ACTA ARITHMETICA
148.1 (2011)

Twisted exponential sums over points of elliptic curves

by

Alina Ostafe (Zürich) and Igor E. Shparlinski (Sydney)

1. Introduction. Let $p \geq 5$ be a prime and $\mathbf{E}$ be an elliptic curve defined over a finite field $\mathbb{F}_p$ of p elements given by an affine Weierstraß equation

$$\mathbf{E} : Y^2 = X^3 + aX + b$$

with some $a, b \in \mathbb{F}_p$ (see [1, 3, 23]).

We recall that the set of all points on $\mathbf{E}$ forms an abelian group, with the "point at infinity" $\mathcal{O}$ as the neutral element, and we use $\oplus$ to denote the group operation. As usual, we write every point $P \neq \mathcal{O}$ on $\mathbf{E}$ as $P = (x(P), y(P))$.

Let $\mathbf{E}(\mathbb{F}_p)$ denote the set of $\mathbb{F}_p$-rational points on $\mathbf{E}$. We recall that the celebrated result of Bombieri [4] implies in particular an estimate of order $p^{1/2}$ for exponential sums with functions from the function field of $\mathbf{E}$ taken over all points of $\mathbf{E}(\mathbb{F}_p)$. More recently, various character sums over points of elliptic curves have been considered in a number of papers (see [2, 7, 10, 11, 14, 15, 16, 18, 20]) and references therein; many of these estimates are motivated by applications to pseudorandom number generators on elliptic curves [19].

Let $\mathbb{Z}_m^*$ denote the unit group of the residue ring $\mathbb{Z}_m$ modulo a positive integer m. We also denote

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

We fix a point $P \in \mathbf{E}(\mathbb{F}_p)$ of order t and a rational function $H \in \mathbb{Z}(X)$ of the form

$$H(X) = b_1 X^{e_1} + \cdots + b_d X^{e_d}, \tag{1}$$

where $b_1, \ldots, b_d, e_1, \ldots, e_d \in \mathbb{Z}$. We consider the character sums

$$S(a, H) = \sum_{n \in \mathbb{Z}_t \setminus \{0\}} \mathbf{e}_p(ax(nP))\mathbf{e}_t(H(n))$$

2010 *Mathematics Subject Classification*: 11L07, 11T23, 14H52.
Key words and phrases: elliptic curves, polynomials, exponential sums.

DOI: 10.4064/aa148-1-6

if all exponents $e_1, \ldots, e_d$ are positive and

$$S^*(a, H) = \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ax(nP))\mathbf{e}_t(H(n))$$

for arbitrary exponents $e_1, \ldots, e_d$, where $\mathbb{Z}_t^*$ is the group of units of the residue ring $\mathbb{Z}_t$ modulo t.

Certainly if $d = 1$, $e_1 = -1$ then the sum

$$\sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ax(nP))\mathbf{e}_t(bn^{-1}) = \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ax(n^{-1}P))\mathbf{e}_t(bn), \tag{2}$$

resembles the classical *Kloosterman sums* (see [13]). We use the method of [6, 21] to derive nontrivial estimates of these sums provided that $t \ge p^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$.

Furthermore, for the sums $S(a, F)$, in the case where $F(X) \in \mathbb{Z}[X]$ is a polynomial and also for the sums

$$T(a, f; N) = \sum_{n=1}^{N} \mathbf{e}_p(ax(nP))\mathbf{e}(f(n))$$

with a polynomial $f(X) \in \mathbb{R}[X]$ and an integer $N < t$, we use a different method to obtain estimates of a different type.

Note that if $F(X) = bX$ is a linear polynomial then [14, Corollary 1] yields the bound

$$S(a, F) = O(p^{1/2}). \tag{3}$$

Moreover, in the case of linear polynomials $f(X) = \beta X$ the sums $T(a, f; N)$ have been estimated in [18] as

$$T(a, f; N) = O(N^{1/2}p^{1/4}). \tag{4}$$

We use the bounds (3) and (4) as the bases of our inductive arguments which extend them to polynomials of arbitrary degree.

The sums $S(a, H)$, $S^*(a, H)$ and $T(a, f; N)$ are analogues of several sums considered in [6, 21, 22] over elements of cyclic subgroups of $\mathbb{F}_p^*$ instead of cyclic subgroups of $\mathbf{E}(\mathbb{F}_p)$, as in the present work. We also remark that taking $k = 4$, $l = 8$ in [21, Theorem 3.1] (instead of $k = 3$, $l = 4$ as in [21]), one improves the exponent in [21, bound (1)] from 239/240 to 127/128. More precisely, with the choice $k = 4$, $l = 8$ we see that [21, Theorem 3.1] implies the bound

$$\max_{a \in \mathbb{F}_p^*} \max_{b \in \mathbb{Z}_t} \left| \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ag^{1/n})\mathbf{e}_t(bn) \right| \le t^{127/128+o(1)},$$

where $g \in \mathbb{F}_p^*$ is of multiplicative order $t = p^{1+o(1)}$ (for example, a primitive root).

Finally we note that general estimates of "pure" exponential sums with monomial rational functions of the type (1) have been derived in [17] (see (10) below), which we actually also use as a part of our argument, see Lemma 5. In some special cases, more precise estimates than (10) are given in [5, 9].

Some of our results (those which are based on [15]) apply only to ordinary (or nonsupersingular) curves, some apply to arbitrary curves (see [1, 3, 23] for definitions of ordinary and supersingular elliptic curves).

Throughout the paper, the implied constants in the symbols "O" and "$\ll$" may occasionally depend on the exponents $e_1, \dots, e_d$ and the integer parameters k, l, s, and are absolute otherwise (we recall that $U \ll V$ and $U = O(V)$ are both equivalent to the inequality $|U| \le cV$ with some constant $c > 0$).

