On the Sum-Product Problem 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
igor@comp.mq.edu.au

Abstract

Let $E$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$ of $q$ elements and $x(Q)$ denote the $x$-coordinate of a point $Q = (x(Q), y(Q))$ on $E$. Given an $\mathbb{F}_q$-rational point $P$ of order $T$, we show that for any subsets $\mathcal{A}, \mathcal{B}$ of the unit group of the residue ring modulo $T$, at least one of the sets

$$\{x(aP) + x(bP) : a \in \mathcal{A}, b \in \mathcal{B}\} \text{ and } \{x(abP) : a \in \mathcal{A}, b \in \mathcal{B}\}$$

is large. This question is motivated by a series of recent results on the sum-product problem over finite fields and other algebraic structures.

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 [17].

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 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.

This question is 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, 5, 6, 9, 10, 11, 12] for the background and further references.

We remark that yet another variant of the sum-product problem for elliptic curves has recently been considered in [16] where it is shown that for sets $\mathcal{R}, \mathcal{S} \subseteq E(\mathbb{F}_q)$ at least one of the sets

$$\{x(R) + x(S) : R \in \mathcal{R}, \ S \in \mathcal{S}\} \quad \text{and} \quad \{x(R \oplus S) : R \in \mathcal{R}, \ S \in \mathcal{S}\}$$

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

As in [16], our approach is based on the argument of M. Garaev [6] which we combine with a bound of certain bilinear character sums over points of $E(\mathbb{F}_q)$ which have been considered in [1] (instead of the estimate of [15] used in [16]).
In fact here we present a slight improvement of the result of [1] that is based on using the argument of [7].

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 $c > 0$.

**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.

## 2 Bilinear Sums over Elliptic Curves

Let

$$T_{\rho, \vartheta}(\psi, \mathcal{K}, \mathcal{M}) = \sum_{k \in \mathcal{K}} \left| \sum_{m \in \mathcal{M}} \rho(k) \vartheta(m) \psi(x(kmP)) \right|, \tag{2}$$

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

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

and $\psi$ is a nontrivial additive character of $\mathbb{F}_q$.

These sums have been introduced and estimated in [1]. Here we obtain a stronger result by using the approach to sums of this type given in [7].

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

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

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

$$T_{\rho, \vartheta}(\psi, \mathcal{K}, \mathcal{M}) \ll \# \mathcal{K}^{\frac{1}{2\nu+2}} \# \mathcal{M}^{\frac{1}{2\nu+2}} T^{\frac{\nu+1}{\nu+2}} q^{\frac{\nu+1}{\nu+2}} (\log q)^{\frac{1}{\nu+2}}.$$
Proof. We follow the scheme of the proof of [7, 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 $\mathcal{K}$, $\mathcal{M}$, $\mathbb{Z}_T^*$ play the roles of $\mathcal{X}$, $\mathcal{L}_d$ and $\mathcal{U}_d$ in the proof of [7, Lemma 4], respectively. In particular, for some integer parameter $L$ with

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

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

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

Then we arrive to the following analogue of [7, Bound (4)]:

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

where

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

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

$$\sum_{z \in \mathcal{H}} \exp \left( \frac{2\pi ia}{p} \left( \sum_{j=1}^{\nu} z^{t v_j} - \sum_{j=\nu+1}^{2\nu} z^{t v_j} \right) \right) \ll \max_{1 \leq j \leq 2\nu} v_j q^{1/2}$$

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 [14]:

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

where $\mathcal{H}$ is the subgroup of $E(\mathbb{F}_p)$ (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 $(v_1, \ldots, v_\nu)$. 

