Exponential sums over points of elliptic curves with reciprocals of primes

Ostafe, Alina ; Shparlinski, Igor E

Abstract: We consider exponential sums with x-coordinates of points qG and q−1G where G is a point of order T on an elliptic curve modulo a prime p and q runs through all primes up toN (with gcd (q,T)=1 in the case of the points q−1G). We obtain a new bound on exponential sums with q−1G and correct an imprecision in the work of W.D. Banks, J.B. Friedlander, M.Z. Garaev and I.E.Shparlinski on exponential sums with qG. We also note that similar sums with g1/q for an integer g with gcd (g,p)=1 have been estimated by J.Bourgain and I.E.Shparlinski

DOI: https://doi.org/10.1112/s0025579311001719

Originally published at:
Ostafe, Alina; Shparlinski, Igor E (2012). Exponential sums over points of elliptic curves with reciprocals of primes. Mathematika, 58(1):21-33.
DOI: https://doi.org/10.1112/s0025579311001719

Mathematika 58 (2012) 21–33 © University College London
doi:10.1112/S0025579311001719

EXPONENTIAL SUMS OVER POINTS OF ELLIPTIC CURVES WITH RECIPROCALS OF PRIMES

ALINA OSTAFE AND IGOR E. SHPARLINSKI

Abstract. We consider exponential sums with x-coordinates of points qG and $q^{-1}G$ where G is a point of order T on an elliptic curve modulo a prime p and q runs through all primes up to N (with $\gcd(q, T) = 1$ in the case of the points $q^{-1}G$). We obtain a new bound on exponential sums with $q^{-1}G$ and correct an imprecision in the work of W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski on exponential sums with qG. We also note that similar sums with $g^{1/q}$ for an integer g with $\gcd(g, p) = 1$ have been estimated by J. Bourgain and I. E. Shparlinski.

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

$$\mathcal{E} : Y^2 = X^3 + AX + B$$

with some $A, B \in \mathbb{F}_p$, see [1, 3, 21].

We recall that the set of all points on $\mathcal{E}$ 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 $\mathcal{E}$ as $P = (\mathbf{x}(P), \mathbf{y}(P))$.

Let $\mathcal{E}(\mathbb{F}_p)$ denote the set of $\mathbb{F}_p$-rational points on $\mathcal{E}$. 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 $\mathcal{E}$ taken over all points of $\mathcal{E}(\mathbb{F}_p)$. More recently, various character sums over points of elliptic curves have been considered in a number of papers, see [2, 7, 9, 10, 14–16, 18, 20] and references therein; many of these estimates are motivated by applications to pseudorandom number generators on elliptic curves [19].

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 $\mathcal{E}(\mathbb{F}_p)$.

We also denote

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

and consider the sums

$$S_a(N) = \sum_{\substack{q \leq N \\ q \text{ prime} \\ \gcd(q,T)=1}} \mathbf{e}_p(a\mathbf{x}(q^{-1}G)), \quad a \in \mathbb{F}_p, \tag{1}$$

Received 12 August 2010, published online 13 July 2011.
MSC (2000): 11L07, 11T23 (primary), 11G20 (secondary).

where the parameter q varies over prime numbers. We estimate these sums (uniformly over $a \not\equiv 0 \pmod p$), provided that N and T are sufficiently large compared to p. Since our results are based on those of [17], they apply only to ordinary curves, see [1, 3, 21] for a definition of ordinary elliptic curves.

We note that the sums $S_a(N)$ are elliptic curve analogues of the exponential sums with reciprocals of primes $1/q$ that have been considered in [5, 11, 12] and with $g^{1/q}$ for $g \in \mathbb{F}_p$ that have been considered in [6].