2. Preliminaries

2.1. Exponential sums over elliptic curves. In one of our main results we need to estimate exponential sums with multiples of a point P on an elliptic curve. The following result gives us an upper bound for this kind of exponential sums (see [15, Corollary 5]), which is the main tool in our results.

LEMMA 1. *Let $\mathbf{E}$ be an ordinary curve defined over $\mathbb{F}_p$. For any integers $1 \le u_1 < \dots < u_s \le U$ and elements $c_1, \dots, c_s \in \mathbb{F}_p$ with $c_s \ne 0$, the following bound holds:*

$$\sum_{\substack{R \in \mathcal{H} \\ R \ne \mathcal{O}}} \mathbf{e}_p\Big(\sum_{i=1}^{s} c_i x(u_i R)\Big) \ll U^2 p^{1/2},$$

where $\mathcal{H}$ is an arbitrary subgroup of $\mathbf{E}(\mathbb{F}_p)$ of order $t = \#\mathcal{H}$ such that $\gcd(t, u_1, \dots, u_s) = 1$.

In order to estimate exponential sums with rational functions in the function field of an elliptic curve $\mathbf{E}$ we use the following bound from [14], which in turn is a generalization of the classical bound of [4].

LEMMA 2. *For any point $P \in \mathbf{E}(\mathbb{F}_p)$ of order t, for any integer b and for any rational function $\psi(X, Y) \in \mathbb{F}_p(X, Y)$ of degree d, which is not constant on $\mathbf{E}$, the bound*

$$\sum_{n \in \mathbb{Z}_t}^{*} \mathbf{e}_p(\psi(nP))\mathbf{e}_t(bn) = O(p^{1/2})$$

holds, where $\sum^*$ means that the poles of $\psi(X, Y)$ are excluded from the summation.

Let f be any rational function in $\mathbb{F}_p(X, Y)$ which is not constant on $\mathbf{E}$ and let Q be a generic point on $\mathbf{E}$. For $\mathbf{a} = (a_1, \dots, a_s) \in \mathbb{F}_p^s$ and $\mathbf{W} =$

$(W_1, \ldots, W_s) \in \mathbf{E}^s$ we consider the function

$$\mathcal{L}_{\mathbf{a},\mathbf{W}}(Q) = \sum_{j=1}^{s} a_j x(W_j \oplus Q)$$

as a function in the function field $\mathbb{F}_p(\mathbf{E})$.

We use Lemma 2 in combination with the following special case of [12, Lemma 1].

LEMMA 3. *For any nonzero vector* $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{F}_p^s$, *and for any vector* $\mathbf{W} = (W_1, \ldots, W_s) \in \mathbf{E}^s$ *with* $W_i \neq W_j$, $1 \le i < j \le s$, *the function* $\mathcal{L}_{\mathbf{a},\mathbf{W}}(Q)$ *is not constant on* $\mathbf{E}$.

2.2. Symmetric systems of congruences. Our estimates depend on upper bounds on the number of solutions of some systems of symmetric congruences.

Let $\mathbf{e} = (e_1, \ldots, e_d) \in \mathbb{Z}^d$. If all exponents $e_1, \ldots, e_d$ are nonnegative, then we denote by $N_k(\mathbf{e}; t)$ the number of solutions of the symmetric system of congruences

$$\sum_{j=1}^{2k} (-1)^j n_j^{e_i} \equiv 0 \pmod{t}, \qquad i = 1, \ldots, d,$$

with $n_1, \ldots, n_{2k} \in \mathbb{Z}_t$. Furthermore, for arbitrary nonzero exponents $e_1, \ldots, e_d$, we denote by $N_k^*(\mathbf{e}; t)$ the number of solutions of the same system of congruences with variables $n_1, \ldots, n_{2k} \in \mathbb{Z}_t^*$.

Clearly we have the trivial bounds

$$N_k^*(\mathbf{e}; t) \ll t^{2k-1} \quad \text{and} \quad N_k(\mathbf{e}; t) \ll t^{2k-1}, \tag{5}$$

which are the best possible if $d = 1$ (and certainly we have $N_k^*(\mathbf{e}; t) \le N_k(\mathbf{e}; t)$ when $N_k(\mathbf{e}; t)$ is defined). However, for t with a small square-full part a much better bound follows by a slight modification of a result of [8, 24].

LEMMA 4. *Assume that* $t \to \infty$ *over a sequence of integers such that for the largest square divisor* $v^2 \mid t$ *we have* $v = t^{o(1)}$. *If the components of the vector* $\mathbf{e} = (e_1, \ldots, e_d)$ *are pairwise distinct positive integers, then for* $k \ge d$ *we have*

$$N_k^*(\mathbf{e}; t) \le N_k(\mathbf{e}; t) \le t^{2k-d+o(1)}.$$

Proof. First of all we recall that if $t = q$ is prime then by [8, Lemma 3.1] or [24, Theorem 1.2] we have

$$N_d(\mathbf{e}; q) \le E q^d \tag{6}$$

where E depends only on $\mathbf{e}$.