4
Now since \(# E(\mathcal{F}_q) = O(q)\), using an argument similar to the one given in [7] and recalling (4) we obtain
\[
M_t \ll \sum_{v_1 \in \mathcal{V}} \cdots \sum_{v_\nu \in \mathcal{V}} \left( \prod_{j=1}^{\nu} \chi_M(v_j t) \right) T
+ \sum_{v_1 \in \mathcal{V}} \cdots \sum_{v_\nu \in \mathcal{V}} \left( \prod_{j=1}^{2\nu} \chi_M(v_j t) \right) q^{1/2}(\# \mathcal{V} \log q)^2.
\]
Therefore
\[
M_t \ll \left( \sum_{v \in \mathcal{V}} \chi_M(v t) \right)^\nu T + \left( \sum_{v \in \mathcal{V}} \chi_M(v t) \right)^{2\nu} q^{1/2}(\# \mathcal{V} \log q)^2.
\]
This leads to the following
\[
T_{\rho, \vartheta}(\psi, \mathcal{K}, \mathcal{M}) \ll \frac{(\# \mathcal{K})^{1-\frac{1}{2\nu}}}{(\# \mathcal{V}^{1/2})} T^{1/2} \sum_{t \in \mathbb{Z}_T^*} \left( \sum_{v \in \mathcal{V}} \chi_M(v t) \right)^{1/2}
+ \frac{(\# \mathcal{K})^{1-\frac{1}{2\nu}}}{(\# \mathcal{V}^{1/2})} (\# \mathcal{V} \log q)^{1/\nu} q^{1/4\nu} \sum_{t \in \mathbb{Z}_T^*} \left( \sum_{v \in \mathcal{V}} \chi_M(v t) \right).
\]
On the other hand we have
\[
\sum_{t \in \mathbb{Z}_T^*} \left( \sum_{v \in \mathcal{V}} \chi_M(v t) \right) = \# \mathcal{M} \# \mathcal{V},
\]
and by the Cauchy inequality we get
\[
\sum_{t \in \mathbb{Z}_T^*} \left( \sum_{v \in \mathcal{V}} \chi_M(v t) \right)^{1/2} \leq (\# \mathbb{Z}_T^*)^{1/2} \left( \sum_{t \in \mathbb{Z}_T^*} \sum_{v \in \mathcal{V}} \chi_M(v t) \right)^{1/2}
\leq T^{1/2} (\# \mathcal{M} \# \mathcal{V})^{1/2}.
\]
Thus
\[
T_{\rho, \vartheta}(\psi, \mathcal{K}, \mathcal{M}) \ll \frac{(\# \mathcal{K})^{1-\frac{1}{2\nu}}}{(\# \mathcal{V}^{1/2})} T^{1/2\nu+1/2} (\# \mathcal{M})^{1/2}
+ (\# \mathcal{K})^{1-\frac{1}{2\nu}} (\# \mathcal{V} \log q)^{1/\nu} q^{1/4\nu} \# \mathcal{M}.
\]
Let
\[ L = \left\lfloor \frac{T^{1/2}}{q^{1/(v+2)} (\log q)^{2/(v+2)} (#M)^{\frac{v}{v+2}}} \right\rfloor. \]

We note that if \( L = 0 \) then
\[ T^{1/2} \leq q^{1/(v+2)} (\log q)^{1/(v+2)} (#M)^{\frac{v}{v+2}} \leq q^{1/(v+2)} (\log q)^{1/(v+2)} T^{1/(v+2)} \]
and thus
\[ T \leq q^{1/2} (\log q)^2. \]

It is easy to check that in this case
\[
\frac{(\#K)^{1-\frac{1}{2v}} (#M)^{\frac{v}{v+2}} T^{\frac{v+1}{(v+2)}} q^{\frac{1}{4(v+2)}} (\log q)^{\frac{1}{v+2}}}{\#K \#M} \\
\geq \frac{(\#K)^{-\frac{1}{2v}} (#M)^{-\frac{1}{2v+2}} q^{\frac{1}{4(v+2)}} (\log q)^{\frac{1}{v+2}}}{T^{-\frac{1}{2v+2}} q^{\frac{1}{4(v+2)}} (\log q)^{\frac{1}{v+2}}} \\
\geq T^{-\frac{1}{2v+2}} q^{\frac{1}{4(v+2)}} (\log q)^{\frac{1}{v+2}} \\
= T^{-\frac{1}{2(v+2)}} q^{\frac{1}{4(v+2)}} (\log q)^{\frac{1}{v+2}} \geq 1.
\]
thus the result is trivial.

We now assume that \( L \geq 1 \) and choose \( V \) to be of cardinality \( \#V = L \). Then we have
\[ T^{1/2} \geq \#V \geq \frac{T^{1/2}}{2q^{1/(v+2)} (\log q)^{1/(v+2)} (#M)^{\frac{v}{v+2}}} \]
and \( L \leq T(\log q)^{-2} \) provided that \( q \) is large enough. Now the result follows from (5). \( \square \)

