Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 344 (2007) 349–352
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

Sum–product theorems and exponential sum bounds in residue classes for general modulus

Jean Bourgain

Institute for Advanced Study, Princeton, NJ 08540, USA

Received 11 January 2007; accepted 22 January 2007

Available online 27 February 2007

Presented by Jean Bourgain

Abstract

The purpose of this Note is to extend (in the appropriate formulation) the sum–product theorem in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ (established in [J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and applications, GAFA 14 (2004) 27–57; 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. 73 (2006) 380–398] for q prime, in [J. Bourgain, M. Chang, Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few factors, GAFA 16 (2) (2006) 327–366] for q composite with few factors and in [J. Bourgain, A. Gamburd, P. Sarnak, Sieving and expanders, C. R. Acad. Sci. Paris, Ser. I 343 (3) (2006) 155–159] for q square free) to the case of arbitrary modulus. Consequences to exponential sum bounds (mod q) are given. ***To cite this article: J. Bourgain, C. R. Acad. Sci. Paris, Ser. I 344 (2007).***

Résumé

Théorèmes sommes–produits et sommes exponentielles dans les classes de résidus pour module arbitraire. Dans cette Note, nous généralisons (avec un énoncé approprié) le théorème somme–produit dans $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, où q est arbitraire (pour q premier, un tel résultat fût obtenu dans [J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and applications, GAFA 14 (2004) 27–57 ; 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. 73 (2006) 380–398], pour q un nombre composé avec un nombre de facteurs premiers borné dans [J. Bourgain, M. Chang, Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few factors, GAFA 16 (2) (2006) 327–366], et pour q un produit simple dans [J. Bourgain, A. Gamburd, P. Sarnak, Sieving and expanders, C. R. Acad. Sci. Paris, Ser. I 343 (3) (2006) 155–159]. Nous en déduisons également des estimées sur certaines sommes exponentielles (mod q). ***Pour citer cet article : J. Bourgain, C. R. Acad. Sci. Paris, Ser. I 344 (2007).***

Version française abrégée

Soit $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ l'anneau des classes de residues (mod q).
Nous établissons la propriété 'sommes-produits' suivante :

E-mail address: bourgain@ias.edu.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2007.01.019

Théorème 1. *Pour tout $\delta_1 > 0, \delta_2 > 0$, il existe $\varepsilon > 0$ et $\delta_3 > 0$ tel que si q est un entier arbitraire suffisament grand et $A \subset \mathbb{Z}_q$ satisfait les conditions*

(i) $|A| < q^{1-\delta_1}$,
(ii) *Si* $q_1|q$ *et* $q_1 > q^{\varepsilon}$, *on a* $|\pi_{q_1}(A)| > q_1^{\delta_2}$

on a

(iii) $|A + A| + |A.A| > q^{\delta_3}|A|$.

Nous dénotons ici $\pi_{q_1} : \mathbb{Z}_q \to \mathbb{Z}_{q_1}$, $q_1|q$, l'application quotient et $A + A = \{x + y \mid x, y \in A\}$ (resp. $A.A = \{x.y \mid x, y \in A\}$) l'ensemble « somme » (resp. l'ensemble « produit »).

Ce genre de résultats fut obtenu antérieurement dans certains cas particuliers, notamment pour q premier [8,7], q composé avec nombre de facteurs borné [4] et q produit simple [6]. Ils mènent à des estimées nouvelles sur les sommes exponentielles (voir [7,4,1,2]) et de nouveaux exemples d'expanseurs sur les groupes $\mathrm{SL}_2(q)$ (voir [6]).

Nous mentionnons ici la conséquence suivante du Théorème 1 :

Théorème 2. *Pour tout $\gamma > 0$, il existe $\varepsilon > 0, \tau > 0$ et un entier positif k tel que si $A_1, \ldots, A_k \subset \mathbb{Z}_q$ et satisfont la condition*

(i) *Si* $q_1|q, q_1 > q^{\varepsilon}$ *et* $\xi \in \mathbb{Z}_{q_1}$, *on a*

$$\left|A_i \cap \pi_1^{-1}(\xi)\right| < q_1^{-\gamma}|A| \quad (1 \leqslant i \leqslant k).$$

Alors, on a

(ii) $\max_{\xi \in \mathbb{Z}_q^*} |\sum_{x_1 \in A_1, \ldots, x_k \in A_k} e_q\ (\xi x_1 \ldots x_k)| < q^{-\tau}|A_1| \cdots |A_k|$ (*où* $e_q(x) = e(\frac{2\pi \mathrm{i}}{q}x)$).

1. Introduction

We denote by $\mathbb{Z}_q$ the ring of residue classes mod q.

For $q_1|q$, let $\pi_{q_1} : \mathbb{Z}_q \to \mathbb{Z}_{q_1}$ be the quotient map.

Our purpose is to state the general case of the sum–product theorems obtained in [8,7,4,6] for special moduli q. We have

Theorem 1. *Given $\delta_1, \delta_2 > 0$, there are $\varepsilon > 0$ and $\delta_3 > 0$ such that the following holds. Let q be an arbitrary* (*sufficiently large*) *modulus and $A \subset \mathbb{Z}_q$ satisfying*

(i) $|A| < q^{1-\delta_1}$,
(ii) *If* $q_1|q$ *and* $q_1 > q^{\varepsilon}$, *then* $|\pi_{q_1}(A)| > q_1^{\delta_2}$.