We recall that for any integer $m \ge 1$ we have the identity

$$\frac{1}{m}\sum_{r\in\mathbb{Z}_m} \mathbf{e}_m(rv) = \begin{cases} 1 & \text{if } v \equiv 0 \pmod m,\\ 0 & \text{if } v \not\equiv 0 \pmod m.\end{cases}$$

Therefore, for any integers $h_1, \dots, h_d$, the number of solutions to the system of congruences

$$\sum_{j=1}^{2d} (-1)^j n_j^{e_i} \equiv h_i \pmod q, \qquad i = 1, \dots, d, \tag{7}$$

can be written as

$$\begin{aligned}\frac{1}{q^d} \sum_{n_1,\dots,n_{2d}\in\mathbb{Z}_q} \prod_{i=1}^{d} \sum_{r_i\in\mathbb{Z}_q} \mathbf{e}_q\Big(r_i\Big(\sum_{j=1}^{2d}(-1)^j n_j^{e_i} - h_i\Big)\Big)\\ = \frac{1}{q^d} \sum_{r_1,\dots,r_d\in\mathbb{Z}_q} \mathbf{e}_q\Big(-\sum_{i=1}^{d} r_i h_i\Big) \prod_{j=1}^{2d} \sum_{n_j\in\mathbb{Z}_q} \mathbf{e}_q\Big((-1)^j \sum_{i=1}^{d} r_i n_j^{e_i}\Big)\\ = \frac{1}{q^d} \sum_{r_1,\dots,r_d\in\mathbb{Z}_q} \mathbf{e}_q\Big(-\sum_{i=1}^{d} r_i h_i\Big) \Big|\sum_{n\in\mathbb{Z}_q} \mathbf{e}_q\Big(\sum_{i=1}^{d} r_i n^{e_i}\Big)\Big|^{2d}.\end{aligned}$$

Since

$$\begin{aligned}\frac{1}{q^d} \sum_{r_1,\dots,r_d\in\mathbb{Z}_q} \mathbf{e}_q\Big(-\sum_{i=1}^{d} r_i h_i\Big) \Big|\sum_{n\in\mathbb{Z}_q} \mathbf{e}_q\Big(\sum_{i=1}^{d} r_i n^{e_i}\Big)\Big|^{2d}\\ \le \frac{1}{q^d} \sum_{r_1,\dots,r_d\in\mathbb{Z}_q} \Big|\sum_{n\in\mathbb{Z}_q} \mathbf{e}_q\Big(\sum_{i=1}^{d} r_i n^{e_i}\Big)\Big|^{2d} = N_d(\mathbf{e}; q),\end{aligned}$$

we see from (6) that for any $h_1, \dots, h_d$ the system of congruences (7) has at most Eq^d solutions. This immediately implies that for $k \ge d$ we have

$$N_k(\mathbf{e}; q) \le Eq^{2k-d}. \tag{8}$$

We now write $t = uv^2$ where u is square-free. Since by the Chinese Remainder Theorem $N_k(\mathbf{e}; t)$ is a multiplicative function of t, we see that

$$N_k(\mathbf{e}; t) \le (t/u)^{2k} N_k(\mathbf{e}; u) = (t/u)^{2k} \prod_{\substack{q\mid u\\ q\,\text{prime}}} N_k(\mathbf{e}; q).$$

Using (8) and the well-known estimate for the number $\omega(t)$ of prime divisors of t:

$$\omega(t) \le (1 + o(1)) \frac{\log t}{\log\log t} \tag{9}$$

(which follows immediately from the trivial inequalities $\omega(u)! \le u$ and $s! \ge (s/2)^{(s-1)/2}$), we now derive

$$\begin{aligned} N_k(\mathbf{e};t) &\le (t/u)^{2k} N_k(\mathbf{e};u) \le (t/u)^{2k} E^{\omega(u)} u^{2k-d} \\ &\le (t/u)^{2k} E^{\omega(t)} u^{2k-d} = t^{2k+o(1)} u^{-d} = t^{2k-d+o(1)} v^{2d}. \end{aligned}$$

Since $v = t^{o(1)}$, the result follows. ∎

We now show that if $d \ge 2$ then for $N_k^*(\mathbf{e};t)$ one can obtain an improvement of (5) by using the bound of exponential sums with monomial rational functions from [17]. Our main tool is the bound

$$\sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_t(r_1 n^{e_1} + \cdots + r_d n^{e_d}) \ll t^{1-1/d+o(1)} D^{1/d} \tag{10}$$

uniformly over integers $r_1, \ldots, r_d$ with $\gcd(r_1, \ldots, r_d, t) = D$, which follows from [17, Lemma 5] and the multiplicative property of exponential sums (see [13, equation (12.21)] or [17, Lemma 6]).

LEMMA 5. *If the components of the vector $\mathbf{e} = (e_1, \ldots, e_d)$ are pairwise distinct nonzero integers, then for any $k \ge 1$ and $d \ge 2$ we have*

$$N_k^*(\mathbf{e};t) \le \begin{cases} t^{2k-1-(2k-2)/d+o(1)}, & k < d(d-1)/2+1, \\ t^{2k-d+o(1)}, & k \ge d(d-1)/2+1. \end{cases}$$

Proof. As in the proof of Lemma 4, we have

$$N_k^*(\mathbf{e};t) = \frac{1}{t^d} \sum_{r_1,\ldots,r_d \in \mathbb{Z}_t} \Big| \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_t\Big(\sum_{i=1}^d r_i n^{e_i}\Big)\Big|^{2k}.$$

Now for each $D \mid t$ we collect together the terms with the same value of $\gcd(r_1, \ldots, r_d, t) = D$, getting

$$N_k^*(\mathbf{e};t) = \frac{1}{t^d} \sum_{D \mid t} \sigma_D, \tag{11}$$

where

$$\sigma_D = \sum_{\substack{r_1,\ldots,r_d \in \mathbb{Z}_t \\ \gcd(r_1,\ldots,r_d,t)=D}} \Big| \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_t\Big(\sum_{i=1}^d r_i n^{e_i}\Big)\Big|^{2k}.$$

