Bilinear Exponential Sums and Sum-Product Problems on Elliptic Curves

OMRAN AHMADI  
Department of Combinatorics & Optimization  
University of Waterloo  
Waterloo, Ontario, N2L 3G1, Canada  
oahmadid@math.uwaterloo.ca

IGOR SHPARLINSKI  
Department of Computing  
Macquarie University  
Sydney, NSW 2109, Australia  
ingor@comp.mq.edu.au

Abstract

Let $E$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$ of $q$ elements. We improve a bound on bilinear additive character sums over points on $E$, and obtain its analogue for bilinear multiplicative character sums. We apply these bounds to some variants of the sum-product problem on $E$.

2000 Mathematics Subject Classification: Primary 11G05, 11L07, 11T23

Keywords: Sum-product problem, elliptic curves, character sums
1 Introduction

We fix an ordinary elliptic curve $E$ over a finite field $\mathbb{F}_q$ of $q$ elements.

We assume that $E$ is given by an affine Weierstraß equation

$$E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6,$$

with some $a_1, \ldots, a_6 \in \mathbb{F}_q$, see [20].

We recall that the set of all points on $E$ forms an Abelian group, with the point at infinity $\mathcal{O}$ as the neutral element. As usual, we write every point $Q \neq \mathcal{O}$ on $E$ as $Q = (x(Q), y(Q))$.

Let $E(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on $E$ and let $P \in E(\mathbb{F}_q)$ be a fixed point of order $T$.

Let $\mathbb{Z}_T$ denote the residue ring modulo $T$ and let $\mathbb{Z}_T^*$ be its unit group.

We use the ideas of M. Z. Garaev and A. A. Karatsuba [8] to improve the bound of [1] on bilinear sums of additive characters with $x(kmP)$ as argument where $k$ and $m$ run through arbitrary sets $K, M \subseteq \mathbb{Z}_T^*$. We also use a result of Z. Chen [4], which in turn is based on a result of M. Perret [16], to estimate similar bilinear sums of multiplicative characters.

We combine this bound with an argument of M. Z. Garaev [7] to study two versions of the sum-product problem on $E$. We show that for any sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_T^*$, at least one of the sets

$$S = \{ x(aP) + x(bP) : a \in \mathcal{A}, \ b \in \mathcal{B} \},$$

$$T = \{ x(abP) : a \in \mathcal{A}, \ b \in \mathcal{B} \},$$

is large. Furthermore, in some ranges of $\# \mathcal{A}, \# \mathcal{B}$ and $T$ we obtain a matching lower bound.

Finally, we also show that at least one of the sets

$$X = \{ x(aP)x(bP) : a \in \mathcal{A}, \ b \in \mathcal{B} \},$$

$$Y = \{ x(abP) : a \in \mathcal{A}, \ b \in \mathcal{B} \},$$

is large.

These questions are motivated by a series of recent results on the sum-product problem over $\mathbb{F}_q$ which assert that for any sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$, at least one of the sets

$$\mathcal{G} = \{ a + b : a \in \mathcal{A}, \ b \in \mathcal{B} \} \quad \text{and} \quad \mathcal{H} = \{ ab : a \in \mathcal{A}, \ b \in \mathcal{B} \}$$
is large, see [2, 3, 6, 7, 10, 11, 12, 13, 19] for the background, various modification of the original problem and further references.

We remark that yet another variant of the sum-product problem for elliptic curves has recently been considered in [18] (which in turn is based on the estimate of some other bilinear character sums given in [17]). It is shown in [18] that for sets \( P, Q \subseteq E(\mathbb{F}_q) \) at least one of the sets

\[
\{ x(P) + x(Q) : P \in P, Q \in Q \} \quad \text{and} \quad \{ x(P \oplus Q) : P \in P, Q \in Q \} \quad (3)
\]

is large, where \( \oplus \) denotes the group operation on the points of \( E \).

Throughout the paper, the implied constants in the symbols ‘\( O \)’ and ‘\( \ll \)’ may depend on an integer parameter \( \nu \geq 1 \). We recall that \( X \ll Y \) and \( X = O(Y) \) are both equivalent to the inequality \( |X| \leq cY \) with some constant \( c > 0 \).

2 Bilinear Sums over Elliptic Curves

Let \( \psi \) and \( \varphi \) be a nontrivial additive character and a nontrivial multiplicative characters of \( \mathbb{F}_q \), respectively.