Then

(iii) $|A + A| + |A.A| > q^{\delta_3}|A|$.

Remark 1. In Theorem 1, ε depends on both δ_1 and δ_2 (unlike in the square-free case where ε only depends on δ_1, see [6]). An important aspect of Theorem 1 is the uniformity of the estimates in q.

Remark 2. If $q = p_1^{m_1} \cdots p_J^{m_J}$ is the prime factorization of q, the ring $\mathbb{Z}_q$ identifies with the product $\mathbb{Z}_{p_1^{m_j}} \times \cdots \times \mathbb{Z}_{p_J^{m_J}}$. To establish Theorem 1, we proceed in two steps. First we establish the result for q of the form $p = p^m$, p prime. We then treat the product, relying in particular on the methods from [2,6]. Both parts are technically rather involved and rely on combinatorial analysis on 'trees'.

2. Further results

Results such as Theorem 1 have further applications to the theory of exponential sums (cf. [7,4,1,2]) and the theory of expanders on groups (cf. [5,6]). We limit ourselves here to exponential sum bounds.

Theorem 2. *Given $\gamma > 0$, there are $\varepsilon > 0, \tau > 0$ and a positive integer $k \in \mathbb{Z}_+$ such that the following holds. Let q be an arbitrary modulus and $A_1, \ldots, A_k \subset \mathbb{Z}_q$ such that*

(i) *If $q_1|q, q_1 > q^\varepsilon$ and $\xi \in \mathbb{Z}_{q_1}$, we have*

$$\left|A_i \cap \pi_{q_1}^{-1}(\xi)\right| < q_1^{-\gamma}|A_i| \quad (1 \leqslant i \leqslant k).$$

Then

(ii) $\max_{\xi \in \mathbb{Z}_q^*} |\sum_{x_1 \in A_1, \ldots, x_k \in A_k} e_q(\xi x_1 \cdots x_k)| < q^{-\tau}|A_1| \cdots |A_k|$.

There is the following consequence to 'almost subgroups' (in the sense of [9]) of $\mathbb{Z}_q^*$, providing a certain generalization of the exponential sum bound for subgroups $H < \mathbb{Z}_q^*$ obtained in [2] (see also remarks below):

Corollary 3. *Given $\gamma > 0$ and $\kappa > 0$, there is $\varepsilon > 0$ such that the following holds. Let q be an arbitrary modulus and $H \subset \mathbb{Z}_q^*$ satisfy*

(i) *If $q_1|q, q_1 > q^\varepsilon$ and $\xi \in \mathbb{Z}_{q_1}$, we have*

$$\left|H \cap \pi_{q_1}^{-1}(\xi)\right| < q_1^{-\gamma}|H|$$

and

(ii) $|H.H| < |H|^{1+\varepsilon}$.

Then

(iii) $|\{\xi \in \mathbb{Z}_q \mid |\sum_{x \in H} e_q(\xi x)| > |H|^{1-\varepsilon}\}| < q^\kappa$.

Remarks.

(1) The previous statement was proven in [3] for q prime (see also [9] for a different proof).
(2) The result from [2] states that if $H < \mathbb{Z}_q^*$ (q arbitrary) is any subgroup such that $|H| > q^\varepsilon$, then

$$\max_{\xi \in \mathbb{Z}_q^*} \left| \sum_{x \in H} e_q(\xi x) \right| < q^{-\delta}|H| \tag{1}$$

where $\delta = \delta(\varepsilon) > 0$.
In the context of 'almost subgroups' i.e. H satisfying a property of the form Corollary 3, condition (ii), additional assumptions (of the form condition (i)) are necessary, however.
For instance, letting $q = p^2$ and

$$H = \left\{1 + pt \mid 0 \leqslant t < \sqrt{p}\right\} \tag{2}$$

it is clear that $|H.H| \leqslant 2|H|$, but

$$\left| \sum_{x \in H} e_{p^2}(\xi x) \right| > \frac{1}{2}|H| \tag{3}$$

for all $0 \leqslant \xi < \frac{1}{10}\sqrt{p}$.

References

[1] J. Bourgain, Mordell's exponential sum estimate revisited, JAMS 18 (2) (2005) 477–499.
[2] J. Bourgain, Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$. q arbitrary, J. Analyse 97 (2005) 317–356.
[3] J. Bourgain, Estimates on exponential sums related to the Diffie–Hellman distributions, GAFA 15 (1) (2005) 1–34.
[4] J. Bourgain, M. Chang, Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few factors, GAFA 16 (2) (2006) 327–366.
[5] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math., in press.
[6] J. Bourgain, A. Gamburd, P. Sarnak, Sieving and expanders, C. R. Acad. Sci. Paris, Ser. I 343 (3) (2006) 155–159.
[7] 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. 73 (2006) 380–398.
[8] J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and applications, GAFA 14 (2004) 27–57.
[9] T. Tao, V. Vu, Additive Combinatorics, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, 2006.