We now write

$$\sigma_D = \sum_{\substack{r_1,\ldots,r_d \in \mathbb{Z}_t \\ \gcd(r_1,\ldots,r_d,t)=D}} \Big| \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_t\Big(\sum_{i=1}^d r_i n^{e_i}\Big)\Big|^{2k-2} \Big| \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_t\Big(\sum_{i=1}^d r_i n^{e_i}\Big)\Big|^{2}$$

and apply (10), getting

$$\sigma_D \le (t^{1-1/d+o(1)}D^{1/d})^{2k-2} \sum_{\substack{r_1,\dots,r_d\in\mathbb{Z}_t\\ \gcd(r_1,\dots,r_d,t)=D}} \Big|\sum_{n\in\mathbb{Z}_t^*} \mathbf{e}_t\Big(\sum_{i=1}^d r_i n^{e_i}\Big)\Big|^2.$$

Writing $r_i = s_i D$, $0 \le s_i < t/D$, $i = 1,\dots,d$ (and discarding the condition $\gcd(r_1,\dots,r_d,t) = D$), we obtain

$$\begin{aligned}(12)\qquad \sigma_D &\le (t^{1-1/d+o(1)}D^{1/d})^{2k-2} \sum_{s_1,\dots,s_d\in\mathbb{Z}_{t/D}} \Big|\sum_{n\in\mathbb{Z}_t^*} \mathbf{e}_{t/D}\Big(\sum_{i=1}^d s_i n^{e_i}\Big)\Big|^2\\ &= (t^{1-1/d+o(1)}D^{1/d})^{2k-2}(t/D)^d W,\end{aligned}$$

where W is the number of solutions to the system of congruences

$$n^{e_i} \equiv m^{e_i} \pmod{t/D}, \quad i = 1,\dots,d,$$

with $n, m \in \mathbb{Z}_t^*$. Clearly for every n there are $O(D)$ possibilities for m, thus $W \ll Dt$. Substituting this bound in (12) we derive

$$\sigma_D \ll t^{d+2k-1-(2k-2)/d+o(1)}D^{-d+(2k-2)/d+1}.$$

Returning to (11) we obtain the estimate

$$\begin{aligned}N_k^*(\mathbf{e};t) &\le t^{2k-1-(2k-2)/d+o(1)} \sum_{D|t} D^{-d+(2k-2)/d+1}\\ &\le t^{2k-1-(2k-2)/d+o(1)} \max\{1, t^{-d+(2k-2)/d+1}\} \sum_{D|t} 1.\end{aligned}$$

Using the well-known estimate

$$\sum_{D|t} 1 = t^{o(1)},$$

we derive the desired result. ∎

We note that even if all exponents $e_1,\dots,e_d$ are positive integers, the bound (10) cannot be extended to the sums over the whole ring $\mathbb{Z}_t$. For the same reason, no analogue of Lemma 5 is possible for $N_k(\mathbf{e};t)$.

3. Main results

3.1. Exponential sums twisted by monomial rational functions. Following the approach of [6, 21], we obtain the following estimate for the sum $S(a,H)$.

THEOREM 6. *Let* $\mathbf{E}$ *be an ordinary curve defined over* $\mathbb{F}_p$ *and let* $P \in \mathbf{E}$ *be of order* t. *Then for any* $d \ge 1$ *fixed pairwise distinct positive integers* $e_1,\dots,e_d$ *and for any integers* $k, l \ge 2$, *uniformly over* $a \in \mathbb{F}_p^*$ *and*

$b_1, \ldots, b_d \in \mathbb{Z}$, we have the bound

$$|S(a, H)| \le t^{1-2\alpha_{k,l}+\beta_{d,k,l}} p^{\alpha_{k,l}+o(1)},$$

where the polynomial H is given by (1) *and*

$$\alpha_{k,l} = \frac{1}{4(4k+l)} \quad \textit{and} \quad \beta_{d,k,l} = \frac{2(d-1)l+1}{4kl}.$$

Proof. Clearly, we can assume that

$$t \ge p^{1/2}(\log p)^2 \tag{13}$$

as otherwise the bound is trivial.

For any integer $k \ge 2$ we have

$$S(a, H)^k = \sum_{n_1,\ldots,n_k=1}^{t-1} \mathbf{e}_p\Big(a \sum_{j=1}^{k} x(n_j P)\Big) \mathbf{e}_t\Big(\sum_{j=1}^{k} H(n_j)\Big).$$

For each vector $(m_1, \ldots, m_d) \in \mathbb{Z}_t^d$, we collect together the terms with $n_1^{e_i} + \cdots + n_k^{e_i} \equiv m_i \pmod t$, $i = 1, \ldots, d$. Then we obtain

$$S(a, H)^k = \sum_{m_1,\ldots,m_d \in \mathbb{Z}_t} \mathbf{e}_t(b_1 m_1 + \cdots + b_d m_d) \times \sum_{\substack{n_1,\ldots,n_k=1 \\ n_1^{e_i}+\cdots+n_k^{e_i} \equiv m_i \pmod t \\ i=1,\ldots,d}}^{t-1} \mathbf{e}_p\Big(a \sum_{j=1}^{k} x(n_j P)\Big),$$

and thus

$$|S(a, H)|^k \le \sum_{m_1,\ldots,m_d \in \mathbb{Z}_t} \Big| \sum_{\substack{n_1,\ldots,n_k=1 \\ n_1^{e_i}+\cdots+n_k^{e_i} \equiv m_i \pmod t \\ i=1,\ldots,d}}^{t-1} \mathbf{e}_p\Big(a \sum_{j=1}^{k} x(n_j P)\Big) \Big|.$$