We consider the bilinear sums

\[
T_{\rho, \vartheta}(\psi, K, M) = \sum_{k \in K} \left| \sum_{m \in M} \rho(k) \vartheta(m) \psi(x(kmP)) \right|,
\]

\[
W_{\rho, \vartheta}(\varphi, K, M) = \sum_{k \in K} \left| \sum_{m \in M} \rho(k) \vartheta(m) \varphi(x(kmP)) \right|,
\]

where \( K, M \subseteq \mathbb{Z}^*_T \), \( \rho(k) \) and \( \vartheta(m) \) are arbitrary complex functions supported on \( K \) and \( M \) with

\[
|\rho(k)| \leq 1, \quad k \in K, \quad \text{and} \quad |\vartheta(m)| \leq 1, \quad m \in M.
\]

The sums \( T_{\rho, \vartheta}(\psi, K, M) \) have been introduced and estimated in [1]. Here we obtain a stronger result by using the approach to sums of this type given in [8].

**Theorem 1.** Let \( E \) be an ordinary elliptic curve defined over \( \mathbb{F}_q \), and let \( P \in E(\mathbb{F}_q) \) be a point of order \( T \). Then, for any fixed integer \( \nu \geq 1 \), for all
subsets $K, M \subseteq \mathbb{Z}_T^*$ and complex functions $\rho(k)$ and $\vartheta(m)$ supported on $K$ and $M$ with

$$|\rho(k)| \leq 1, \ k \in K, \quad \text{and} \quad |\vartheta(m)| \leq 1, \ m \in M,$$

uniformly over all nontrivial additive characters $\psi$ of $\mathbb{F}_q$.

$$T_{\rho, \vartheta}(\psi, K, M) \ll \left(\#K\right)^{1 - \frac{1}{2\nu}} \left(\#M\right)^{\frac{\nu + 1}{2\nu + 2}} T^{\frac{\nu + 1}{2\nu + 3}} q^{\frac{1}{2\nu + 2}} (\log q)^{\frac{1}{2\nu + 2}}.$$

Proof. We follow the scheme of the proof of [8, Lemma 4] in the special case of $d = 1$ (and also $\mathbb{Z}_T$ plays the role of $\mathbb{Z}_{p-1}$). Furthermore, in our proof $K, M, \mathbb{Z}_T^*$ play the roles of $\mathcal{X}, \mathcal{L}_d$ and $\mathcal{U}_d$ in the proof of [8, Lemma 4], respectively. In particular, for some integer parameter $L$ with

$$1 \leq L \leq T^{(\log q)^{-2}} \quad (4)$$

we define $\mathcal{V}$ as the set of the first $L$ prime numbers which do not divide $\#E(\mathbb{F}_q)$ (clearly we can assume that, say $T \geq (\log q)^3$, since otherwise the bound is trivial). We also note that in this case

$$\max_{v \in \mathcal{V}} v = O(\#\mathcal{V} \log q). \quad (5)$$

Then we arrive to the following analogue of [8, Bound (4)]:

$$T_{\rho, \vartheta}(\psi, K, M) \leq \left(\#K\right)^{1 - 1/(2\nu)} \left(\#\mathcal{V}\right) \sum_{t \in \mathbb{Z}_T^*} M_t^{1/(2\nu)}$$

where

$$M_t = \sum_{z \in \mathbb{Z}_T^*} \left| \sum_{v \in \mathcal{V}} \vartheta(vt) \chi_M(vt) \psi(x(zvP)) \right|^{2\nu}$$

and $\chi_M$ is the characteristic function of the set $M$. We only deviate from that proof at the point where the Weil bound is applied to the sums

$$\sum_{z \in \mathcal{H}} \exp \left( \frac{2\pi ia}{p} \left( \sum_{j=1}^{\nu} z^{t_{1j}} - \sum_{j=\nu+1}^{2\nu} z^{t_{1j}} \right) \right) \ll \max_{1 \leq j \leq 2\nu} v_j q^{1/2}$$
where $\mathcal{H}$ is an arbitrary subgroup of $\mathbb{F}_q^*$ and $v_1, \ldots, v_{2\nu}$ are positive integers (such that $(v_{\nu+1}, \ldots, v_{2\nu})$ is not a permutation of $(v_1, \ldots, v_{\nu})$). Here, as in [1] we use instead the following bound from [15]:

