Journal of Number Theory 167 (2016) 304–316

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Bounds of double multiplicative character sums and gaps between residues of exponential functions ☆

Igor E. Shparlinski [a,*], Kam-hung Yau [b]

[a] *Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia*
[b] *Department of Mathematics, The University of Auckland, Auckland 1010, New Zealand*

ARTICLE INFO

Article history:
Received 27 November 2015
Received in revised form 14 March 2016
Accepted 14 March 2016
Available online 6 May 2016
Communicated by David Goss

MSC:
11A07
11L40

Keywords:
Character sums
Intervals
Exponential function
Gaps

ABSTRACT

We derive two new upper bounds on the double multiplicative character sum over subgroups and intervals

$$R_\chi(a, g, \mathcal{I}, N) = \sum_{x=1}^{H} \left| \sum_{n=1}^{N} \chi(x + ag^n) \right|$$

where χ is a multiplicative character modulo a prime p, H and N are positive integers and a and g are integers with $\gcd(ag, p) = 1$. One bound is unconditional and based on a recent result of Cilleruelo and Garaev (2014), the other bound is conditional on the Generalised Riemann Hypothesis (GRH). These bounds complement and improve in some ranges on the recent results of Chang and Shparlinski (2014).

☆ This work was supported by Australian Research Council Grants DP130100237 and DP140100118.
* Corresponding author.
E-mail addresses: igor.shparlinski@unsw.edu.au (I.E. Shparlinski), kyau548@aucklanduni.ac.nz (K.-h. Yau).

http://dx.doi.org/10.1016/j.jnt.2016.03.022
0022-314X/© 2016 Elsevier Inc. All rights reserved.

1. Introduction

For an interval $\mathcal{I} = \{1, \dots, H\}$ of H consecutive integers and a multiplicative subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ of order T we define the sums

$$S_\chi(a, \mathcal{I}, \mathcal{G}) = \sum_{x\in\mathcal{I}} \left| \sum_{\lambda\in\mathcal{G}} \chi(x + a\lambda) \right|, \quad 1 \le a < p,$$

with a multiplicative character χ of $\mathbb{F}_p^*$. Nontrivial upper bound can be obtained by applying the Burgess bound [6, Theorem 12.6] if $H \ge p^{1/4+\varepsilon}$. Several other bounds, nontrivial in a wide range of parameters H and T, have been shown by Chang and Shparlinski [3].

Here we combine a result of Cilleruelo and Garaev [4, Theorem 1(i)] with the approach of Chang and Shparlinski [3] to obtain new bounds on double multiplicative character sums

$$R_\chi(a, g, \mathcal{I}, N) = \sum_{x\in\mathcal{I}} \left| \sum_{n=1}^{N} \chi(x + ag^n) \right|, \quad 1 \le a < p,$$

where g is a generator of a multiplicative subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ of order T and an integer $N \le T$. In particular, these estimates are nontrivial in a very wide range of parameters (H, T). We remark that the results of [3] can be extended for incomplete sums, however we improve such potential extensions in a wide range of parameters H and N, see also Section 6.

Finally, we also obtain stronger bounds on the sums $R_\chi(a, g, \mathcal{I}, N)$ under the Generalised Riemann Hypothesis (GRH).

We also give an application of our results to some exponential congruence which in its simplest form has appeared in a number of works [11,12,16]. In particular, it is related to the problem of the distribution of spacings between residues of exponential functions that has been considered by Rudnick and Zaharescu [11].

Throughout the paper, as usual $A \ll B$ is equivalent to the inequality $|A| \le cB$ with some constant $c > 0$ (all implied constants are absolute throughout the paper).

2. Main results

The following results give nontrivial upper bounds that are valid without any restrictions on the smallest length of the intervals $\mathcal{I}$. It is however sometimes convenient to assume that this length is at most $p^{0.3}$.

For real $\kappa > 0$ we define

$$\vartheta(\kappa) = \min\left\{ \frac{\lfloor \alpha(\kappa) \rfloor + 1}{4\lfloor \alpha(\kappa) \rfloor + 2}, \frac{\lceil \alpha(\kappa) \rceil \kappa}{2} \right\}, \tag{1}$$