We now apply the Cauchy inequality and derive

$$|S(a, H)|^{2k} \le t^d \sum_{m_1,\ldots,m_d \in \mathbb{Z}_t} \Big| \sum_{\substack{n_1,\ldots,n_k=1 \\ n_1^{e_i}+\cdots+n_k^{e_i} \equiv m_i \pmod t \\ i=1,\ldots,d}}^{t-1} \mathbf{e}_p\Big(a \sum_{j=1}^{k} x(n_j P)\Big) \Big|^2$$

$$= t^d \sum_{(n_1,\ldots,n_{2k}) \in \mathcal{N}_k} \mathbf{e}_p\Big(a \sum_{j=1}^{2k} (-1)^j x(n_j P)\Big),$$

where the outside summation is taken over the set of vectors

$$\mathcal{N}_k = \{(n_1, \ldots, n_{2k}) \in (\mathbb{Z}_t \setminus \{0\})^{2k} \ : \ n_1^{e_i} + \cdots + n_{2k-1}^{e_i} \equiv n_2^{e_i} + \cdots + n_{2k}^{e_i} \pmod t,\ i = 1, \ldots, d\}.$$

We note that for any m with $\gcd(m,t)=1$ we have

$$\sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j x(n_jP)\Big) = \sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j x(mn_jP)\Big). \tag{14}$$

Let the integer Q be such that

$$Q \ge 2\log t \tag{15}$$

and define

$$\mathcal{Q} = \{q \le Q : q \text{ prime}, \gcd(q,t)=1\}.$$

Averaging over all $q\in\mathcal{Q}$ and changing the order of summation we obtain

$$|S(a,H)|^{2k} \le \frac{t^d}{\#\mathcal{Q}} \sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k} \Big|\sum_{q\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j x(qn_jP)\Big)\Big|.$$

We remark that $\#\mathcal{N}_k \le \varphi(t)^{2k-1} \le t^{2k-1}$, where $\varphi(t)$ is the Euler function. Moreover, recalling (9), by the prime number theorem and (15), we see that

$$\#Q \ge (1+o(1))\frac{Q}{\log Q} - (1+o(1))\frac{\log t}{\log\log t} \ge 0.4\frac{Q}{\log Q}$$

for a sufficiently large Q.

We now apply the Hölder inequality and then extend the summation over all integers $1 \le n_1,\dots,n_{2k} \le t-1$. Then we obtain

$$\begin{aligned}
|S(a,H)|^{4kl} &\le \frac{t^{2dl}}{\#\mathcal{Q}^{2l}}(\#\mathcal{N}_k)^{2l-1} \sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k} \Big|\sum_{q\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j x(qn_jP)\Big)\Big|^{2l} \\
&\le \frac{t^{2dl}}{\#\mathcal{Q}^{2l}}(\#\mathcal{N}_k)^{2l-1} \sum_{n_1,\dots,n_{2k}=1}^{t-1} \Big|\sum_{q\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j x(qn_jP)\Big)\Big|^{2l} \\
&= \frac{t^{2dl}}{\#\mathcal{Q}^{2l}}(\#\mathcal{N}_k)^{2l-1} \\
&\quad\times \sum_{n_1,\dots,n_{2k}=1}^{t-1} \sum_{q_1,\dots,q_{2l}\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}\sum_{h=1}^{2l}(-1)^{j+h} x(q_hn_jP)\Big) \\
&= \frac{t^{2dl}}{\#\mathcal{Q}^{2l}}(\#\mathcal{N}_k)^{2l-1} \sum_{q_1,\dots,q_{2l}\in\mathcal{Q}} \Big|\sum_{n=1}^{t-1} \mathbf{e}_p\Big(a\sum_{h=1}^{2l}(-1)^h x(q_hnP)\Big)\Big|^{2k}.
\end{aligned}$$

We now write the inner sum as

$$\sum_{n=1}^{t-1} \mathbf{e}_p\Big(a \sum_{h=1}^{2l} (-1)^h x(q_h(nP))\Big) = \sum_{\substack{R \in \mathcal{H} \\ R \neq \mathcal{O}}} \mathbf{e}_p\Big(a \sum_{h=1}^{2l} (-1)^h x(q_h R)\Big),$$

where $\mathcal{H} = \{nP : n = 1, \ldots, t\}$.

For $O((\#\mathcal{Q})^l) = O(Q^l (\log Q)^{-l})$ tuples $(q_1, \ldots, q_{2l}) \in \mathcal{Q}^{2l}$ such that the tuple of the elements on the odd positions $(q_1, \ldots, q_{2l-1})$ is a permutation of the tuple of the elements on the even positions $(q_2, \ldots, q_{2l})$ we estimate the inner sum trivially by t.

For the rest of $O((\#\mathcal{Q})^{2l}) = O(Q^{2l} (\log Q)^{-2l})$ tuples, we apply Lemma 1 and estimate the inner sum by $O(Q^2 p^{1/2})$.

Putting all together, we get

$$\begin{aligned} |S(a,H)|^{4kl} &\ll \frac{t^{2dl} (\log Q)^{2l}}{Q^{2l}} (\#\mathcal{N}_k)^{2l-1} (Q^l (\log Q)^{-l} t^{2k} + Q^{2l+4k} (\log Q)^{-2l} p^k) \\ &= t^{2dl} (\#\mathcal{N}_k)^{2l-1} (Q^{-l} (\log Q)^l t^{2k} + Q^{4k} p^k). \end{aligned}$$

Taking

$$Q = \lceil 2t^{2k/(4k+l)} p^{-k/(4k+l)} (\log p)^{l/(4k+l)} \rceil$$

and recalling (13) for which (15) is satisfied, we derive

$$|S(a,H)|^{4kl} \ll t^{2dl+8k^2/(4k+l)} (\#\mathcal{N}_k)^{2l-1} p^{kl/(4k+l)} (\log p)^{4kl/(4k+l)}. \tag{16}$$