$$\sum_{Q \in \mathcal{H}} \psi\left(\sum_{j=1}^{\nu} x(v_j Q) - \sum_{j=\nu+1}^{2\nu} x(v_j Q)\right) \ll \max_{1 \leq j \leq 2\nu} v_j^2 q^{1/2}, \quad (6)$$

where $\mathcal{H}$ is a subgroup of $\mathbf{E}(\mathbb{F}_q^*)$ (in our particular case $\mathcal{H} = \langle P \rangle$ is generated by $P$) and $v_1, \ldots, v_{2\nu}$ are the same as in the above, that is, such that $(v_{\nu+1}, \ldots, v_{2\nu})$ is not a permutation of $(v_1, \ldots, v_{\nu})$.

Now since $\#\mathbf{E}(\mathbb{F}_q) = O(q)$, using an argument similar to the one given in [8] and recalling (5) we obtain

$$M_t \ll \sum_{v_1 \in V} \cdots \sum_{v_{2\nu} \in V} \left(\prod_{j=1}^{\nu} \chi_M(v_j t)\right) T^{\nu} + \sum_{v_1 \in V} \cdots \sum_{v_{2\nu} \in V} \left(\prod_{j=1}^{2\nu} \chi_M(v_j t)\right) q^{1/2}(\#V \log q)^2.$$

Therefore

$$M_t \ll \left(\sum_{v \in V} \chi_M(v t)\right)^{\nu} T + \left(\sum_{v \in V} \chi_M(v t)\right)^{2\nu} q^{1/2}(\#V \log q)^2.$$

This leads to the following

$$T_{\rho,\vartheta}(\psi, \mathcal{K}, \mathcal{M}) \ll \frac{(\#\mathcal{K})^{1-\frac{1}{2\nu}}}{\#V} T^{\nu} \sum_{t \in \mathbb{Z}_T^*} \left(\sum_{v \in V} \chi_M(v t)\right)^{1/2} + \frac{(\#\mathcal{K})^{1-\frac{1}{2\nu}}}{\#V} (\#V \log q)^{1/\nu} q^{1/4\nu} \sum_{t \in \mathbb{Z}_T^*} \left(\sum_{v \in V} \chi_M(v t)\right).$$

On the other hand we have

$$\sum_{t \in \mathbb{Z}_T^*} \left(\sum_{v \in V} \chi_M(v t)\right) = \#\mathcal{M} \#V,$$
and by the Cauchy inequality we get
\[
\sum_{t \in \mathbb{Z}_T} \left( \sum_{v \in V} \chi_M(vt) \right)^{1/2} \leq \left( \# \mathbb{Z}_T \right)^{1/2} \left( \sum_{t \in \mathbb{Z}_T} \sum_{v \in V} \chi_M(vt) \right)^{1/2}
\]
\[
\leq T^{1/2} (\#M \#V)^{1/2}.
\]
Thus
\[
T_\rho,\vartheta(\psi, \mathcal{K}, \mathcal{M}) \ll \frac{(\#\mathcal{K})^{1-\frac{1}{2\nu}}}{(\#V)^{1/2}} T^{1/2\nu+1/2} (\#\mathcal{M})^{1/2}
\]
\[
+ (\#\mathcal{K})^{1-\frac{1}{2\nu}} (\#V \log q)^{1/\nu} q^{1/4\nu} \#\mathcal{M}.
\]