In particular, in the most interesting case of $T = p^{1+o(1)}$ (that is, when G generates a large subgroup of $\mathcal{E}(\mathbb{F}_p)$) we obtain the bound

$$|S_a(N)| \le (Np^{-1/256} + N^{5/6}p^{5/12})N^{o(1)} \tag{2}$$

which is non-trivial if $p^C \ge N \ge p^{5/2+\varepsilon}$ for some fixed C and $\varepsilon > 0$. Furthermore, for $N \ge p^{323/128}$ the bound (2) simplifies as

$$|S_a(N)| \le N^{1+o(1)}p^{-1/256}. \tag{3}$$

One can use our bounds in a standard fashion to obtain an asymptotic formula for the number of solutions to the congruence

$$\mathbf{x}(q_1^{-1}G) + \cdots + \mathbf{x}(q_k^{-1}G) \equiv c \pmod p \tag{4}$$

in primes $q_1, \ldots, q_k \le N$, which is an analogue of the congruence

$$q_1^{-1} + \cdots + q_k^{-1} \equiv c \pmod p$$

studied in [11]. We do not derive all possible results of this kind but simply give one example which relies on the bound (3).

We remark that the sums

$$T_a(N) = \sum_{\substack{q \le N \\ q \text{ prime}}} \mathbf{e}_p(a\mathbf{x}(qG)), \qquad a \in \mathbb{F}_p, \tag{5}$$

have been considered in [2]. However, the proof of [2, Theorem 6] unfortunately contains an imprecision. Here we present an estimate on $T_a(N)$ which can be obtained by the same method as our bound on $S_a(N)$.

§2. *Preparations.*

2.1. *Notation.* We use $\mathbb{Z}_M^*$ to denote the unit group of the residue ring $\mathbb{Z}_M$ modulo a positive integer M.

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

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

with log being the natural logarithm.

Throughout the paper, the implied constants in symbols "O" and "$\ll$" may occasionally depend on the integer parameters r and 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 $c > 0$).

2.2. *Vaughan identity.* We decompose Λ by means of the Vaughan identity, given for example in [8, Ch. 24], which we use in the following form.

LEMMA 1. *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

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

$$\Sigma_2 = (\log UV) \sum_{k \le UV} \left| \sum_{\ell \le N/k} f(k\ell) \right|,$$

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

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

2.3. *Single sums.* We also need the following result which is proved in [17, Theorem 6].

LEMMA 2. *Let $\mathcal{E}$ be an ordinary curve defined over $\mathbb{F}_p$ and let $G \in \mathcal{E}$ of order T. Then for any $d \ge 1$ fixed pairwise distinct integers $e_1, \ldots, e_d$ and positive integers $r, s \ge 2$, uniformly over $a \in \mathbb{F}_p^*$ and $b_1, \ldots, b_d \in \mathbb{Z}$, we have the bound*

$$\sum_{n \in \mathbb{Z}_T^*} \mathbf{e}_p(ax(nP)) \mathbf{e}_T(H(n)) \ll T^{1 - 2\eta_{r,s} + \kappa_{d,r,s}} p^{\eta_{r,s} + o(1)},$$

where the rational function H is given by

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

and

$$\eta_{r,s} = \frac{1}{4(4r+s)} \quad \text{and} \quad \kappa_{d,r,s} = \frac{2(d-1)s + 1}{4rs}.$$

Taking $d = 1$ and $e_1 = -1$ in Lemma 2 and using the standard reduction between complete and incomplete sums, see [13, §12.2], we obtain the following estimate.

COROLLARY 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 any integers $r, s \ge 2$, real numbers $H_1 < H_2$ and integer a not divisible by p, the following estimate holds:*

$$\sum_{\substack{H_1 < n \le H_2 \\ \gcd(n,T)=1}} \mathbf{e}_p(a\mathbf{x}(n^{-1}G)) \ll \left(\frac{H_2 - H_1}{T} + 1 \right) T^{1 - 1/2(4r+s) + 1/4rs} p^{1/4(4r+s) + o(1)}.$$

2.4. *Double sums.* We need an estimate of certain double exponential sums that follows directly from [2, Theorem 3].