Using the trivial bound (5), after simple calculations we conclude the proof. ∎

Clearly, as for any m with $\gcd(m,t) = 1$ we have a full analogue of (14) with

$$\begin{aligned} \mathcal{N}_k^* = \{&(n_1, \ldots, n_{2k}) \in (\mathbb{Z}_t^*)^{2k} : \\ &n_1^{e_i} + \cdots + n_{2k-1}^{e_i} \equiv n_2^{e_i} + \cdots + n_{2k}^{e_i} \pmod t,\ i = 1, \ldots, d\} \end{aligned} \tag{17}$$

instead of $\mathcal{N}_k$, the proof of Theorem 6 also applies to the sums $S^*(a,H)$. In particular, for $d = 1$, for example for the sums (2), and points P of order of the largest possible magnitude $t = p^{1+o(1)}$ with $k = 4$ and $l = 16$ the bound of Theorem 6 becomes

$$|S(a,H)|, |S^*(a,H)| \le t^{255/256+o(1)}.$$

However, for $d \ge 2$, using Lemma 5 instead of (5) we obtain a stronger result, but only for the sums $S^*(a,H)$.

THEOREM 7. *Let $\mathbf{E}$ be an ordinary curve defined over $\mathbb{F}_p$ and let $P \in \mathbf{E}$ be of order t. Then for any $d \ge 1$ fixed pairwise distinct positive integers $e_1, \ldots, e_d$ and for any integers $k, l \ge 2$, uniformly over $a \in \mathbb{F}_p^*$ and*

$b_1, \dots, b_d \in \mathbb{Z}$, we have the bounds

$$|S^*(a,H)| \le \begin{cases} t^{1-2\alpha_{k,l}+\gamma_{d,k,l}} p^{\alpha_{k,l}+o(1)}, & k < d(d-1)/2+1, \\ t^{1-2\alpha_{k,l}+\delta_{d,k,l}} p^{\alpha_{k,l}+o(1)}, & k \ge d(d-1)/2+1, \end{cases}$$

where the rational function H is given by (1) *and*

$$\alpha_{k,l} = \frac{1}{4(4k+l)}, \qquad \gamma_{d,k,l} = \frac{2d^2l - (2l-1)(2k-2+d)}{4kld}$$

and

$$\delta_{d,k,l} = \frac{d}{4kl}.$$

For $d \ge 2$ and "almost" square-free integers, using the bound of Lemma 4 in the estimate (16), we derive:

THEOREM 8. *Assume that $t \to \infty$ over a sequence of integers such that for the largest square divisor $v^2 \mid t$ we have $v = t^{o(1)}$. Let $\mathbf{E}$ be an ordinary curve defined over $\mathbb{F}_p$ and let $P \in \mathbf{E}$ be of order t. Then for any fixed integers $k \ge d \ge 2$ and $l \ge 2$, uniformly over $a \in \mathbb{F}_p^*$ and $b_1, \dots, b_d \in \mathbb{Z}$, we have the bounds*

$$|S(a,H)| \le t^{1-2\alpha_{k,l}+\delta_{d,k,l}} p^{\alpha_{k,l}+o(1)}$$

for any fixed pairwise distinct positive integers $e_1, \dots, e_d$, and

$$|S^*(a,H)| \le t^{1-2\alpha_{k,l}+\delta_{d,k,l}} p^{\alpha_{k,l}+o(1)}$$

for any fixed pairwise distinct nonzero integers $e_1, \dots, e_d$, where the rational function H is given by (1) *and*

$$\alpha_{k,l} = \frac{1}{4(4k+l)} \quad \text{and} \quad \delta_{d,k,l} = \frac{d}{4kl}.$$

Clearly, almost all (in the sense of asymptotic density) integers t satisfy the conditions of Theorem 8.

3.2. Exponential sums twisted by rational polynomials. Here we estimate the sums $S(a,F)$ with $F \in \mathbb{Z}[X]$ and we use the inductive argument on the degree of F. For this we define and estimate the more general exponential sums

$$S_r(\mathbf{a}, \mathbf{W}, F) = \sum_{n=1}^{t}{}^{*} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j x(nP \oplus W_j)\Big) \mathbf{e}_t(F(n)),$$

where $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{F}_p^r$, $\mathbf{W} = (W_1, \dots, W_r) \in \mathbf{E}^r$ with $W_i \ne W_j$ for $i \ne j$, and, as before, $\sum^*$ means that the poles of the function in the exponent are excluded from the summation.

We have the following estimate for the sums $S_r(\mathbf{a}, \mathbf{W}, F)$:

THEOREM 9. *Let $F \in \mathbb{Z}[X]$ be a polynomial of degree $d \ge 1$. Then for any vector $\mathbf{W} = (W_1, \ldots, W_r) \in \mathbf{E}^r$ with $W_i \ne W_j$, $1 \le i < j \le r$, and for any nonzero vector $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{F}_p^r$ we have*

$$S_r(\mathbf{a}, \mathbf{W}, F) \ll t^{1-1/2^{d-1}} p^{1/2^d}.$$

Proof. We proceed by induction on the degree d of the polynomial F. When $d = 1$, the polynomial $F(X) = bX$ with $b \in \mathbb{Z}$ is linear and thus Lemmas 2 and 3 imply that

$$S_r(\mathbf{a}, \mathbf{W}, F) \ll p^{1/2}.$$

We assume that $d \ge 2$ and that the result holds for polynomials of degree $d-1$, $d \ge 1$, and we prove it for d. We have

$$|S_r(\mathbf{a}, \mathbf{W}, F)|^2 = \sum_{m=1}^{t} \sideset{}{^*}\sum_{n=1}^{t} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j (x(nP \oplus W_j) - x(mP \oplus W_j))\Big) \times \mathbf{e}_t(F(n) - F(m)).$$