Let
\[
L = \left\lfloor \frac{T^{\nu+1}}{q^{\frac{1}{\nu+2}}} (\log q)^{\frac{1}{\nu+2}} (\#\mathcal{M})^{\frac{1}{\nu+2}} \right\rfloor.
\]
We note that if \( L = 0 \) then
\[
T^{\nu+1} \leq q^{\frac{1}{\nu+2}} (\log q)^{\frac{2}{\nu+2}} (\#\mathcal{M})^{\frac{2}{\nu+2}} \leq q^{\frac{1}{\nu+2}} (\log q)^{\frac{2}{\nu+2}} T^{\nu+2}
\]
and thus
\[
T \leq q^{1/2} (\log q)^{2}.
\]
It is easy to check that in this case
\[
\frac{(\#\mathcal{K})^{1-\frac{1}{2\nu}} (\#\mathcal{M})^{\frac{\nu+1}{\nu+2}} T^{\frac{\nu+1}{\nu+2}} q^{\frac{1}{\nu+2}} (\log q)^{\frac{1}{\nu+2}}}{\#\mathcal{K} \#\mathcal{M}}
\]
\[
\geq (\#\mathcal{K})^{-\frac{1}{\nu}} (\#\mathcal{M})^{-\frac{\nu+1}{\nu+2}} T^{\frac{\nu+1}{\nu+2}} q^{\frac{1}{\nu+2}} (\log q)^{\frac{1}{\nu+2}}
\]
\[
\geq T^{-\frac{1}{\nu}} T^{-\frac{1}{\nu+2}} T^{\frac{\nu+1}{\nu+2}} T q^{\frac{1}{\nu+2}} (\log q)^{\frac{1}{\nu+2}}
\]
\[
= T^{-\frac{1}{\nu+2}} q^{\frac{1}{\nu+2}} (\log q)^{\frac{1}{\nu+2}} \geq 1,
\]
and thus the result is trivial.

We now assume that \( L \geq 1 \) and choose \( V \) to be of cardinality \( \#V = L \).

Then we have
\[
T^{\frac{\nu+1}{\nu+2}} q^{\frac{1}{\nu+2}} (\log q)^{\frac{2}{\nu+2}} (\#\mathcal{M})^{\frac{2}{\nu+2}} \geq \#V \geq T^{\frac{\nu+1}{\nu+2}} q^{\frac{1}{\nu+2}} (\log q)^{\frac{2}{\nu+2}} (\#\mathcal{M})^{\frac{2}{\nu+2}},
\]
and \( L \leq T (\log q)^{-2} \) provided that \( q \) is large enough. Now the result follows from (7).
We also have the same result for sums of multiplicative characters

**Theorem 2.** Let $E$ be an ordinary elliptic curve defined over $\mathbb{F}_q$, and let $P \in E(\mathbb{F}_q)$ be a point of order $T$. Then, for any fixed integer $\nu \geq 1$, for all subsets $\mathcal{K}, \mathcal{M} \subseteq \mathbb{Z}/T$ and complex functions $\rho(k)$ and $\vartheta(m)$ supported on $\mathcal{K}$ and $\mathcal{M}$ with

$$|\rho(k)| \leq 1, \ k \in \mathcal{K}, \ \text{and} \ \ |\vartheta(m)| \leq 1, \ m \in \mathcal{M},$$

uniformly over all nontrivial additive characters $\psi$ of $\mathbb{F}_q$

$$W_{\rho, \vartheta}(\varphi, \mathcal{K}, \mathcal{M}) \ll \left(\#\mathcal{K}\right)^{1-\frac{1}{2\nu+1}} \left(\#\mathcal{M}\right)^{\frac{\nu+1}{2\nu+1}} T^\frac{\nu+1}{2\nu+2} q^\frac{1}{\nu+1} (\log q)^{\frac{1}{\nu+2}}.$$

**Proof.** The proof is fully analogous to that of Theorem 1 and so we only briefly indicate a few changes.

First of all we notice that the proof of [15, Lemma 3] which implies that the sum

$$\sum_{j=1}^\nu x(v_j Q) - \sum_{j=\nu+1}^{2\nu} x(v_j Q), \quad v_1, \ldots, v_{2\nu},$$

are non-constant rational functions of components $x(Q)$ and $y(Q)$ of $Q$ of degree $O\left(\max_{1 \leq j \leq 2\nu} v_j^2\right)$ (unless $(v_{\nu+1}, \ldots, v_{2\nu})$ is a permutation of $(v_1, \ldots, v_\nu)$) extends to the products

$$\prod_{j=1}^\nu x(v_j Q) \prod_{j=\nu+1}^{2\nu} x(v_j Q)^{-1}, \quad v_1, \ldots, v_{2\nu}$$

at the cost of only typographical changes. Furthermore, using the bound of Z. Chen [4, Proposition 1] instead of the bound of [14] used in [15] we obtain the following analogue of (6):

$$\sum_{Q \in \mathcal{H}} \varphi \left(\prod_{j=1}^\nu x(v_j Q)\right) \overline{\varphi} \left(\prod_{j=\nu+1}^{2\nu} x(v_j Q)\right) \ll \max_{1 \leq j \leq 2\nu} v_j^2 q^{1/2},$$

where $\overline{\varphi}$ is the complex conjugate character (we also recall that $\varphi(z^{-1}) = \overline{\varphi}(z)$ for any $z \in \mathbb{F}_q^*$). The rest of the proof follows through without any changes.

