathcal{V}_d \\ dmz \in \mathcal{V}_d}} \left| \sum_{\lambda \in \mathcal{H}_d} \chi\left(\frac{\lambda^k + a}{\lambda^m + a}\right) \right| ,$$

where $\mathcal{H}_d = \langle \vartheta^d \rangle$ is the subgroup of $\mathbb{F}_p^*$ generated by ϑ^d. If $k \neq m$, we use Lemma 9 together with (10) to estimate the innermost sum as $O(Kp^{1/2+\varepsilon})$, whereas if

$k = m$ the value of the sum is $\#\mathcal{H}_d = T/d$. This leads to the estimate:

$$\begin{aligned}\widetilde{\sigma}_d^2 &\ll \frac{B^2 T p^{1/2+\varepsilon} \#\mathcal{U}}{K} \sum_{z \in \mathbb{Z}_{T/d}^*} \sum_{\substack{k,m \in \mathcal{K} \\ dkz \in \mathcal{V}_d \\ dmz \in \mathcal{V}_d}} 1 + \frac{B^2 T^2 \#\mathcal{U}}{dK^2} \sum_{z \in \mathbb{Z}_{T/d}^*} \sum_{\substack{k \in \mathcal{K} \\ dkz \in \mathcal{V}_d}} 1 \\ &\le B^2 T K p^{1/2+\varepsilon} \#\mathcal{U} \#\mathcal{V} + d^{-1} K^{-1} B^2 T^2 \#\mathcal{U} \#\mathcal{V} \\ &= B^2 T \#\mathcal{U} \#\mathcal{V} (K p^{1/2+\varepsilon} + T K^{-1}).\end{aligned}$$

Recalling our choice of K, which balances the two terms in this estimate, we find that

$$\widetilde{\sigma}_d \ll B T^{3/4} (\#\mathcal{U} \#\mathcal{V})^{1/2} p^{1/8+\varepsilon}.$$

Substituting this bound in (16) and using again the fact that $\tau(T) \ll p^{\varepsilon}$, we conclude the proof. □

3.2. **Sums over Primes.** In this subsection, we apply the bound of Theorem 10 to estimate the sums $S_a(N; \chi)$ defined by (8). The following result, an analogue of Lemma 5, follows immediately from results given in [12, 41]:

Lemma 11. *Let χ be a nonprincipal multiplicative character of $\mathbb{F}_p^*$, and let ϑ be an element of multiplicative order T in $\mathbb{F}_p^*$. Then, for real numbers $H_1 < H_2$ and any integer a not divisible by p, the following estimate holds:*

$$\sum_{H_1 < n \le H_2} \chi(\vartheta^n + a) \ll \left(\frac{H_2 - H_1}{T} + 1 \right) p^{1/2} \log p.$$

We are now ready to prove:

Theorem 12. *Let χ be a nonprincipal multiplicative character of $\mathbb{F}_p^*$ and let ϑ be an element of multiplicative order T in $\mathbb{F}_p^*$. Then, for every $a \in \mathbb{F}_p^*$ we have*

$$\sum_{n \le N} \Lambda(n) \chi(\vartheta^n + a) \ll \left(N T^{-1} p^{1/2} + N^{2/3} T^{1/2} p^{1/12} \right) N^{\varepsilon}$$

where the implied constant depends only on ε.

Proof. Since the bound of the theorem is trivial if $N \ll T^{3/2} p^{1/4}$ we can assume that $T^{3/2} p^{1/4} = o(N)$; in particular $\log p \ll N^{\varepsilon}$.

Let $U, V > 1$ with $UV \le N$ and apply Lemma 4 with the function $f(n) = \chi(\vartheta^n + a)$. Proceeding as in the proof of Theorem 6 (and using similar notation), but applying Lemma 11 in place of Lemma 5, we derive that

$$\Sigma_1 \ll U, \tag{17}$$

$$\Sigma_2 \ll \left(N T^{-1} p^{1/2} + U V p^{1/2} \right) N^{\varepsilon}, \tag{18}$$

$$\Sigma_3 \ll \left(N T^{-1} p^{1/2} + V p^{1/2} \right) N^{\varepsilon}, \tag{19}$$

and

$$\Sigma_4 = \sum_{K \in \Omega} \widetilde{\sigma}(K) + O\left(\Delta N^{1+\varepsilon}\right), \tag{20}$$

where

$$\widetilde{\sigma}(K) = \sum_{\substack{K<k\le K(1+\Delta)\\ k<N/U}} \sum_{U<\ell\le N/K} A(k)\,\Lambda(\ell)\,\chi(\vartheta^{k\ell}+a).$$

We now estimate each $\widetilde{\sigma}(K)$ using Theorem 10 together with (14), obtaining

$$\begin{aligned}\widetilde{\sigma}(K) &\ll N^{\varepsilon}T^{3/4}p^{1/8}\left(\Delta K\cdot(N/K)\right)^{1/2}\\ &= \Delta^{1/2}N^{1/2+\varepsilon}T^{3/4}p^{1/8}.\end{aligned}$$