Replacing n with $n + m$, we obtain

$$\begin{aligned}
&|S_r(\mathbf{a}, \mathbf{W}, F)|^2 \\
&= \sum_{n=1}^{t} \sideset{}{^*}\sum_{m=1}^{t} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j (x(nP \oplus mP \oplus W_j) - x(mP \oplus W_j))\Big) \mathbf{e}_t(F(n+m) - F(m)) \\
&= \sum_{n=1}^{t} \sideset{}{^*}\sum_{m=1}^{t} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j (x(nP \oplus mP \oplus W_j) - x(mP \oplus W_j))\Big) \mathbf{e}_t(G_n(m)),
\end{aligned}$$

where $G_n(X) = F(X + n) - F(X) \in \mathbb{Z}[X]$, $n = 1, \ldots, t$.

We note that G_n, $n = 1, \ldots, t$, is a polynomial of degree $d-1$, and thus, in the case when the points

$$nP \oplus W_1, \ldots, nP \oplus W_r, W_1, \ldots, W_r \tag{18}$$

are pairwise distinct, the induction hypothesis applies and gives the bound $O(t^{2-1/2^{d-2}} p^{1/2^{d-1}})$ on the inner sum over m.

Clearly, since $W_i \ne W_j$, $1 \le i < j \le r$, the points (18) are pairwise distinct for all but at most r^2 values of $n = 1, \ldots, t$ for which $nP = W_i - W_j$. In this case we use the trivial bound t for the sum over m. Putting everything together, we get

$$|S_r(\mathbf{a}, \mathbf{W}, F)|^2 \ll t^{2-1/2^{d-2}} p^{1/2^{d-1}} + t \ll t^{2-1/2^{d-2}} p^{1/2^{d-1}},$$

from which the desired result follows. ∎

We remark that although for polynomials of high degree the bounds of Theorems 6 and 7 are stronger, for polynomials of small degree Theorem 9 is sharper.

3.3. Exponential sums twisted by real polynomials. As before, to estimate the sums $T(a, f; N)$ with $f \in \mathbb{R}[X]$ we use the inductive argument on the degree of f. For this we define and estimate the more general exponential sum

$$T_r(\mathbf{a}, \mathbf{W}, f, N) = \sum_{n=1}^{N}{}^{*} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j x(nP \oplus W_j)\Big)\mathbf{e}(f(n)),$$

that can be of independent interest, where $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{F}_p^r$, $\mathbf{W} = (W_1, \dots, W_r) \in \mathbf{E}^r$ with $W_i \neq W_j$ for $i \neq j$, and, as before, $\sum^*$ means that the poles of the function in the exponent are excluded from the summation.

We have the following estimate for the sums $T_r(\mathbf{a}, \mathbf{W}, f, N)$:

THEOREM 10. *Let $f \in \mathbb{R}[X]$ be a polynomial of degree $d \geq 1$. Then for any vector $\mathbf{W} = (W_1, \dots, W_r) \in \mathbf{E}^r$ with $W_i \neq W_j$, $1 \leq i < j \leq r$, for any nonzero vector $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{F}_p^r$ and for any positive integer $N < t$, we have*

$$T_r(\mathbf{a}, \mathbf{W}, f, N) \ll N^{1-1/2^d} p^{1/2^{d+1}}.$$

Proof. As in the proof of Theorem 9, we use induction on the degree d of the polynomial f.

When $d = 1$, we use the bound (4) as the basis of our induction.

We assume that $d \geq 2$ and that the result holds for polynomials of degree $d-1$, $d \geq 1$, and we prove it for d. For any integer $k \geq 0$, we see that

$$T_r(\mathbf{a}, \mathbf{W}, f, N) = \sum_{n=1}^{N}{}^{*} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j x((n+k)P \oplus W_j)\Big)\mathbf{e}(f(n+k)) + O(k).$$

Therefore, for any integer $K \geq 1$, we have

$$T_r(\mathbf{a}, \mathbf{W}, f, N) = \frac{1}{K} W + O(K),$$

where

$$W = \sum_{k=0}^{K-1} \sum_{n=1}^{N}{}^{*} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j x((n+k)P \oplus W_j)\Big)\mathbf{e}(f(n+k)).$$

Changing the order of summation and using the Cauchy inequality, we derive

$$|W|^2 \leq N \sum_{k,m=0}^{K-1} \sum_{n=1}^{N}{}^{*} \mathbf{e}_p\Big(\sum_{j=1}^{r} a_j (x((n+k)P \oplus W_j) - x((n+m)P \oplus W_j))\Big) \times \mathbf{e}(f(n+k) - f(n+m)).$$

In the case when the points

$$kP \oplus W_1, \dots, kP \oplus W_r, mP \oplus W_1, \dots, mP \oplus W_r \tag{19}$$

are pairwise distinct for any i, j, we apply the induction hypothesis and get the bound $O(K^2N^{2-1/2^{d-1}}p^{1/2^d})$ on the inner sum over n.