LEMMA 4. *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 $\mathcal{K}, \mathcal{L} \subset \mathbb{Z}_T^*$, sequences α_k and β_ℓ of arbitrary complex numbers, supported on the sets $\mathcal{K}$ and $\mathcal{L}$, respectively, and all $a \in \mathbb{F}_p^*$, the following bound holds:*

$$\sum_{k\in\mathcal{K}}\sum_{\ell\in\mathcal{L}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) \ll ABT^{5/6}(\#\mathcal{K}\#\mathcal{L})^{1/2}p^{1/12+o(1)},$$

where

$$A = \max_{k\in\mathcal{K}} |\alpha_k| \quad \textit{and} \quad B = \max_{\ell\in\mathcal{L}} |\beta_\ell|.$$

Proof. We define the subsets of $\mathbb{Z}_T^*$

$$\mathcal{K}^* = \{k^{-1} : k \in \mathcal{K}\}, \qquad \mathcal{L}^* = \{\ell^{-1} : \ell \in \mathcal{L}\}.$$

Using these notations, we obtain

$$\sum_{k\in\mathcal{K}}\sum_{\ell\in\mathcal{L}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) = \sum_{k\in\mathcal{K}^*}\sum_{\ell\in\mathcal{L}^*} \alpha_{k^{-1}}\beta_{\ell^{-1}} \mathbf{e}_p(a\mathbf{x}(k\ell G)).$$

Now applying [2, Theorem 3], we obtain the desired result. □

We now immediately derive the following corollary.

COROLLARY 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 arbitrary positive integers K, L, sequences α_k and β_ℓ of arbitrary complex numbers, supported on the intervals $[1, K]$ and $[1, L]$, respectively, and all $a \in \mathbb{F}_p^*$, the following bound holds:*

$$\sum_{\substack{k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$\ll ABT^{5/6}(KT^{-1/2}+K^{1/2})(LT^{-1/2}+L^{1/2})p^{1/12+o(1)},$$

where

$$A = \max_{1\le k\le K} |\alpha_k| \quad \textit{and} \quad B = \max_{1\le \ell\le L} |\beta_\ell|.$$

Proof. We split the sum into at most $(K/T+1)(L/T+1)$ double sums with at most $\min\{K, T\}\min\{L, T\}$ terms obtaining from Lemma 4 that

$$\sum_{\substack{k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$\ll ABT^{5/6}\left(\frac{K}{T}+1\right)\left(\frac{L}{T}+1\right)(\min\{K, T\}\min\{L, T\})^{1/2}p^{1/12+o(1)}.$$

Since for any $R > 0$

$$\max\{R, T\}(\min\{R, T\})^{1/2} = R^{1/2}T^{1/2}(\max\{R, T\})^{1/2}$$

we derive

$$\left(\frac{R}{T}+1\right)\max\{R^{1/2}, T^{1/2}\} \ll T^{-1}\max\{R, T\}\max\{R^{1/2}, T^{1/2}\}$$
$$= R^{1/2}T^{-1/2}\max\{R^{1/2}, T^{1/2}\}$$
$$\le R^{1/2}T^{-1/2}(R^{1/2}+T^{1/2}).$$

The result now follows. □

We now use the idea of [12] which allows us to vary the limit of summation for ℓ.

LEMMA 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 arbitrary positive integers K, L, a sequence of positive integers L_k with $L_k \le L$, $1 \le k \le K$, sequences α_k and β_ℓ of arbitrary complex numbers, supported on the intervals $[1, K]$ and $[1, L]$, and all $a \in \mathbb{F}_p^*$, the following bound holds:*

$$\sum_{\substack{k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L_k\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$\ll ABT^{5/6}(KT^{-1/2}+K^{1/2})(LT^{-1/2}+L^{1/2})p^{1/12+o(1)}\log L,$$

where

$$A=\max_{1\le k\le K}|\alpha_k| \quad \text{and} \quad B=\max_{1\le \ell\le L}|\beta_\ell|.$$

Proof. We have

$$\sum_{\ell\le L_k}\alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$=\sum_{\substack{\ell\le L\\ \gcd(\ell,T)=1}}\alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))\frac{1}{L}\sum_{-(L-1)/2\le s\le L/2}\ \sum_{w\le L_k}\mathbf{e}_L(s(\ell-w))$$
$$=\frac{1}{L}\sum_{-(L-1)/2\le s\le L/2}\ \sum_{w\le L_k}\mathbf{e}_L(-sw)$$
$$\times\sum_{\substack{\ell\le L\\ \gcd(\ell,T)=1}}\alpha_k\beta_\ell \mathbf{e}_L(s\ell)\mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)).$$