Applying this estimate to (20), we have

$$\Sigma_4 \ll \left(\Delta^{-1/2}N^{1/2}T^{3/4}p^{1/8} + \Delta N\right)N^{\varepsilon}.$$

Combining the preceding result with (17), (18), and (19), we see that

$$\sum_{n\le N}\Lambda(n)\chi(\vartheta^n+a) \ll (B_1+B_2+B_3+B_4)N^{\varepsilon},$$

where

$$\begin{aligned}B_1 &= NT^{-1}p^{1/2},\\ B_2 &= UVp^{1/2},\\ B_3 &= \Delta^{-1/2}N^{1/2}T^{3/4}p^{1/8},\\ B_4 &= \Delta N.\end{aligned}$$

We again choose $U = V = N^{1/2}T^{-1/2}$ which balances the terms B_1 and B_2, and we choose $\Delta = N^{-1/3}T^{1/2}p^{1/12}$ to balance the terms B_3 and B_4. Thus,

$$B_1 = B_2 = NT^{-1}p^{1/2} \qquad \text{and} \qquad B_3 = B_4 = N^{2/3}T^{1/2}p^{1/12}.$$

With these choices we remark that the condition $1/V < \Delta < 1/2$ is satisfied since $T^{3/2}p^{1/4} = o(N)$. The result follows. □

Using partial summation, we immediately obtain the following corollary to Theorem 12:

Corollary 13. *Let χ be a nonprincipal multiplicative character of $\mathbb{F}_p^*$ and let ϑ be an element of multiplicative order T in $\mathbb{F}_p^*$. Then, for every $a \in \mathbb{F}_p^*$ the following estimate holds:*

$$\sum_{q\le N}\chi(\vartheta^q+a) \ll \left(NT^{-1}p^{1/2} + N^{2/3}T^{1/2}p^{1/12}\right)N^{\varepsilon},$$

where the sum is taken over prime numbers $q \le N$ and the implied constant depends only on ε.

3.3. **Sums with Double Exponential Sequences.** Similarly to the proof of Theorem 8 one can derive from Theorem 10 the following estimate.

Theorem 14. *Let χ be a nonprincipal multiplicative character of $\mathbb{F}_p^*$. Suppose that ϑ is an element of multiplicative order T in $\mathbb{F}_p^*$ and e is an integer with* $\gcd(e,T)=1$ *of multiplicative order t modulo T. Then, for $1 \le N \le t$ and every $a \in \mathbb{F}_p^*$, we have*

$$\sum_{n=0}^{N-1} \chi(\vartheta^{e^n}+a) \ll T^{1/2}N^{1/3}p^{1/12+\varepsilon},$$

where the implied constant depends only on ε.

It is easy to check that if $T = p^{1+o(1)}$ then the bound of Theorem 14 is nontrivial for $t \ge N \ge p^{7/8+\varepsilon}$.

4. Remarks

It is easy to see that, if N is exponentially large compared to q, then the bounds of Theorem 6 and 12 become trivial due to the presence of the factor N^ε. However, the case of such long sums can be dealt with by using results about the distribution of primes in arithmetic progressions, in exactly the same fashion as in [1].

Variants of our main bounds for the sums $W_a(\mathcal{U},\mathcal{V})$ and $W_a(\mathcal{U},\mathcal{V};\chi)$ can be given, as has been done in [1], in terms of the ℓ_2–norms of the sequences α, β rather than the sup–norm, and this has many potential applications, especially for thin sequences. As in [21], we also remark that similar arguments allow us to estimate the higher moments

$$\sum_{u\in\mathcal{U}} \left|\sum_{v\in\mathcal{V}} \beta_v\, \mathbf{e}_p(a\mathbf{x}(uvG))\right|^k \qquad \text{and} \qquad \sum_{u\in\mathcal{U}} \left|\sum_{v\in\mathcal{V}} \beta_v\, \chi(\vartheta^{uv}+a)\right|^k,$$

for an integer $k \ge 1$ and $a \in \mathbb{F}_p^*$.

In the same way as Theorem 3 implies Theorem 8, the bound of exponential sums from [21] leads to the estimate

$$\sum_{n=0}^{N-1} \mathbf{e}_p(a\vartheta^{e^n}) \ll T^{1/2}N^{1/3}p^{1/12+\varepsilon},$$

for $1 \le N \le t$ and $a \in \mathbb{F}_p^*$, which complements the bound from [13] for complete sums of this type.

Finally, using the same ideas as in [2], one can also estimate the sums

$$\sum_{\substack{s\le N\\ s\ M-\text{smooth}}} \mathbf{e}_p(a\mathbf{x}(sG)) \qquad \text{and} \qquad \sum_{\substack{s\le N\\ s\ M-\text{smooth}}} \chi(\vartheta^s + a)$$

over M-smooth positive integers $s \le N$ (that is, over the integers which are not divisible by any primes $q > M$).