3 Lower Bound for the Sum-Product Problem on Elliptic Curves

**Theorem 2.** Let \( A \) and \( B \) be arbitrary subsets of \( \mathbb{Z}_q^* \). Then for the sets \( S \) and \( T \), given by (1), we have
\[ \#S \#T \geq \operatorname{min} \{ q\#A, (#A)^2 (#B)^{5/3} q^{-1/6} T^{-4/3} (\log q)^{-2/3} \}. \]
Proof. Let
\[ \mathcal{H} = \{ab : a \in \mathcal{A}, b \in \mathcal{B}\}. \]
Following the idea of M. Garaev \cite{6}, we now denote by \( J \) the number of solutions \((b_1, b_2, h, u)\) to the equation
\[ x(hb_1^{-1}P) + x(b_2P) = u, \quad b_1, b_2 \in \mathcal{B}, h \in \mathcal{H}, u \in S. \]  \hspace{1cm} (6)
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 (6), we obtain
\[ J \geq \# \mathcal{A}(\# \mathcal{B})^2. \]  \hspace{1cm} (7)
To obtain an upper bound on \( J \) we use \( \Psi \) to denote the set of all additive characters of \( \mathbb{F}_q \) and write \( \Psi^* \) for the set of nontrivial characters. Using the identity
\[ \frac{1}{q} \sum_{\psi \in \Psi} \psi(z) = \begin{cases} 0, & \text{if } z \in \mathbb{F}_q^*, \\ 1, & \text{if } z = 0, \end{cases} \]  \hspace{1cm} (8)
we obtain
\[ J = \sum_{b_1 \in \mathcal{B}} \sum_{b_2 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \sum_{u \in S} \frac{1}{q} \sum_{\psi \in \Psi} \psi \left( x(hb_1^{-1}P) - x(b_2P) - u \right) \]
\[ = \frac{1}{q} \sum_{\psi \in \Psi} \sum_{b_2 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi \left( x(hb_1^{-1}P) \right) \sum_{b_2 \in \mathcal{B}} \psi \left( x(b_2P) \right) \sum_{u \in S} \psi \left( -u \right) \]
\[ = \frac{\# \mathcal{B} \# S \# \mathcal{H}}{q} \]
\[ + \frac{1}{q} \sum_{\psi \in \Psi^*} \sum_{b_1 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi \left( x(hb_1^{-1}P) \right) \sum_{b_2 \in \mathcal{B}} \psi \left( x(b_2P) \right) \sum_{u \in S} \psi \left( -u \right). \]
Applying Theorem \([\text{I}]\) 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
\[ \left| \sum_{b_1 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi \left( x(hb_1^{-1}P) \right) \right| \ll \Delta. \]
where
\[
\Delta = (\#H)^{1/2}(\#B)^{2/3}T^{2/3}q^{1/12}(\log q)^{1/3}.
\]

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

(9)

Extending the summation over \( \psi \) to the full set \( \Psi \) and using the Cauchy inequality, we obtain
\[
\sum_{\psi \in \Psi} \left| \sum_{b \in B} \psi(x(bP)) \right| \left| \sum_{u \in S} \psi(u) \right| \leq \sqrt{\sum_{\psi \in \Psi} \left| \sum_{b \in B} \psi(x(bP)) \right|^2} \sqrt{\sum_{\psi \in \Psi} \left| \sum_{u \in S} \psi(u) \right|^2}.
\]  

(10)

Recalling the orthogonality property (8), we derive
\[
\sum_{\psi \in \Psi} \left| \sum_{b \in B} \psi(x(bP)) \right|^2 = q\#\{(b_1, b_2) \in \mathcal{B}^2 : b_1 \equiv \pm b_2 \pmod{T}\} \ll \#B.
\]

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

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

Substituting these bounds in (10) we obtain
\[
\sum_{\psi \in \Psi^*} \left| \sum_{b \in B} \psi(x(bP)) \right| \left| \sum_{u \in S} \psi(u) \right| \ll q\sqrt{\#B\#S},
\]

which after inserting in (9), yields
\[
J \ll \frac{(\#B)^2\#S\#H}{q} + \Delta(\#S)^{1/2}(\#B)^{1/2}.
\]  

(11)
Thus, comparing (7) and (11), we derive
\[
\frac{(#B)^2 #S#H}{q} + \Delta(#S)^{1/2} (#B)^{1/2} \gg #A(#B)^2.
\]
Thus either
\[
\frac{(#B)^2 #S#H}{q} \gg #A(#B)^2, \tag{12}
\]
or
\[
\Delta(#S)^{1/2} (#B)^{1/2} \gg #A(#B)^2. \tag{13}
\]
If (12) holds, then we have
\[
#S#H \gg q#A.
\]
If (13) 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 3.** For any fixed \(\varepsilon > 0\) there exists \(\delta > 0\) such that if \(A, B \subseteq \mathbb{Z}_T^*\) are arbitrary subsets with
\[
q^{-\varepsilon} \geq #A \geq #B \geq T^{4/5+\varepsilon} q^{1/10},
\]
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 3 applies.