Since for $|s|\le L/2$ we have

$$\sum_{w\le L_k}\mathbf{e}_L(sw)=\eta_{k,s}\frac{L}{|s|+1},$$

for some complex numbers $\eta_{k,s}\ll 1$, see [13, Bound (8.6)], we conclude that for $|s|\le L/2$ and $k\le K$ there are some complex numbers $\gamma_{k,s}=\eta_{k,s}\alpha_k$

such that

$$\sum_{\substack{k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L_k\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$= \sum_{-(L-1)/2\le s\le L/2} \frac{1}{|s|+1}$$
$$\times \sum_{\substack{k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L\\ \gcd(\ell,T)=1}} \gamma_{k,s}\beta_\ell \mathbf{e}_L(s\ell)\mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)).$$

Using Corollary 5, we derive the desired result. □

Finally, we are ready to derive our main technical tool of this section.

LEMMA 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 arbitrary positive integers H, K, L, sequences α_k and β_ℓ of arbitrary complex numbers, supported on the intervals* $[1, K]$ *and* $[1, L]$, *and all $a\in\mathbb{F}_p^*$, the following bound holds:*

$$\sum_{\substack{H\le k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L/k\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$\ll ABT^{5/6}\left(\frac{L}{T}+\frac{K^{1/2}L^{1/2}}{T^{1/2}}+\frac{L}{H^{1/2}T^{1/2}}+L^{1/2}\right)p^{1/12+o(1)}(KL)^{o(1)},$$

where

$$A=\max_{1\le k\le K}|\alpha_k| \quad \text{and} \quad B=\max_{1\le \ell\le L}|\beta_\ell|.$$

Proof. Defining some values of α_k as zeros we write

$$\sum_{\substack{H\le k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L/k\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$=\sum_{j=I}^{J}\ \sum_{\substack{e^j\le k\le e^{j+1}\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L/k\\ \gcd(\ell,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)),$$

where $I=\lfloor\log H\rfloor$ and $J=\lfloor\log K\rfloor$. So, by Lemma 6, we get

$$\sum_{\substack{H\le k\le K\\ \gcd(k,T)=1}}\ \sum_{\substack{\ell\le L/k\\ \gcd(k,T)=1}} \alpha_k\beta_\ell \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G))$$
$$\ll ABT^{5/6}p^{1/12+o(1)}\log L\sum_{j=I}^{J}(LT^{-1}+L^{1/2}e^{j/2}T^{-1/2}$$
$$+Le^{-j/2}T^{-1/2}+L^{1/2})$$
$$\le ABT^{5/6}p^{1/12+o(1)}\log L(JLT^{-1}+e^{J/2}L^{1/2}T^{-1/2}$$
$$+Le^{-I/2}T^{-1/2}+JL^{1/2}).$$

Since $H\ll e^I\le e^J\ll K$, we immediately obtain the desired result. □

§3. *Main results.*

3.1. *Sums over primes.* In this subsection, we combine Lemma 1 with the bounds of Corollary 3 and Lemma 4 to estimate the sums $S_a(N)$ defined by (1).

THEOREM 8. *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 $a \in \mathbb{F}_p^*$ and integers r, $s \geq 2$, we have*

$$\left| \sum_{\substack{n \leq N \\ \gcd(n,T)=1}} \Lambda(n) \mathbf{e}_p(a\mathbf{x}(n^{-1}G)) \right| \leq (N\Delta + N^{5/6}T^{1/3}p^{1/12})N^{o(1)},$$

where

$$\Delta = T^{-1/2(4r+s)+1/4rs} p^{1/4(4r+s)}.$$

Proof. We remark that the result is trivial if $T \leq p^{1/2}$ or $N \leq T^{7/3}$. Hence we can always assume that

$$T > p^{1/2} \quad \text{and} \quad N \geq T^{7/3} \geq p. \tag{6}$$

Let U, $V > 1$ with $UV \leq N$ and apply Lemma 1 with the function $f(n) = \mathbf{e}_p(a\mathbf{x}(n^{-1}G))$. By the prime number theorem, we have

$$\Sigma_1 = \left| \sum_{\substack{n \leq U \\ \gcd(n,T)=1}} \Lambda(n) f(n) \right| \leq \sum_{n \leq U} \Lambda(n) \ll U. \tag{7}$$