Clearly, since $W_i \neq W_j$, $1 \le i \le j < r$, the points (19) are pairwise distinct for all but at most Kr^2 pairs (k, m) with $k, m = 0, \ldots, K-1$ for which $kP = mP \oplus W_i \ominus W_j$. In this case we use the trivial bound N for the sum over n. Putting everything together, we have

$$T_r(\mathbf{a}, \mathbf{W}, f, N) \ll N^{1-1/2^d}p^{1/2^{d+1}} + K^{-1/2}N + K. \tag{20}$$

Taking $K = \lceil N^{2/3} \rceil$ and noting that then the first term in (20) always dominates, we get the desired result. ∎

4. Comments. The method of this paper applies to several other sums of similar flavour such as

$$V(a, H) = \sum_{n \in \mathbb{Z}_t} \mathbf{e}_p(ag^n)\mathbf{e}_t(H(n)),$$

$$V^*(a, H) = \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ag^n)\mathbf{e}_t(H(n))$$

with $g \in \mathbb{F}_p^*$ of multiplicative order t and a polynomial or rational function H of the type (1). It also applies to the sums

$$U(a, f, N) = \sum_{n \in \mathbb{Z}_t} \mathbf{e}_p(ag^n)\mathbf{e}(f(n))$$

with a real polynomial $f(X) \in \mathbb{R}[X]$, just generalizing some estimates of [6, 21, 22]. In particular, using the Weil bound (see [13, bound (12.23)]), instead of Lemma 1, for the sums $V(a, H)$ and $V^*(a, H)$, one can obtain full analogies of Theorems 6, 7 and 8 with

$$\widetilde{\alpha}_{k,l} = \frac{1}{4(2k+l)}$$

instead of $\alpha_{k,l}$ and the same values of $\beta_{d,k,l}$, $\gamma_{d,k,l}$ and $\delta_{d,k,l}$. The sums $U(a, f, N)$ can also be estimated using the inductive argument of the proofs of Theorems 9 and 10.

Our approach also applies to the sums

$$\sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ax(nP))\chi(n) \quad \text{and} \quad \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ax(nP))\mathbf{e}_m(bg^n),$$

where χ is a multiplicative character modulo t and g is an element of order t modulo some integer $m \ge 1$. It should also be possible to replace the $x(Q)$ with more general functions from the function field of $\mathbf{E}$. However, extensions to arbitrary finite fields may take more effort; in particular, one needs an appropriate analogue of Lemma 3 for the trace of $\mathcal{L}_{\mathbf{a},\mathbf{W}}(Q)$ (see [12, Section 4] for a discussion of this issue).

Furthermore, estimating the sums $S(a, H)$ with an arbitrary rational function $H(X) \in \mathbb{Z}(X)$ and also sums of the form

$$\sum_{\substack{n \in \mathbb{Z}_t \\ F(n) \not\equiv 0 \pmod t}} \mathbf{e}_p(ax(F(n)P)) \quad \text{and} \quad \sum_{n \in \mathbb{Z}_t^*} \mathbf{e}_p(ax(n^{-1}P))\mathbf{e}_m(bg^n),$$

where $F(X) \in \mathbb{Z}[X]$ and g is an element of order t modulo an integer $m \geq 1$, is certainly of interest but seems to require some new ideas.

Acknowledgements. During the preparation of this paper, A. O. was supported in part by the Swiss National Science Foundation Grant 121874 and I. S. by the Australian Research Council Grant DP0881473.

References

[1] R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005.

[2] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, *Double character sums over elliptic curves and finite fields*, Pure and Appl. Math. Quart. 2 (2006), 179–197.

[3] I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Math. Soc. Lecture Note Ser. 265, Cambridge Univ. Press, 1999.

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

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

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

[7] Z. Chen, *Elliptic curve analogue of Legendre sequences*, Monatsh. Math. 154 (2008), 1–10.

[8] T. Cochrane and C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. 133 (2005), 313–320.

[9] T. Cochrane, C. Pinner and J. Rosenhouse, *Sparse polynomial exponential sums*, Acta Arith. 108 (2003), 37–52.

[10] E. El-Mahassni and I. E. Shparlinski, *On the distribution of the elliptic curve power generator*, in: Finite Fields and Applications, Contemp. Math. 461, Amer. Math. Soc., 2008, 111–118.

[11] R. R. Farashahi and I. E. Shparlinski, *Pseudorandom bits from points on elliptic curves*, preprint, 2009.

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

[13] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., 2004.

[14] D. R. Kohel and I. E. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields*, in: Lecture Notes in Comput. Sci. 1838, Springer, 2000, 395–404.

[15] T. Lange and I. E. Shparlinski, *Certain exponential sums and random walks on elliptic curves*, Canad. J. Math. 57 (2005), 338–350.

[16] T. Lange and I. E. Shparlinski, *Distribution of some sequences of points on elliptic curves*, J. Math. Cryptol. 1 (2007), 1–11.
[17] I. E. Shparlinski, *On exponential sums with sparse polynomials and rational functions*, J. Number Theory 60 (1996), 233–244.
[18] —, *Bilinear character sums over elliptic curves*, Finite Fields Appl. 14 (2008), 132–141.
[19] —, *Pseudorandom number generators from elliptic curves*, in: Recent Trends in Cryptography, Contemp. Math. 477, Amer. Math. Soc., 2009, 121–141.
[20] —, *Some special character sums over elliptic curves*, Bol. Soc. Mat. Mexicana 15 (2009), 37–40.
[21] —, *Exponential sums with consecutive modular roots of an integer*, Quart. J. Math. 62 (2011), 207–213.
[22] —, *On some exponential sums with exponential and rational functions*, Rocky Mountain J. Math., to appear.
[23] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1992.
[24] T. D. Wooley, *A note on simultaneous congruences, II: Mordell revised*, J. Austral. Math. Soc. 88 (2010), 261–275.

Alina Ostafe
Institut für Mathematik
Universität Zürich
Winterthurerstrasse 190
CH-8057, Zürich, Switzerland
E-mail: alina.ostafe@math.uzh.ch

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

Received on 20.5.2010
and in revised form on 2.1.2011 (6386)