$\square$
3 Lower Bounds for Sum-Product Problems on Elliptic Curves

Theorem 3. Let $\mathcal{A}$ and $\mathcal{B}$ be arbitrary subsets of $\mathbb{Z}_T^*$. Then for the sets $\mathcal{S}$ and $\mathcal{T}$, given by (1), we have

$$\# \mathcal{S} \# \mathcal{T} \gg \min\{q \# \mathcal{A}, (\# \mathcal{A})^2(\# \mathcal{B})^{5/3}q^{-1/6}T^{-4/3}(\log q)^{-2/3}\}.$$

Proof. Let

$$\mathcal{H} = \{ab : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

Following the idea of M. Z. Garaev [7], we now denote by $J$ the number of solutions $(b_1, b_2, h, u)$ to the equation

$$x(hb_1^{-1}P) + x(b_2P) = u, \quad b_1, b_2 \in \mathcal{B}, \ h \in \mathcal{H}, \ u \in \mathcal{S}. \quad (8)$$

Since obviously the vectors

$$(b_1, b_2, h, u) = (b_1, b_2, ab_1, x(aP) + x(b_2P)), \quad a \in \mathcal{A}, \ b_1, b_2 \in \mathcal{B},$$

are all pairwise distinct solutions to (8), we obtain

$$J \geq \# \mathcal{A}(\# \mathcal{B})^2. \quad (9)$$

To obtain an upper bound on $J$ we use $\Psi$ to denote the set of all $q$ additive characters of $\mathbb{F}_q$ and write $\Psi^*$ for the set of nontrivial characters. Using the identity

$$\frac{1}{q} \sum_{\psi \in \Psi} \psi(z) = \begin{cases} 1, & \text{if } z = 0, \\ 0, & \text{otherwise}, \end{cases} \quad (10)$$

we obtain

$$J = \sum_{b_1 \in \mathcal{B}} \sum_{b_2 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \frac{1}{q} \sum_{u \in \mathcal{S}} \psi \left( x(hb_1^{-1}P) + x(b_2P) - u \right)$$

$$= \frac{1}{q} \sum_{\psi \in \Psi} \sum_{b_1 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi \left( x(hb_1^{-1}P) \right) \sum_{b_2 \in \mathcal{B}} \psi \left( x(b_2P) \right) \sum_{u \in \mathcal{S}} \psi \left( -u \right)$$

$$= \frac{(\# \mathcal{B})^2 \# \mathcal{S} \# \mathcal{H}}{q}$$

$$+ \frac{1}{q} \sum_{\psi \in \Psi^*} \sum_{b_1 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi \left( x(hb_1^{-1}P) \right) \sum_{b_2 \in \mathcal{B}} \psi \left( x(b_2P) \right) \sum_{u \in \mathcal{S}} \psi \left( -u \right).$$
Applying Theorem 1 with \( \rho(k) = \vartheta(m) = 1 \), \( K = \mathcal{H} \) and \( \mathcal{M} = \{ b^{-1} : b \in \mathcal{B} \} \) and also taking \( \nu = 1 \), we obtain

\[
\left| \sum_{b_1 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi \left( x(bh_1^{-1}P) \right) \right| \ll \Delta
\]

where

\[
\Delta = \left( \# \mathcal{H} \right)^{1/2} \left( \# \mathcal{B} \right)^{2/3} T^{2/3} q^{1/12} (\log q)^{1/3}.
\]

Therefore,

\[
J \ll \left( \frac{\# \mathcal{B}^2 \# \mathcal{S} \# \mathcal{H}}{q} + \frac{1}{q} \Delta \sum_{\psi \in \Psi^*} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right| \sum_{u \in \mathcal{S}} \psi(-u) \right).
\]  \hspace{1cm} (11)

Extending the summation over \( \psi \) to the full set \( \Psi \) and using the Cauchy inequality, we obtain

\[
\left| \sum_{\psi \in \Psi^*} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right| \sum_{u \in \mathcal{S}} \psi(u) \right| \leq \sqrt{\sum_{\psi \in \Psi} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right|^2} \sqrt{\sum_{\psi \in \Psi} \left| \sum_{u \in \mathcal{S}} \psi(u) \right|^2}.
\]  \hspace{1cm} (12)

Recalling the orthogonality property (10), we derive

\[
\sum_{\psi \in \Psi} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right|^2 = q \# \{(b_1, b_2) \in \mathcal{B}^2 : b_1 \equiv \pm b_2 \pmod{T} \} \ll q \# \mathcal{B}.
\]

Notice that \( b_1 \equiv -b_2 \pmod{T} \) has been included since \( x(P) = x(-P) \) for \( P \in \mathbf{E}(\mathbb{F}_q) \).

