Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 339 (2004) 463–466
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

Sum-product theorem and exponential sum estimates in residue classes with modulus involving few prime factors

Jean Bourgain [a], Mei-Chu Chang [b]

[a] *School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA*
[b] *Department of Mathematics, University of California, Riverside, California, USA*

Received 19 August 2004; accepted 28 August 2004

Available online 28 September 2004

Presented by Jean Bourgain

Abstract

In this Note, we extend the results of Bourgain, Konyagin and Glibichuk to certain composite moduli q involving few 'large' primes. First a 'sum-product' theorem for subsets A of $\mathbb{Z}_q$ is obtained, ensuring that $|A+A|+|A.A| > c|A|^{1+\varepsilon}$ provided $|A| < q^{1-\delta}$ and A does not have a 'large' intersection with a translate of a subring. Next, exponential sum estimates are established. In particular nontrivial bounds are obtained for the exponential sums associated to a multiplicative subgroup $H < \mathbb{Z}_q^*$, with applications to Heilbronn-type sums. ***To cite this article: J. Bourgain, M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***
© 2004 Académie des sciences. Published by Elsevier SAS. All rights reserved.

Résumé

Un théorème somme-produit et des estimées des sommes exponentielles dans les classes de résidus avec module composé comportant un nombre borné de nombres premiers. Nous présentons dans cette Note une extension des résultats obtenus par Bourgain, Konyagin et Glibichuk pour les modules composés q dont la factorization ne comporte qu'un nombre borné de nombres premiers 'grands'. D'abord nous démontrons un théorème « somme-produit » pour les sous-ensembles A de $\mathbb{Z}_q$, affirmant que $|A+A|+|A.A| > c|A|^{1+\varepsilon}$ si $|A| < q^{1-\delta}$ et n'a pas de « grosse » intersection avec une translatée d'un sous-anneau de $\mathbb{Z}_q$. Ensuite on obtient des estimées sur des sommes exponentielles, en particulier associées à des sous-groupes multiplicatifs $H < \mathbb{Z}_q^*$. Ils s'appliquent aux sommes de type Heilbronn pour lesquelles on établit des estimées non-trivials. ***Pour citer cet article : J. Bourgain, M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***
© 2004 Académie des sciences. Published by Elsevier SAS. All rights reserved.

Version française abrégée

On considère les classes de résidus $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ où q est un nombre composé $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où $\alpha_1 + \cdots + \alpha_r$ est suppose borné et les $p_i > q^{\varepsilon_0}$. Dans ce contexte, nous généralisons les résultats de [2,3].

E-mail address: bourgain@ias.edu (J. Bourgain).

1631-073X/$ – see front matter © 2004 Académie des sciences. Published by Elsevier SAS. All rights reserved.
doi:10.1016/j.crma.2004.08.007

Soit $A \subset \mathbb{Z}_q$ tel gue $|A| < q^{1-\delta}$ et $|\pi_p(A)| > q^{\delta}$ pour tout nombre premier p divisant q. On dénote ici $\pi_p : \mathbb{Z}_q \to \mathbb{Z}_p$ l'application quotient mod p. Alors $|A+A| + |A.A| > c|A|^{1+\varepsilon}$, où $\varepsilon = \varepsilon(\delta) > 0$. Ce théorème somme-produit nous permet ensuite d'obtenir des estimées non-triviales sur les sommes exponentielles mod q, suivant la même approche de [2,3]. Soit $H < \mathbb{Z}_q^*$ un sous-groupe multiplicatif et supposons $|\pi_p(H)| > q^{\delta}$ pour tout premier $p|q$. Alors

$$\max_{a \in \mathbb{Z}_q^*} \left| \sum_{x \in H} e_q(ax) \right| < C|H|q^{-\varepsilon}$$

où $\varepsilon = \varepsilon(\delta) > 0$.

