Available online at www.sciencedirect.com
SCIENCE DIRECT
C. R. Acad. Sci. Paris, Ser. I 337 (2003) 75–80
COMPTES RENDUS MATHEMATIQUE

Group Theory/Number Theory

Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order

Jean Bourgain [a,b], S.V. Konyagin [c]

[a] School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA
[b] Department of Mathematics, University of Illinois, Urbana, IL 61801, USA
[c] Department of Mechanics and Mathematics, Moscow State University, Moscow 119992, Russia

Received 18 May 2003; accepted 27 May 2003

Presented by Jean Bourgain

Abstract

Our first result is a 'sum–product' theorem for subsets A of the finite field $\mathbb{F}_p$, p prime, providing a lower bound on $\max(|A+A|, |A\cdot A|)$. As corollary, the second and main result provides new bounds on exponential sums associated to subgroups of the multiplicative group $\mathbb{F}_p^*$. ***To cite this article: J. Bourgain, S.V. Konyagin, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Résumé

Estimes sommes–produits et sur les sommes exponentielles associées à des sous-groupes d'un corps d'ordre premier. Notre premier résultat est un théorème « sommes–produits » pour des sous-ensembles A d'un corps fini $\mathbb{F}_p$, p un nombre premier, donnant une minoration du $\max(|A+A|, |A\cdot A|)$. Comme corollaire et résultat principal, on en déduit de nouvelles bornes sur les sommes exponentielles associées à des sous-groupes du groupe multiplicatif $\mathbb{F}_p^*$. ***Pour citer cet article : J. Bourgain, S.V. Konyagin, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Version française abrégée

Pour un sous-ensemble A d'un anneau, on dénote $A+A=\{a+b;\ a,b\in A\}$ et $A\cdot A=\{ab\mid a,b\in A\}$. Soit p un nombre premier. On démontre que si A est un sous-ensemble du corps $\mathbb{F}_p$ tel que $|A|<p^{1/2}$ on a une borne $\max(|A+A|, A\cdot A|)>c_1|A|^{1+c_2}$ où $c_1>0,\ c_2>0$ sont des constantes. Cette propriété nous permet ensuite d'obtenir l'estimée suivante sur les sommes exponentielles : il existe des constantes $c_1,\ c_2$ telles que pour p un nombre premier, $\delta>0$ et G un sous-groupe du groupe multiplicatif $\mathbb{F}_p^*$, $|G|\geqslant p^\delta$, on ait

$$\max_{\xi\in\mathbb{F}^*}\left|\sum_{x\in G}\exp\left(\frac{2\pi\mathrm{i}x\xi}{p}\right)\right|\leqslant|G|p^{-\gamma},$$

où $\gamma=\exp(-c_1/\delta^{c_2})$.

E-mail addresses: bourgain@math.ias.edu (J. Bourgain), konyagin@ok.ru (S.V. Konyagin).

1631-073X/$ – see front matter
doi:10.1016/S1631-073X(03)00281-4

1. Sum–product estimates

For a subset A of some ring, we consider the sum set

$$A + A := \{a + b:\ a, b \in A\}$$

and the product set

$$A \cdot A := \{ab:\ a, b \in A\}.$$

Let $|A|$ denote the cardinality of A. We have the obvious bounds

$$|A + A|, |A \cdot A| \geqslant |A|.$$

Erdős and Szemerédi [4] proved the inequality

$$\max\bigl(|A + A|, |A \cdot A|\bigr) \gg |A|^{1+\alpha}$$

for some $\alpha > 0$, where A is a subset of integers. (We write standard notation $g \gg f$ or $f \ll g$ if $|f| \leqslant Cg$ for some constant C.) The estimate (2) was improved in the series of papers [10,5,3]. As far as we know, the best estimate belongs to Solymosi [12] who has proved that for any set A of complex numbers with $|A| \geqslant 2$ we have

$$\max\bigl(|A + A|, |A \cdot A|\bigr) \gg |A|^{14/11}/\bigl(\log^3 |A|\bigr).$$

However, the proofs in all the cited papers could not be directly extended to subsets of finite fields. Let p be a prime, $F = \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, and let A be a nonempty subset of F. The inequality (1) is sharp if $|A| = p$ or $|A| = 1$, but it was believed that the lower estimate (2) holds for $|A|$ small comparatively to p. However, no related results were known until the recent paper [1] where the following theorem has been established.

Theorem A. *Let A be a subset of F such that*

$$p^{\delta} \leqslant |A| \leqslant p^{1-\delta}$$

for some $\delta > 0$. Then one has a bound of the form

$$\max\bigl(|A + A|, |A \cdot A|\bigr) \geqslant c(\delta)|A|^{1+\alpha}$$

for some $\alpha = \alpha(\delta) > 0$ and $c(\delta) > 0$.

Also, in [1] the reader can find some related problems, generalizations and applications of Theorem A. The proof of Theorem A uses an elegant idea of [2]. In this paper we present the following estimate.

Theorem 1.1. *Let A be a subset of F such that*

$$|A| < p^{1/2}.$$

Then one has a bound of the form

$$\max\bigl(|A + A|, |A \cdot A|\bigr) \geqslant c_1|A|^{1+c_2}$$

for some $c_1 > 0$ and $c_2 > 0$.

To prove Theorem A, the authors associated with a set $A \subset F$ the set

$$I(A) := \bigl\{a_1(a_2 - a_3) + a_4(a_5 - a_6):\ a_1, \ldots, a_6 \in A\bigr\}.$$

They found lower bounds for $|I(A)|$ and applied those bounds for estimation of $\max(|A + A|, |A \cdot A|)$. Using the ideas from [2] and [1] we give new lower estimates for $|I(A)|$.

We denote

$$A - A := \{a - b\colon\ a, b \in A\}.$$

Throughout the paper c and C will denote absolute positive constants.

Theorem 1.2. *Let A be a subset of F such that*

$$|A| < p^{1/2}.$$

Then one has a bound of the form

$$|A - A| \times \bigl|I(A)\bigr| \geqslant c|A|^{5/2}.$$

Observing that $|I(A)| \geqslant |A - A|$ we deduce from Theorem 1.2 an estimate for $|I(A)|$.

Corollary 1.3. *Let A be a subset of F such that*

$$|A| < p^{1/2}.$$

Then one has a bound of the form

$$\bigl|I(A)\bigr| \geqslant c|A|^{5/4}.$$

Also, one can get a good lower bound for $|I(A)|$ if $|A| > p^{1/2}$.

Theorem 1.4. *Let A be a subset of F such that*

$$|A| > p^{1/2}.$$

Then one has a bound of the form

$$\bigl|I(A)\bigr| \geqslant p/2.$$

Corollary 1.5. *Let A be a subset of F such that*

$$p^{\delta} \leqslant |A| \leqslant p^{1-\delta/4}$$

for some $\delta > 0$. Then one has a bound of the form

$$\bigl|I(A)\bigr| \geqslant c|A|p^{\delta/4}.$$

Using technique of [1], Theorem 1.1 can be deduced from Theorem 1.2. Also, Corollary 1.3 implies the following result:

Corollary 1.6. *Let A be a subset of F such that*

$$p^{\delta} \leqslant |A| \leqslant p^{1-\delta}$$

for some $\delta > 0$. Then one has a bound of the form

$$\max\bigl(|A + A|, |A \cdot A|\bigr) \geqslant c_1|A|p^{c_2\delta}$$

for some $c_1 > 0$ and $c_2 > 0$.

Denote $F^* := F \setminus \{0\}$. Let $A \subset F^*$ and

$$H := \bigl\{s \in F\colon\ \bigl|\bigl\{(a, b)\colon\ a, b \in A,\ s = a/b\bigr\}\bigr| \geqslant |A|^2/\bigl(5|A \cdot A|\bigr)\bigr\}.$$

Denote by G the multiplicative subgroup of F^* generating by H. We show that there is a coset G_1 of G such that

$$|A \cap G_1| \geqslant |A|/3.$$

To prove Theorem 1.2, we estimate $|A - A|$ and $|I(A)|$ from below in terms of $|G|$. To estimate $|A - A|$, we use (3) and the following fact.

Lemma 1.7. *Let G be a subgroup of F^*, $B \subset G$, $|B| < \sqrt{p}$. Then*

$$|B - B| \gg |A|^{5/2}/|G|.$$

To prove Lemma 1.7, we use some results on additive structure of subgroups of $\mathbb{F}_p^*$ established in [6] for estimation of exponential sums over subgroups.

2. Estimates of exponential sums over subgroups of $\mathbb{F}_p^*$

We denote $e(u) := \exp(2\pi \mathrm{i} u))$. Let $F = \mathbb{F}_p$, G be a subgroup of F^*. We wish to estimate

$$S(G) = \max_{\xi \in F^*} \left| \sum_{x \in G} e\left(\frac{x\xi}{p}\right) \right|$$

and, in particular, to have a bound of the form

$$S(G) \ll |G| p^{-\gamma}$$

with some $\gamma > 0$ for a wide class of subgroups G. Various applications of exponential sums over subgroups can be found in [9]. We have already mentioned that study of exponential sums was useful for sum–product estimates; we will see that, conversely, sum–product estimates can help to prove (4) in the most general situation.

It is well known that $S(G) \leqslant \sqrt{p}$ (this follows, for example, from [8], Theorem 5). Thus, (4) holds for $|G| \geqslant p^{1/2+\delta}$ with $\gamma = \gamma(\delta)$ (in our case $\gamma = \delta$). Shparlinski [11] proved (4) under a weaker assumption $|G| \geqslant p^{3/7+\delta}$, and this was further weakened to $|G| \geqslant p^{1/3+\delta}$ in [6] and to $|G| \geqslant p^{1/4+\delta}$ in [7]. Now we can prove (4) for all subgroups G satisfying the condition $|G| \geqslant p^{\delta}$ which is clearly sharp if do not care about dependence of γ on δ.

Theorem 2.1. *There exist positive constants C_1 and C_2 such that for $\delta > 0$ and $|G| \geqslant p^{\delta}$ we have*

$$S(G) \leqslant |G| p^{-\gamma}, \quad \gamma = \exp\bigl(-C_1/\delta^{C_2}\bigr).$$

The proof is based on the following assertion which, we hope, has an independent interest.

Theorem 2.2. *Let μ be a probability measure on $F = \mathbb{F}_p$ (equipped with normalized measure). There are constant $c > 0$ and $C > 0$ such that for all $\varepsilon > 0$ and $\varepsilon' = c\varepsilon > 0$ such that if*

$$p^{\varepsilon} \leqslant \sum \bigl|\hat{\mu}(\xi)\bigr|^2 \leqslant p^{1-\varepsilon}$$

then

$$\sum_{\xi} \int \bigl|\hat{\mu}(\xi)\bigr|^2 \bigl|\hat{\mu}(y\xi)\bigr|^2 \mu(\mathrm{d}y) \leqslant C p^{-\varepsilon'} \sum_{\xi} \bigl|\hat{\mu}(\xi)\bigr|^2.$$

The proof uses Theorem 1.1.

Let G be a subgroup of F^*, $|G| = p^\delta$. Let

$$\nu := \frac{1}{|G|}\sum_{x\in G}\delta_x \quad \text{and} \quad \nu_- = \frac{1}{|G|}\sum_{x\in G}\delta_{(-x)},$$

where δ_x is the indicator function of the element $x \in F$. Introduce the symmetric probability measures (for ℓ even)

$$\nu_\ell := \nu * \nu_- * \nu * \nu_- * \cdots * \nu_- \quad (\ell \text{ fold}).$$

Theorem 2.1 is a simple corollary of the following lemma.

Lemma 2.3. *There exist positive constants c, C_3, C_4 such that for every $\ell \geqslant 2$ which is a power of 2 there exists a power of $2\ell' = \ell'(\ell)$ such that for*

$$U := \sum_\xi \left|\hat{\nu}_\ell(\xi)\right|^2,$$

$$\varepsilon := \varepsilon(\ell) = \min(\log U/\log p, 1 - \log U/\log p), \quad p \geqslant C_3^{1/\varepsilon},$$

the following conditions hold:

$$\ell' \leqslant C_4\ell^2/\varepsilon;$$

$$\sum_\xi \left|\hat{\nu}_{\ell'}(\xi)\right|^2 \leqslant U p^{-c\varepsilon}.$$

To deduce Theorem 2.1 from Lemma 2.3, we define the sequence $\{\ell_j\}$ as $\ell_0 = 2$, $\ell_{j+1} = \ell'(\ell_j)$ for $j \geqslant 0$. We terminate the process when

$$\sum_\xi \left|\hat{\nu}_{\ell_J}(\xi)\right|^2 \leqslant p^{\delta/2}.$$

We observe that

$$\sum_\xi \left|\hat{\nu}(\xi)\right|^2 \leqslant p^{1-\delta}.$$

Therefore, for $\ell = \ell_j$, $j = 0, \ldots, J-1$, we have $\varepsilon(\ell_j) \geqslant \delta/2$, and, by Lemma 2.3,

$$\ell_{j+1} \leqslant 2C_4\ell_j^2/\delta.$$

Also, it is easy to get from Lemma 2.3 that $J \ll \log(1/\delta)$, and, by (6),

$$\ell_J \leqslant \exp\left(\frac{C_5}{\delta^{C_6}}\right).$$

Returning to the exponential sum, assume

$$|G|\left|\hat{\nu}(\xi)\right| = \left|\sum_{x\in G} e\left(\frac{x\xi}{p}\right)\right| > |G|^{1-\tau} \quad \text{for some } \xi \not\equiv 0.$$

Then (8) holds also for all ξy, $y \in G$, so that by (5)

$$|G|^{1-\ell_J\tau} < p^{\delta/2}.$$

Take $\tau = 1/(2\ell_J(\delta/2))$ to get a contradiction.

We observe that by using Lemma 3.1 from [9] we can terminate the iterations when

$$\sum_{\xi} \left|\hat{\nu}_{\ell_J}(\xi)\right|^2 \leqslant p^{\alpha}$$

for a fixed $\alpha < 1/2$.

To prove Lemma 2.3, we apply Theorem 2.2 to the measure $\mu = \nu_\ell$ and use the following lemma.

Lemma 2.4. *If a probability measure μ has a property*

$$\forall \xi \; \forall x \in G \quad \hat{\mu}(\xi) = \hat{\mu}(x\xi)$$

and for some $\xi \in F$ and $\gamma > 0$ we have $|\hat{\mu}(\xi)| > p^{-\gamma}$ then for any k which is a power of 2 the inequality

$$\sum_{G^k} \hat{\mu}\big(\xi(x_1 - x_2 + x_3 \cdots - x_k)\big) > p^{-k\gamma} |G|^k$$

holds.

Using Lemma 2.4 for $\mu = \nu_\ell$, $k = \ell$, we get the inequality

$$\int \hat{\mu}(\xi y)\mu(\mathrm{d}y) > p^{-\ell\gamma}$$

which can be combined with Theorem 2.2 to get Lemma 2.3.

Acknowledgements

The first author was partially supported by NSF grant 0322370. The second author was supported by grants 02-01-00248 from the Russian Foundation for Basic Research and RF N NSh-3004.2003.1.

References

[1] J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and their applications, ArXiv: math.CO/0301343v1, January 29, 2003, to appear in GAFA.
[2] G.A. Edgar, C. Miller, Borel subrings of the reals, Proc. Amer. Math. Soc. 131 (2003) 1121–1129.
[3] Gy. Elekes, On the umber of sums and products, Acta Arith. 81 (1997) 1121–1129.
[4] P. Erdős, E. Szemerédi, On sums and the products of integers, in: P. Erdős, L. Alpár, G. Halász (Eds.), Studies in Pure Mathematics, Akadémiai Kiadó–Birkhäuser, Budapest–Basel, 1983, pp. 213–218 (To the memory of Paul Turan).
[5] K. Ford, Sums and products from a finite set of real numbers, Ramanujan J. 2 (1998) 59–66.
[6] D.R. Heath-Brown, S.V. Konyagin, New bounds for Gauss sums derived from k-th powers, and for Heilbronn's exponential sums, Quart. J. Math. 51 (2000) 221–235.
[7] S.V. Konyagin, Estimates of trigonometric sums over subgroups and Gaussian sums, in: IV International Conference "Modern Problems of Number Theory and its Applications" dedicated to 180th anniversary of P.L. Chebyshev and 110th anniversary of I.M. Vinogradov, Topical Problems, Part 3, Department of Mechanics and Mathematics, Moscow Lomonosov State University, Moscow, 2002, pp. 86–114 [in Russian].
[8] N.M. Korobov, Exponential Sums and their Applications, Kluwer Academic, Dordrecht, 1992.
[9] S.V. Konyagin, I.E. Shparlinski, Character Sums with Exponential Functions and their Applications, in: Cambridge Tracts in Math., Vol. 136, Cambridge University Press, Cambridge, 1999.
[10] M. Nathanson, On sums and products of integers, Proc. Amer. Math. Soc. 125 (1997) 9–16.
[11] I.E. Shparlinski, Estimates for Gauss sums, Math. Notes 50 (1991) 140–146.
[12] J. Solymosi, On a question of Erdős and Szemerédi, Preprint, 2003.