Similarly,

\[
\sum_{\psi \in \Psi} \left| \sum_{u \in \mathcal{S}} \psi(u) \right|^2 \leq q \# \mathcal{S}.
\]

Substituting these bounds in (12) we obtain

\[
\sum_{\psi \in \Psi^*} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right| \sum_{u \in \mathcal{S}} \psi(u) \ll q \sqrt{\# \mathcal{B} \# \mathcal{S}},
\]
which after inserting in (11), yields

\[ J \ll \frac{(\#B)^2 \#S \#H}{q} + \Delta(\#S)^{1/2}(\#B)^{1/2}. \]  
(13)

Thus, comparing (9) and (13), we derive

\[ \frac{(\#B)^2 \#S \#H}{q} + \Delta(\#S)^{1/2}(\#B)^{1/2} \gg \#A(\#B)^2. \]

Thus either

\[ \frac{(\#B)^2 \#S \#H}{q} \gg \#A(\#B)^2, \]  
(14)

or

\[ \Delta(\#S)^{1/2}(\#B)^{1/2} \gg \#A(\#B)^2. \]  
(15)

If (14) holds, then we have

\[ \#S \#H \gg q \#A. \]

If (15) holds, then recalling the definition of \( \Delta \), we derive

\[ (\#S)^{1/2}(\#H)^{1/2}(\#B)^{5/3}T^{2/3}q^{1/12}(\log q)^{1/3} \gg \#A(\#B)^2. \]

It only remains to notice that \( \#T \geq 0.5 \#H \) to conclude the proof. \( \square \)

We now consider several special cases.

**Corollary 4.** For any fixed \( \varepsilon > 0 \) there exists \( \delta > 0 \) such that if \( A, B \subseteq \mathbb{Z}_T^* \) are arbitrary subsets with

\[ q^{1-\varepsilon} \geq \#A \geq \#B \geq T^{4/5+\varepsilon}q^{1/10}, \]

then for the sets \( S \) and \( T \), given by (1), we have

\[ \#S \#T \gg (\#A)^{2+\delta}. \]

In particular, if \( T \geq q^{1/2+\varepsilon} \) then there is always some nontrivial range of cardinalities \( \#A \) and \( \#B \) in which Corollary 4 applies.
Corollary 5. If $A, B \subseteq \mathbb{Z}_T^*$ are arbitrary subsets with 
$$\#A = \#B \geq T^{1/2}q^{7/16}(\log q)^{1/4}$$
then for the sets $S$ and $T$, given by (1), we have
$$\#S\#T \gg q\#A.$$ 

We now obtain the multiplicative analogue of the above results for the sets $X$ and $Y$, given by (2).

Theorem 6. Let $A$ and $B$ be arbitrary subsets of $\mathbb{Z}_T^*$. Then for the sets $X$ and $Y$, given by (2), we have
$$\#X\#Y \gg \min\{q\#A, (\#A)^2(\#B)^{5/3}q^{-1/6}T^{-4/3}(\log q)^{-2/3}\}.$$ 

Proof. Let 
$$G = \{ab : a \in A, b \in B\}.$$ 

We remove, if necessary at most two elements $a \in A$, $b \in B$ for which $x(aP) = x(bP) = 0$, and denote by $I$ the number of solutions $(b_1, b_2, g, w)$ to the equation
$$x(gb_1^{-1}P)x(b_2P) = w, \quad b_1, b_2 \in B, \quad g \in G, \quad w \in X.$$ 