We now write

$$\Sigma_2 = \Sigma_{2,1} + \Sigma_{2,2}$$

where

$$\Sigma_{2,1} = (\log UV) \sum_{\substack{k \leq N/T \\ \gcd(k,T)=1}} \left| \sum_{\substack{\ell \leq N/k \\ \gcd(\ell,T)=1}} \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) \right|$$

$$\Sigma_{2,2} = (\log UV) \sum_{\substack{N/T \leq k \leq UV \\ \gcd(k,T)=1}} \left| \sum_{\substack{\ell \leq N/k \\ \gcd(\ell,T)=1}} \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) \right|.$$

Next, for any $k \geq 1$ with $\gcd(k, T) = 1$ the point kG has also order T in $\mathcal{E}(\mathbb{F}_p)$; thus Corollary 3 provides the bound

$$\begin{aligned} \Sigma_{2,1} &= (\log UV) \sum_{\substack{k \leq N/T \\ \gcd(k,T)=1}} \left| \sum_{\substack{\ell \leq N/k \\ \gcd(\ell,T)=1}} \mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) \right| \\ &\leq N^{o(1)} \sum_{k \leq N/T} \left(\frac{N}{kT} + 1 \right) T\Delta \\ &\leq N^{1+o(1)} \Delta \sum_{k \leq N/T} \frac{1}{k} \\ &= N^{1+o(1)} \Delta. \end{aligned}$$

To estimate $\Sigma_{2,2}$ we use Lemma 7:

$$\Sigma_{2,2} \le T^{5/6}(NT^{-1} + N^{1/2}U^{1/2}V^{1/2}T^{-1/2} + N^{1/2})p^{1/12}N^{o(1)}.$$

Since under the conditions (6)

$$\Delta \ge T^{-1/2(4r+s)}p^{1/4(4r+s)} \ge T^{-1/6}p^{1/12} \quad \text{and} \quad NT^{-1} \ge N^{1/2}$$

for $T \ge p^{1/2}$ and r, $s \ge 2$, we derive

$$\Sigma_2 \le N^{1+o(1)}\Delta + N^{1/2+o(1)}U^{1/2}V^{1/2}T^{1/3}p^{1/12}. \tag{8}$$

Similar to the estimate of $\Sigma_{2,1}$, we also have

$$\Sigma_3 \le N^{o(1)} \sum_{k \le V} \left(\frac{N}{kT} + 1\right) T\Delta.$$

Thus

$$\Sigma_3 \le (N + VT)\Delta N^{o(1)}. \tag{9}$$

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

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

Since k, $\ell \le N$, we have

$$A(k) \le \tau(k) \ll N^{o(1)} \quad \text{and} \quad \Lambda(\ell) \le \log \ell \le N^{o(1)},$$

where $\tau(k)$ is the number of integer positive divisors of k.

Then,

$$\begin{aligned}\Sigma_4 &= \left| \sum_{\substack{k\ell \le N, \gcd(k\ell, T)=1 \\ k>V, \ell>U}} A(k)\Lambda(\ell)\mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) \right| \\ &= \left| \sum_{\substack{V \le k \le N/U \\ \gcd(k,T)=1}} \sum_{\substack{U \le \ell \le N/k \\ \gcd(\ell,T)=1}} A(k)\Lambda(\ell)\mathbf{e}_p(a\mathbf{x}(k^{-1}\ell^{-1}G)) \right|.\end{aligned}$$

Applying Lemma 7 we derive

$$\begin{aligned}\Sigma_4 &\le T^{5/6}(NT^{-1} + NT^{-1/2}U^{-1/2} + NT^{-1/2}V^{-1/2} + N^{1/2})p^{1/12}N^{o(1)} \\ &\le T^{5/6}(NT^{-1} + NT^{-1/2}U^{-1/2} + NT^{-1/2}V^{-1/2})p^{1/12}N^{o(1)}\end{aligned} \tag{10}$$

since, as we have noticed, $NT^{-1} \ge N^{1/2}$ under the conditions (6).