References

[1] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, 'Exponential sums with Mersenne numbers', *Compos. Math.*, **140** (2004), 15–30.

[2] W. Banks, J. B. Friedlander, M. Garaev and I. E. Shparlinski, 'Character sums with exponential functions over smooth numbers', *Indag. Math.*, (to appear).

[3] I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc., Lecture Note Series, **265**, Cambridge Univ. Press, 1999.

[4] I. Blake, G. Seroussi and N. Smart, *Advances in elliptic curve cryptography*, London Math. Soc., Lecture Note Series, **317**, Cambridge Univ. Press, 2005.

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

[6] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, 'On the statistical properties of Diffie–Hellman distributions', *Israel J. Math.*, **120** (2000), 23–46.

[7] R. Canetti, J. B. Friedlander and I. E. Shparlinski, 'On certain exponential sums and the distribution of Diffie–Hellman triples', *J. London Math. Soc.*, **59** (1999), 799–812.

[8] J. H. H. Chalk, 'Polynomial congruences over incomplete residue systems modulo k', *Proc. Kon. Ned. Acad. Wetensch.*, **A92** (1989), 49–62.

[9] F. R. K. Chung, 'Several generalizations of Weil sums', *J. Number Theory*, **49** (1994), 95–106.

[10] T. W. Cusick, C. Ding and A. Renvall, *Stream ciphers and number theory*, Elsevier, Amsterdam, 2004.

[11] H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York 1980.

[12] 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.

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

[14] J. B. Friedlander, J. Hansen and I. E. Shparlinski, 'On the distribution of the power generator modulo a prime power', *Proc. DIMACS Workshop on Unusual Applications of Number Theory, 2000*, Amer. Math. Soc., 2004, 71–79.

[15] J. Friedlander and H. Iwaniec, 'Estimates for character sums', *Proc. Amer. Math. Soc.*, **119** (1993), 363–372.

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

[17] J. B. Friedlander, D. Lieman and I. E. Shparlinski, 'On the distribution of the RSA generator', *Proc. Intern. Conf. on Sequences and their Applications, Singapore 1998*, Springer-Verlag, London, 1999, 205–212.

[18] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, 'Period of the power generator and small values of Carmichael's function', *Math. Comp.*, **70** (2001), 1591–1605 (see also **71** (2002), 1803-1806).

[19] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, **70** (2001), 1575–1589.

[20] J. B. Friedlander and I. E. Shparlinski, 'Double exponential sums over thin sets', *Proc. Amer. Math. Soc.*, **129** (2001), 1617–1621.

[21] M. Z. Garaev, 'Double exponential sums related to Diffie–Hellman distributions', *Int. Math. Res. Notices*, **2005:17** (2005), 1005–1014.

[22] D. Hankerson, A. Menezes and S. Vanstone, *Elliptic curve cryptography*, Springer-Verlag, Berlin, 2004.

[23] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[24] F. Hess and I. E. Shparlinski, 'On the linear complexity and multidimensional distribution of congruential generators over elliptic curves', *Designs, Codes and Cryptography*, **35** (2005), 111–117.

[25] H. Iwaniec and A. Sárközy, 'On a multiplicative hybrid problem', *J. Number Theory*, **26** (1987), 89–95.

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

[27] A. A. Karatsuba, 'Kloosterman double sums', *Matem. Zametki*, **66** (1999), 682–687 (in Russian).

[28] N. Koblitz, 'Elliptic curve cryptosystem', *Math. Comp.*, **48** (1987), 203–209.

[29] D. R. Kohel and I. E. Shparlinski, 'Exponential sums and group generators for elliptic curves over finite fields', *Proc. the 4th Algorithmic Number Theory Symp., Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1838** (2000), 395–404.

[30] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.*, (to appear).

[31] J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143.

[32] T. Lange and I. E. Shparlinski, 'Certain exponential sums and random walks on elliptic curves', *Canad. J. Math.*, **57** (2005), 338–350.

[33] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[34] V. Miller, 'Use of elliptic curves in cryptography', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **218** (1986), 224–314.

[35] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.

[36] A. Sárközy, 'On the distribution of residues of products of integers', *Acta Math. Hungar.*, **49** (1987), 397–401.

[37] I. E. Shparlinski, 'On the distribution of primitive and irreducible polynomials modulo a prime', *Diskretnaja Matem.*, **1** (1989), no.1, 117–124 (in Russian).

[38] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[39] R. C. Vaughan, 'An elementary method in prime number theory', *Acta Arith.*, **37** (1980), 111–115.

[40] I. M. Vinogradov, *Elements of Number Theory*, Dover Publ., NY, 1954.

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

William D. Banks
Department of Mathematics
University of Missouri Columbia, MO 65211, USA
E-mail: bbanks@math.missouri.edu

John B. Friedlander
Department of Mathematics
University of Toronto
OntarioM5S 3G3, Canada
E-mail: frdlndr@math.toronto.edu

Moubariz Z. Garaev
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
E-mail: garaev@matmor.unam.mx

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