As before we notice that
$$I \geq \#A(\#B)^2.$$ 

To obtain an upper bound on $I$ we use $\Phi$ to denote the set of all $q$ multiplicative characters of $\mathbb{F}_q$ and write $\Phi^*$ for the set of nontrivial characters. Using the multiplicative analogue of (10)
$$\frac{1}{q-1} \sum_{\varphi \in \Phi} \varphi(z) = \begin{cases} 1, & \text{if } z = 1, \\ 0, & \text{otherwise}, \end{cases}$$
we obtain

\[
I = \sum_{b_1 \in B} \sum_{b_2 \in B} \sum_{g \in G} \sum_{w \in X} \frac{1}{q-1} \sum_{\varphi \in \Phi} \varphi(x(g b_1^{-1} P) x(b_2 P) w^{-1})
\]

\[
= \frac{1}{q-1} \sum_{\varphi \in \Phi} \sum_{b_1 \in B} \sum_{b_2 \in B} \sum_{g \in G} \varphi(x(g b_1^{-1} P)) \sum_{b_2 \in B} \varphi(x(b_2 P)) \sum_{w \in X} \varphi(w)
\]

\[
= \frac{(#B)^2 \#S \#H}{q-1} + \frac{1}{q-1} \sum_{\varphi \in \Phi} \sum_{b_1 \in B} \sum_{b_2 \in B} \sum_{g \in G} \varphi(x(g b_1^{-1} P)) \sum_{b_2 \in B} \varphi(x(b_2 P)) \sum_{w \in X} \varphi(w)
\]

Applying Theorem 2 instead of Theorem 1, and proceeding as in the proof of Theorem 3, we derive the desired result.

Accordingly, we also obtain:

**Corollary 7.** For any fixed \(\varepsilon > 0\) there exists \(\delta > 0\) such that if \(A, B \subseteq \mathbb{Z}_T^*\) are arbitrary subsets with

\[
q^{1-\varepsilon} \geq \#A \geq \#B \geq T^{4/5+\varepsilon} q^{1/10},
\]

then for the sets \(X\) and \(Y\), given by (2), we have

\[
\#X \#Y \gg \#A^{2+\delta}.
\]

**Corollary 8.** If \(A, B \subseteq \mathbb{Z}_T^*\) are arbitrary subsets with

\[
\#A = \#B \geq T^{1/2} q^{7/16} (\log q)^{1/4}
\]

then for the sets \(X\) and \(Y\), given by (2), we have

\[
\#X \#Y \gg q \#A.
\]

4 Upper Bound for a Sum-Product Problem on Elliptic Curves

We now show that in some cases the sets \(S\) and \(T\) are not very big.

As usual, we use \(\varphi(T) = \#\mathbb{Z}_T^*\) to denote the Euler function.
Theorem 9. Let $q = p$ be prime and let $T \geq p^{3/4+\varepsilon}$. Then there are sets $\mathcal{A} = \mathcal{B} \subset \mathbb{Z}_T^*$ of cardinality

$$\# \mathcal{A} = \# \mathcal{B} = (1 + o(1)) \left( \frac{\omega(T)^2}{2p} \right)$$

such that for the sets $\mathcal{S}$ and $\mathcal{T}$, given by (1), we have

$$\max \{ \# \mathcal{S}, \# \mathcal{T} \} \leq (\sqrt{2} + o(1)) \sqrt{p \# \mathcal{A}}$$

as $p \to \infty$.

Proof. We recall the bound from [14] of exponential sums over subgroups of the group of points on elliptic curves which in particular implies that for any subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_p)$ the bound

$$\sum_{G \in \mathcal{G}} \exp \left( \frac{2\pi i \lambda x(G)}{p} \right) \ll p^{1/2}, \quad (16)$$

holds uniformly over all integer $\lambda$ with $\gcd(\lambda, p) = 1$.

Let $\mu(d)$ be the Möbius function, that is, $\mu(1) = 1$, $\mu(m) = 0$ if $m \geq 2$ is not square-free and $\mu(m) = (-1)^{\omega(m)}$ otherwise, where $\omega(d)$ is the number of distinct prime divisors of $d \geq 2$, see [9, Section 16.2].