Combining (7), (8), (9) and (10), and recalling that $\Delta \ge T^{-1/6}p^{1/12}$, we find that

$$\left| \sum_{n \le N} \Lambda(n)\mathbf{e}_p(a\mathbf{x}(nG)) \right| \le U + (N + VT)\Delta N^{o(1)} + (\Psi_1 + \Psi_2 + \Psi_3)N^{o(1)},$$

where

$$\Psi_1 = N^{1/2}T^{1/3}U^{1/2}V^{1/2}p^{1/12},$$
$$\Psi_2 = NT^{1/3}U^{-1/2}p^{1/12},$$
$$\Psi_3 = NT^{1/3}V^{-1/2}p^{1/12}.$$

Choosing $U = V = N^{1/3}$, we obtain

$$\left|\sum_{n\le N} \Lambda(n)\mathbf{e}_p(a\mathbf{x}(nG))\right| \le (N + N^{1/3}T)\Delta + N^{5/6+o(1)}T^{1/2}p^{1/12}.$$

Since under the conditions (6) we have

$$N \ge N^{1/3}T \quad \text{and} \quad N^{5/6}T^{-1/2} \ge N^{1/2},$$

the desired result follows. □

Using partial summation we immediately derive the following corollary from Theorem 8.

COROLLARY 9. *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 $a \in \mathbb{F}_p^*$ and integers $r, s \ge 2$, we have*

$$|S_a(N)| \le (N\Delta + N^{5/6}T^{1/3}p^{1/12})N^{o(1)},$$

where

$$\Delta = T^{-1/2(4r+s)+1/4rs}p^{1/4(4r+s)}.$$

We see that if $T = p^{1+o(1)}$ then taking $r = 4$ and $s = 16$ in Corollary 9 we derive the bound (2).

Furthermore, if $N \ge T^2p^{1/2+\varepsilon}$ and $T \ge p^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$ then taking sufficiently large $r = s$ we obtain

$$|S_a(N)| \le N^{1+o(1)}p^{-\delta}$$

where $\delta > 0$ depends only on ε.

3.2. *Congruences with primes.* Here we study the congruence (4). As we have mentioned, we only consider the case in which the bound (3) applies.

Let $\pi(N)$ be the number of primes $q \le N$ as usual.

THEOREM 10. *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 $T = p^{1+o(1)}$. Then, for $N \ge p^{323/128}$ and any fixed integer $k \ge 3$ the congruence (4) has*

$$R_k(N, c) = \frac{1}{p}\pi(N)^k + O(N^{k+o(1)}p^{-1-(k-2)/256})$$

solutions.

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

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

Therefore, for any integer h, the number of solutions to the congruence (4) can be written as

$$\begin{aligned} R_k(N, c) &= \frac{1}{p}\sum_{\substack{q_1,\ldots,q_k\le N\\ q_i \text{ prime}\\ \gcd(q_i,T)=1}}\sum_{\lambda\in\mathbb{F}_p}\mathbf{e}_p\left(\lambda\left(\sum_{j=1}^{k} x(q_j^{-1}G) - c\right)\right)\\ &= \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p}\mathbf{e}_p(-\lambda c)\prod_{j=1}^{k}\sum_{\substack{q_j\le N\\ q_j \text{ prime}\\ \gcd(q_j,T)=1}}\mathbf{e}_p(\lambda x(q_j^{-1}G))\\ &= \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p}\mathbf{e}_p(-\lambda c)S_\lambda(N)^k. \end{aligned}$$

Separating the term $\pi(N)^k/p$ corresponding to $\lambda = 0$ we obtain

$$\left|R_k(N, c) - \frac{1}{p}\pi(N)^k\right| \le \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}|S_\lambda(N)|^k. \tag{11}$$