En particulier, pour les sommes de Gauss, on à

$$\max_{a \in \mathbb{Z}_q^*} \left| \sum_{x=1}^{q} e_q(ax^k) \right| < Cq^{1-\varepsilon}$$

à condition que $\frac{p}{(p-1,k)} > q^{\delta}$ pour tout premier $p|q$.

Ceci nous permet d'établir des bornes sur les sommes de Heilbronn (voir [8,5,6]) en toute généralité, donc

$$\max_{(a,p)=1} \left| \sum_{x=1}^{p} e_{p^{r+1}}(ax^{p^r}) \right| < c_r p^{1-\varepsilon_r}.$$

Seulement le cas $r = 1$ ne semble avoir été traiter dans la littérature (voir [5,6]).

1. A sum-product estimate

In what follows, we consider the residue classes $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ where q is a composite number of the form $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ involving a bounded number of large primes, thus

$$\alpha_1 + \cdots + \alpha_r < C, \tag{1}$$

$$p_i > q^{\varepsilon_0} \quad (1 \leqslant i \leqslant r). \tag{2}$$

All statements in this and the next section depend on the constants C, ε_0 and we shall no longer make this explicit.

The results and methods involved in this Note follow closely [2,3] dealing with the case of prime modulus $q = p$. Ruling out the 'obvious' exceptions we will obtain here very similar results for $\mathbb{Z}_q$, with q as a above.

The main combinatorial tool is a 'sum-product' type theorem for general subsets $A \subset \mathbb{Z}_q$. If $q = p$ is prime, it was shown in [4] that

$$|A+A| + |A.A| < c|A|^{1+\varepsilon} \quad \text{provided} \quad p^{\delta} < |A| < p^{1-\delta} \tag{3}$$

and in [2,3] the assumption on A was weakened to $|A| < p^{1-\delta}$. Such a result is obviously false in $\mathbb{Z}_q$ with q composite, due to the presence of nontrivial subrings. The following result holds, however.

Theorem 1.1. *Let $A \subset \mathbb{Z}_q$ satisfy $|A+A| + |A.A| < |A|^{1+\varepsilon}$. Then one of the following holds.*

(i) $|A| > q^{2-\delta}$
(ii) $|\pi_p(A)| < Cq^{\delta}$ *for some divisor p of q*

where $\delta = \delta(\varepsilon) \xrightarrow{\varepsilon \to 0} 0$.

The proof is closely related to Proposition 2 in [1], where a sum-product theorem is established for subsets A of the Cartesian product $\mathbb{Z}_p \times \mathbb{Z}_p$.

2. Exponential sums over $\mathbb{Z}_q$

With Theorem 1.1 at hand, one can extend most of the results from [2,3] to composite moduli q as considered above. Denote $e_q(y) = \exp(\frac{2\pi i}{q} y)$.

Theorem 2.1. *Let $H \lhd \mathbb{Z}_q^*$ be a multiplicative subgroup satisfying*

$$\big|\pi_p(H)\big| > q^{\varepsilon} \quad \text{for all prime divisors } p \text{ of } q. \tag{4}$$

Then

$$\max_{a\in\mathbb{Z}_q^*}\left|\sum_{x\in H} e_q(ax)\right| < C|H|q^{-\delta} \quad \text{with } \delta = \delta(\varepsilon) > 0. \tag{5}$$

More generally, in the spirit of [3] we may state the following estimate. For a subset $\mathcal{X}$ of $\mathbb{Z}_q^*$, denote

$$S_k(\mathcal{X}, a) = \sum_{x_1,\dots,x_k\in\mathcal{X}} e_q(ax_1\dots x_k). \tag{6}$$

Theorem 2.2. *Let $\mathcal{X} \subset \mathbb{Z}_q^*$ be an arbitrary set satisfying*

$$\big|\pi_p^{-1}(\xi) \cap \mathcal{X}\big| < q^{-\varepsilon}|\mathcal{X}| \quad \text{for all } p|q \text{ and } \xi \in \mathbb{Z}_p. \tag{7}$$

Then

$$\max_{a\in\mathbb{Z}_q^*}\big|S_k(\mathcal{X}, a)\big| < C|\mathcal{X}|^k q^{-\delta} \tag{8}$$

for $k > k_0(\varepsilon)$ and $\delta = \delta(\varepsilon) > 0$.