Using the inclusion-exclusion principle, we obtain

$$\sum_{\substack{a=1 \\ \gcd(a,T)=1}}^{T} \exp \left( \frac{2\pi i \lambda x(aP)}{p} \right) = \sum_{d \mid T} \mu(d) \sum_{\substack{a=1 \\ d \mid a}}^{T} \exp \left( \frac{2\pi i \lambda x(aP)}{p} \right)$$

$$= \sum_{d \mid T} \mu(d) \sum_{b=1}^{T/d} \exp \left( \frac{2\pi i \lambda x(bP)}{p} \right).$$

Using (16) and recalling that

$$\sum_{d \mid T} 1 = T^{o(1)}$$

see [9, Theorem 317], we derive

$$\sum_{\substack{a=1 \\ \gcd(a,T)=1}}^{T} \exp \left( \frac{2\pi i \lambda x(aP)}{p} \right) \ll p^{1/2 + o(1)}.$$
Combining this with the Erdős-Turán inequality, see [5, Theorem 1.21], we see that for any positive integer $H$, there are $H\varphi(T)/p+O\left(p^{1/2+o(1)}\right)$ elements $a \in \mathbb{Z}_T$ with $x(aP) \in [0, H - 1]$. Let $\mathcal{A} = \mathcal{B}$ be the set of these elements $a$. For the sets $\mathcal{S}$ and $\mathcal{T}$, we obviously have

$$\#\mathcal{S} \leq 2H \quad \text{and} \quad \#\mathcal{T} \leq \varphi(T).$$

We now choose $H = \varphi(T)/2$. Since $T \geq p^{3/4+\varepsilon}$ and also since

$$\varphi(T) \gg \frac{T}{\log \log T},$$

see [9, Theorem 328], we have

$$\#\mathcal{A} = \#\mathcal{B} = \frac{\varphi(T)^2}{2p} + O\left(p^{1/2+o(1)}\right) = (1+o(1))\frac{\varphi(T)^2}{2p},$$

as $p \to \infty$. Therefore

$$\max\{\#\mathcal{S}, \#\mathcal{T}\} \leq (\sqrt{2} + o(1))\sqrt{p\#\mathcal{A}}$$

which concludes the proof.

We remark that if $T \geq p^{23/24+\varepsilon}$, then the cardinality of the sets $\mathcal{A}$ and $\mathcal{B}$ of Theorem 9 is

$$\#\mathcal{A} = \#\mathcal{B} = T^{2+o(1)}p^{-1} \geq T^{1/2}p^{7/16}(\log p)^{1/4}$$

and thus Corollary 5 applies as well and we have

$$(\sqrt{2} + o(1))\sqrt{p\#\mathcal{A}} \geq \max\{\#\mathcal{S}, \#\mathcal{T}\} \geq \sqrt{\#\mathcal{S}\#\mathcal{T}} \gg \sqrt{p\#\mathcal{A}}$$

showing that both Corollary 5 and Theorem 9 are tight in this range.

5 Comments

We remark that using Theorems 1 and 2 with other values of $\nu$ in the scheme of the proof of Theorems 3 and 6, respectively, one can obtain a series of other statements. However they cannot be formulated as a lower bound on the products $\#\mathcal{S}\#\mathcal{T}$ and $\#\mathcal{X}\#\mathcal{Y}$. Rather they only give a lower bound
on \( \max\{\#S, \#T\} \) and \( \max\{\#X, \#Y\} \) which however may in some cases be more precise than those which follow from Theorems 3 and 6, respectively.

We remark that we do not have any upper bound for the sets \( X \) and \( Y \), given by (2). Some analogue of Theorem 9 can be obtained for such sets too, but only when \( \mathbb{F}_q \) contains a subgroup of a desired size.

Certainly extending the range in which the upper and lower bounds on \( \#S \) and \( \#T \) coincide is also a very important question.

Finally, we note that using the bound of M. Perret [16] (see also [4]) on multiplicative character sums along an elliptic curve, one can obtain an analogue of the estimate of [17] for the bilinear multiplicative character sum with \( x(P \oplus Q) \) over \( P \in \mathcal{P}, Q \in \mathcal{Q} \) for two arbitrary sets \( \mathcal{P}, \mathcal{Q} \subseteq \mathbb{E}(\mathbb{F}_q) \). In turn this allows to derive analogue of the results of [18], obtained for (3), also for the sets

\[
\{x(P)x(Q) : P \in \mathcal{P}, Q \in \mathcal{Q}\} \quad \text{and} \quad \{x(P \oplus Q) : P \in \mathcal{P}, Q \in \mathcal{Q}\}.
\]

Acknowledgements

This paper was initiated during a very enjoyable visit of I. S. at the Department of Combinatorics & Optimization of the University of Waterloo whose hospitality, support and stimulating research atmosphere are gratefully appreciated. Research of I. S. was supported by ARC grant DP0556431.

References