Since under the conditions of the theorem the bound (3) holds, we derive

$$\begin{aligned} \sum_{\lambda\in\mathbb{F}_p^*}|S_\lambda(N)|^k &\le (N^{1+o(1)}p^{-1/256})^{k-2}\sum_{\lambda\in\mathbb{F}_p^*}|S_\lambda(N)|^2\\ &\le (N^{1+o(1)}p^{-1/256})^{k-2}\sum_{\lambda\in\mathbb{F}_p}|S_\lambda(N)|^2 = (N^{1+o(1)}p^{-1/256})^{k-2}pW, \end{aligned}$$

where W is the number of solutions to the congruence

$$x(q_1^{-1}G) \equiv x(q_2^{-1}G) \pmod p.$$

For every prime $q_1 \le N$ we have at most $2(N/T + 1) = Np^{-1+o(1)}$ possibilities for q_2, thus $W \ll N^2p^{-1+o(1)}$, from where we obtain

$$\sum_{\lambda\in\mathbb{F}_p^*}|S_\lambda(N)|^k \le N^{k+o(1)}p^{-(k-2)/256} \tag{12}$$

and after the substitution in (11) the desired result follows. □

One can easily see that under the conditions of Theorem 10 we have the asymptotic formula $R_k(N, c) = (1 + o(1))\pi(N)^k/p$ for any $k \ge 3$. We now consider the moments

$$M_{k,\nu}(N) = \sum_{c\in\mathbb{F}_p}\left|R_k(N, c) - \frac{1}{p}\pi(N)^k\right|^{2\nu},$$

for which we obtain a non-trivial estimate starting with $k = 2$.

THEOREM 11. *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 $T = p^{1+o(1)}$. Then, for $N \ge p^{323/128}$ and any fixed integers $k \ge 2$, $\nu \ge 1$ we have*

$$M_{k,\nu}(N) \le N^{2k\nu+o(1)} p^{-2\nu+1-(k\nu-2\nu+1)/128}.$$

Proof. As in the proof of Theorem 10, we have

$$R_k(N, c) - \frac{1}{p}\pi(N)^k = \frac{1}{p} \sum_{\lambda \in \mathbb{F}_p^*} \mathbf{e}_p(-\lambda c) S_\lambda(N)^k.$$

Therefore,

$$M_{k,\nu}(N) = \frac{1}{p^{2\nu}} \sum_{c \in \mathbb{F}_p} \sum_{\lambda_1,\ldots,\lambda_{2\nu} \in \mathbb{F}_p^*} \mathbf{e}_p(-(\lambda_1 + \cdots + \lambda_{2\nu})c) \times S_{\lambda_1}(N)^k \cdots S_{\lambda_{2\nu}}(N)^k.$$

Thus we obtain

$$M_{k,\nu}(N) = \frac{1}{p^{2\nu-1}} \sum_{\substack{\lambda_1,\ldots,\lambda_{2\nu} \in \mathbb{F}_p^* \\ \lambda_1+\cdots+\lambda_{2\nu}=0}} S_{\lambda_1}(N)^k \cdots S_{\lambda_{2\nu-1}}(N)^k S_{\lambda_{2\nu}}(N)^k.$$

Since under the conditions of the theorem the bound (3) holds for every sum $S_{\lambda_j}(N)$ above, which we apply to $S_{\lambda_{2\nu}}(N)$, we derive

$$\begin{aligned} M_{k,\nu}(N) &\le \frac{1}{p^{2\nu-1}} (N^{1+o(1)} p^{-1/256})^k \sum_{\substack{\lambda_1,\ldots,\lambda_{2\nu-1} \in \mathbb{F}_p^* \\ \lambda_1+\cdots+\lambda_{2\nu-1}\neq 0}} |S_{\lambda_1}(N)|^k \cdots |S_{\lambda_{2\nu-1}}(N)|^k \\ &\le \frac{1}{p^{2\nu-1}} (N^{1+o(1)} p^{-1/256})^k \sum_{\lambda_1,\ldots,\lambda_{2\nu-1} \in \mathbb{F}_p^*} |S_{\lambda_1}(N)|^k \cdots |S_{\lambda_{2\nu-1}}(N)|^k \\ &= \frac{1}{p^{2\nu-1}} (N^{1+o(1)} p^{-1/256})^k \left(\sum_{\lambda \in \mathbb{F}_p^*} |S_\lambda(N)|^k \right)^{2\nu-1}. \end{aligned}$$

Using (12) we conclude the proof. □

Theorem 11 (taken with $k = 2$ and, say, $\nu = 1$) immediately implies that under the same conditions we have $R_2(N, c) > 0$ for all but at most $p^{127/128+o(1)}$ elements $c \in \mathbb{F}_p$.