Theorem 2.1 applies in particular to Gauss sums mod q. Letting $H = \{x^k \mid x \in \mathbb{Z}_q^*\}$ (with $k \geqslant 2$ a fixed integer) we get for $p|q$ that $|\pi_p(H)| = \frac{p-1}{(p-1,k)}$. Hence

Theorem 2.3. *For q as above and k satisfying*

$$(p-1, k) < q^{-\varepsilon} p \quad \text{for all } p|q \tag{9}$$

we have

$$\max_{a\in\mathbb{Z}_q^*}\left|\sum_{x=1}^{q} e_q(ax^k)\right| < q^{1-\delta} \quad \text{with } \delta = \delta(\varepsilon) > 0. \tag{10}$$

There is the following consequence for Heilbronn-type exponential sums as considered in [8].

Corollary 2.4. *Let $r \geqslant 1$ be a fixed integer. For p prime, we have the bound*

$$\max_{(a,p)=1}\left|\sum_{x=1}^{p} e_{p^{r+1}}(ax^{p^r})\right| < Cp^{1-\varepsilon_r}. \tag{11}$$

Already for the case $r = 1$, no nontrivial bound was known for a long time (the problem was attributed in [8] to Davenport).

In [5], it is shown that

$$\max_{(a,p)=1}\left|\sum_{x=1}^{p} e_{p^2}(ax^p)\right| < cp^{11/12} \tag{12}$$

and this estimate is improved in [6] to $p^{7/8}$. Both arguments rely on Stepanov's method.

There seems to be no results in the literature for $r \geqslant 2$. Very recently, Konyagin mentioned to the author the work of his student Malyhin, establishing a nontrivial bound for $r = 2$.

Theorem 2.2 applies to exponential sums associated to powers of a fixed $\theta \in \mathbb{Z}_q^*$ (also incomplete sums). These are also of interest in cryptography (see [7] and its references). Thus we have the following estimate:

Theorem 2.5. *Let q be as above and $\varepsilon > 0$. Let $\theta \in \mathbb{Z}_q^*$ be such that for all prime divisors p of q, the multiplicative order $O_p(\theta)$ of θ* mod *p satisfies*

$$O_p(\theta) > q^{\varepsilon}. \tag{13}$$

Let $t > q^{\varepsilon}$. Then

$$\max_{a\in\mathbb{Z}_q^*}\left|\sum_{s=1}^{t} e_q(a\theta^s)\right| < Ctq^{-\delta} \quad \text{with } \delta = \delta(\varepsilon) > 0. \tag{14}$$

References

[1] J. Bourgain, Mordell's exponential sum estimate revisited, preprint, 2004; JAMS, submitted for publication.
[2] J. Bourgain, S. Konyagin, Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order, C. R. Acad. Sci. Paris, Ser. I 337 (2) (2003) 75–80.
[3] J. Bourgain, A. Glibichuk, S. Konyagin, Estimate for the number of sums and products and for exponential sums in fields of prime order, J. London Math. Soc., submitted for publication.
[4] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields and their applications, Geom. Funct. Anal. (GAFA) 14 (1) (2004) 27–57.
[5] R. Heath-Brown, An estimate for Heilbronn's exponential sum, in: Analytic Number Theory, Proc. Conf. in honor of H. Halberstam, Birkhäuser, Boston, MA, 1996, pp. 451–463.
[6] R. Heath-Brown, S. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sums, Quart. J. Math. 51 (2000) 221–235.
[7] S. Konyagin, I. Shparlinski, Character Sums with Exponential Functions and their Applications, Cambridge Tracts in Mathematics, vol. 136, Cambridge University Press, Cambridge, 1999.
[8] R. Odoni, Trigonometric sums of Heilbronn's type, Math. Proc. Comb. Philos. Soc. 98 (1985) 389–396.