**Corollary 4.** for arbitrary subsets of \(A, B \subseteq \mathbb{Z}_T^*\) with
\[
#A = #B \geq T^{1/2} q^{7/16} (\log q)^{1/4}
\]
and for the sets \(S\) and \(T\), given by (1), we have
\[
#S#T \gg q#A.
\]
4 Upper Bound for the 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 5.** Let \( q = p \) be prime and let \( T \geq p^{3/4+\varepsilon} \). Then there are sets \( A = B \subset \mathbb{Z}_T^* \) of cardinality

\[
\#A = \#B = (1 + o(1))\varphi(T)^2/2p
\]

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

\[
\max\{\#S, \#T\} \leq (\sqrt{2} + o(1))\sqrt{p\#A}
\]
as \( p \to \infty \).

**Proof.** We recall the bound from [13] of exponential sums over subgroups of the group of points on elliptic curves which in particular implies that for any subgroup \( G \) of \( E(\mathbb{F}_p) \) the bound

\[
\sum_{G \in G} \exp(2\pi i \lambda x(G)/p) \ll p^{1/2}, \quad (14)
\]
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 [3, Section 16.2].

Using the inclusion-exclusion principle, we obtain

\[
\sum_{a=1 \atop \gcd(a,T)=1}^{T} \exp(2\pi i \lambda x(aP)/p) = \sum_{d|T} \mu(d) \sum_{a=1 \atop d|a}^{T/d} \exp(2\pi i \lambda x(aP)/p)
\]
\[
= \sum_{d|T} \mu(d) \sum_{b=1 \atop T/d}^{T/d} \exp(2\pi i \lambda x(bP)/p).
\]
Using (14) and recalling that
\[ \sum_{d|T} 1 = T^{o(1)} \]
see [8, Theorem 317], we derive
\[ \sum_{\gcd(a,T) = 1}^T \exp \left( 2\pi i \lambda (aP/p) \right) \ll p^{1/2+o(1)}. \]
Combining this with the Erdős-Turán inequality, see [4, 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 [8, 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. \qed

We remark that if \( T \geq p^{23/24+\varepsilon} \), then the cardinality of the sets \( \mathcal{A} \) and \( \mathcal{B} \) of Theorem 5 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 4 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 4 and Theorem 5 are tight in this range.
5 Comments

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

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

References

[1] 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.

[2] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, ‘Estimates for the number of sums and products and for exponential sums in fields of prime order’, J. Lond. Math. Soc., 73 (2006), 380–398.

[3] J. Bourgain, N. Katz and T. Tao, ‘A sum product estimate in finite fields and applications’, Geom. Funct. Analysis, 14 (2004), 27–57.

[4] M. Drmota and R. Tichy, Sequences, discrepancies and applications, Springer-Verlag, Berlin, 1997.

[5] M. Z. Garaev, ‘An explicit sum-product estimate in $\mathbb{F}_p$’, Intern. Math. Res. Notices, 2007 (2007), Article ID rnm035, 1–11.

[6] M. Z. Garaev, ‘The sum-product estimate for large subsets of prime fields’, Preprint, Proc. Amerc. Math. Soc., (to appear).

[7] M. Z. Garaev and A. A. Karatsuba, ‘New estimates of double trigonometric sums with exponential functions’, Arch. Math., 87 (2006), 33–40.

[8] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford Univ. Press, Oxford, 1979.
[9] D. Hart, A. Iosevich, D. Koh and M. Rudnev, ‘Averages over hyperplanes, sum-product theory in finite fields, and the Erdos-Falconer distance conjecture’, Preprint, 2007 (available from http://arxiv.org/abs/0707.3473).

[10] D. Hart, A. Iosevich and J. Solymosi, ‘Sums and products in finite fields via Kloosterman Sums’, Intern. Math. Res. Notices, 2007 (2007), Article ID rnm007, 1–14.

[11] N. H. Katz and C.-Y. Shen, ‘Garaev’s inequality in finite fields not of prime order’, J. Anal. Combin., 3 (2008), Article #3.

[12] N. H. Katz and C.-Y. Shen, ‘A slight improvement to Garaev’s sum product estimate’, Proc. Amerc. Math. Soc., (to appear).

[13] 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.

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

[15] I. E. Shparlinski, ‘Bilinear character sums over elliptic curves’, Finite Fields and Their Appl., 14 (2008), 132–141.

[16] I. E. Shparlinski, ‘On the elliptic curve analogue of the sum-product problem’, Finite Fields and Their Appl., (to appear).

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