§4. *Comments.* As we have noticed, the proof of [**2**, Theorem 6] contains a gap as the double sums which appear in the proof are sometimes over sets which are not subsets of $\mathbb{Z}_T$ and thus [**2**, Theorem 6] does not apply. However using the estimate

$$\left| \sum_{H_1 < n \le H_2} \mathbf{e}_p(a\mathbf{x}(nG)) \right| \le \left(\frac{H_2 - H_1}{T} + 1 \right) p^{1/2+o(1)}, \qquad (13)$$

see [2, Lemma 5], instead of Corollary 3, and also a full analogue of Lemma 7 with $k\ell$ instead of $k^{-1}\ell^{-1}$, one can easily derive the following analogue of the estimate of Corollary 9 for the sums $T_a(N)$ given by (5): for every $a \in \mathbb{F}_p^*$ we have

$$|T_a(N)| \le N^{1+o(1)}T^{-1}p^{1/2} + N^{5/6+o(1)}T^{1/3}p^{1/12}.$$

Acknowledgements. The authors are very grateful to Moubariz Garaev for his comments. 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 DP1092835.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice*, CRC Press (Boca Raton, FL, 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 Appl. Math. Q.* **2** (2006), 179–197.
3. I. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography* (*London Mathematical Society Lecture Note Series* **265**), Cambridge University Press (Cambridge, MA, 1999).
4. E. Bombieri, On exponential sums in finite fields. *Amer. J. Math.* **88** (1966), 71–105.
5. J. Bourgain, More on the sum–product phenomenon in prime fields and its applications. *Int. J. Number Theory* **1** (2005), 1–32.
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. H. Davenport, *Multiplicative Number Theory*, 2nd edn., Springer (New York, 1980).
9. E. El Mahassni and I. E. Shparlinski, On the distribution of the elliptic curve power generator. In *Proceedings of the 8th International Conference on Finite Fields and Applications* (*Contemporary Mathematics* **461**), American Mathematical Society (Providence, RI, 2008), 111–119.
10. R. R. Farashahi and I. E. Shparlinski, Pseudorandom bits from points on elliptic curves. *Preprint*, 2009.
11. E. Fouvry and P. Michel, Sur certaines sommes d'exponentielles sur les nombres premiers. *Ann. Sci. Éc. Norm. Supér.* (4) **31** (1998), 93–130.
12. M. Z. Garaev, An estimate of Kloosterman sums with prime numbers and an application. *Mat. Zametki* **88**(3) (2010), 365–373 (in Russian).
13. H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society (Providence, RI, 2004).
14. D. R. Kohel and I. E. Shparlinski, Exponential sums and group generators for elliptic curves over finite fields. In *Proceedings of the 4th Algorithmic Number Theory Symposium* (*Lecture Notes in Computer Science* **1838**), Springer (Berlin, 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. A. Ostafe and I. E. Shparlinski, Twisted exponential sums over points of elliptic curves. *Acta Arith.* **148** (2011), 77–92.
18. I. E. Shparlinski, Bilinear character sums over elliptic curves. *Finite Fields Appl.* **14** (2008), 132–141.
19. I. E. Shparlinski, Pseudorandom number generators from elliptic curves. In *Recent Trends in Cryptography* (*Contemporary Mathematics* **477**), American Mathematical Society (Providence, RI, 2009), 121–141.
20. I. E. Shparlinski, Some special character sums over elliptic curves. *Bol. Soc. Mat. Mexicana* (3) **15** (2009), 37–40.
21. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (Berlin, 1995).

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