Journal of Number Theory 140 (2014) 299–313

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Exponential sums over points of elliptic curves

Omran Ahmadi [a], Igor E. Shparlinski [b,*]

[a] *School of Mathematics, Institute for Research in Fundamental Sciences, P.O. Box 19395-5746, Tehran, Iran*

[b] *Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia*

ARTICLE INFO

Article history:
Received 21 August 2013
Received in revised form 31 January 2014
Accepted 31 January 2014
Available online 4 March 2014
Communicated by David Goss

MSC:
primary 11L07, 11T23
secondary 11G20

Keywords:
Exponential sums
Finite fields
Elliptic curves

ABSTRACT

We derive a new bound for some bilinear sums over points of an elliptic curve over a finite field. We use this bound to improve a series of previous results on various exponential sums and some arithmetic problems involving points on elliptic curves.

1. Introduction

Let q be a prime power and let $\mathcal{E}$ be an elliptic curve defined over the finite field $\mathbb{F}_q$ of q elements of characteristic $p \geqslant 5$ given by an affine Weierstraß equation

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

with some $A, B \in \mathbb{F}_q$, see [2,5,34].

* Corresponding author.
E-mail addresses: oahmadid@ipm.ir (O. Ahmadi), igor.shparlinski@unsw.edu.au (I.E. Shparlinski).

http://dx.doi.org/10.1016/j.jnt.2014.01.016

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. In particular, we sometimes work with group characters associated with this group.

As usual, we write every point $P \neq \mathcal{O}$ on $\mathcal{E}$ as $P = (x(P), y(P))$. Let $\mathcal{E}(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on $\mathcal{E}$. We recall that the celebrated result of Bombieri [6] implies, in particular, an estimate of order $q^{1/2}$ for exponential sums with functions from the function field of $\mathcal{E}$ taken over all points of $\mathcal{E}(\mathbb{F}_q)$. More recently, various character sums over points of elliptic curves have been considered in a number of papers, see [1,3,8,12,13,17–19,25,26,28,30,32] and references therein. These estimates are motivated by various applications to such areas as

- pseudorandom number generators from elliptic curves, see the most recent works [4,8,20–23] and also the survey [31];
- randomness extractors from elliptic curves [9,10];
- analysing an attack on the Digital Signature Algorithm on elliptic curves [24];
- hashing to elliptic curves [14];
- finding generators and the structure of the groups of points on elliptic curves [17,32];
- constructing some special bases related to quantum computing [33].

We fix a nonprincipal additive character ψ of $\mathbb{F}_q$. All of our estimates are uniform with respect to the additive character ψ.

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

Given two sets $\mathcal{A}$, $\mathcal{B}$ in the unit group $\mathbb{Z}_T^*$ of the ring of integers $\mathbb{Z}_T$ modulo T, and arbitrary complex functions α and β supported on $\mathcal{A}$ and $\mathcal{B}$ with

$$|\alpha_a| \leqslant 1, \ a \in \mathcal{A}, \quad \text{and} \quad |\beta_b| \leqslant 1, \ b \in \mathcal{B},$$

we consider the bilinear sums of *multiplicative type*:

$$U_{\alpha,\beta}(\psi, \mathcal{A}, \mathcal{B}; G) = \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \alpha_a \beta_b \psi\bigl(x(abG)\bigr). \tag{1}$$

Furthermore, given two sets $\mathcal{P}, \mathcal{Q} \subseteq \mathcal{E}(\mathbb{F}_q)$ and arbitrary complex functions $\rho(P)$ and $\vartheta(Q)$ supported on $\mathcal{P}$ and $\mathcal{Q}$ we consider the bilinear sums of *additive type*:

$$V_{\rho,\vartheta}(\psi, \mathcal{P}, \mathcal{Q}) = \sum_{P \in \mathcal{P}} \sum_{Q \in \mathcal{Q}} \rho(P)\vartheta(Q)\psi\bigl(x(P \oplus Q)\bigr). \tag{2}$$

Bounds of the sums $U_{\alpha,\beta}(\psi, \mathcal{A}, \mathcal{B}; G)$ and $V_{\rho,\vartheta}(\psi, \mathcal{P}, \mathcal{Q})$ are proved in [1,3] and [28], respectively, where several applications of these bounds have been shown.

Here we improve the bound of [28] and use it with the bound of [1], and also with some additional arguments, to refine a series of previous results. In particular, we give improvements: