Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 338 (2004) 825–830
COMPTES RENDUS MATHEMATIQUE

Logic

New bounds on exponential sums related to the Diffie–Hellman distributions

Jean Bourgain

Institute for Advanced Study, School of Mathematics, Princeton, NJ 08540, USA

Received 24 February 2004; accepted 2 March 2004

Available online 17 April 2004

Presented by Jean Bourgain

Abstract

Given $\theta \in \mathbb{F}_p^*$ (p prime) of multiplicative order $t > p^\delta$, we obtain nontrivial bounds on exponential sums

$$\sum_{s'=1}^{t} \left| \sum_{s=1}^{t} e_p\left(a\theta^s + c\theta^{ss'}\right) \right|$$

as well as the corresponding incomplete sums. These estimates are of relevance to several issues, such as the Diffie–Hellman distributions in cryptography, prime divisors of 'sparse integers', the distribution mod p of Mersenne numbers $M_q = 2^q - 1$ (q prime). The method is closely related to that of Bourgain and Konyagin (C. R. Acad. Sci. Paris, Ser. I 337 (2) (2003) 75–80). ***To cite this article: J. Bourgain, C. R. Acad. Sci. Paris, Ser. I 338 (2004).***

Résumé

Nouvelles estimées des sommes exponentielles liées aux distributions de Diffie–Hellman. Soit $\theta \in \mathbb{F}_p^*$ (p premier) d'ordre multiplicatif $t > p^\delta$, on obtient des bornes non-triviales sur les sommes exponentielles

$$\sum_{s'=1}^{t} \left| \sum_{s=1}^{t} e_p\left(a\theta^s + c\theta^{ss'}\right) \right|$$

de même que les sommes incomplètes correspondantes. Ces estimations sont importantes dans divers contextes, comme, par exemple, les distributions de Diffie–Hellman en cryptography, les diviseurs premiers d'entiers à représentation « clairsemée », la distribution mod p de nombres de Mersenne ($M_q = 2^q - 1$ (q premier)). Cette méthode est très proche de celle de Bourgain et Konyagin (C. R. Acad. Sci. Paris, Ser. I 337 (2) (2003) 75–80). ***Pour citer cet article : J. Bourgain, C. R. Acad. Sci. Paris, Ser. I 338 (2004).***

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

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.03.027

Version française abrégée

Soit $\theta \in \mathbb{F}_p^*$ (p premier) d'ordre multiplicatif t. On démontre que pour tout $\delta > 0$, il existe $\delta' > 0$ tel que si $t \geqslant t_1 > p^\delta$, alors

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{1 \leqslant s \leqslant t_1} e_p\bigl(a\theta^s\bigr) \right| < c t_1 p^{-\delta'}. \tag{1}$$

On a également l'estimée sur les sommes doubles suivantes

$$\max_{(a,c,p)=1} \sum_{s'=1}^{t} \left| \sum_{s=1}^{t} e_p\bigl(a\theta^s + c\theta^{ss'}\bigr) \right| < c t^2 p^{-\delta'} \quad \text{si } t > p^\delta \tag{2}$$

et, plus généralement, les sommes incomplètes

$$\max_{(a,c,p)=1} \sum_{s'=1}^{t_1'} \left| \sum_{s=1}^{t_1} e_p\bigl(a\theta^s + c\theta^{ss'}\bigr) \right| < c t_1 t_1' p^{-\delta'} \quad \text{si } t \geqslant t_1,\ t_1' > p^\delta. \tag{3}$$

Des sommes exponentielles du type (1)–(3) apparaissent dans divers contextes : les distributions de Diffie–Hellman en cryptography (cf. [5,6]), la distribution de nombres de Mersenne (cf. [2]), les diviseurs premiers d'entiers à représentation « clairsemée » (cf. [8]). Les estimées (1), (2) permettent d'obtenir des résultats sous hypothèses moins restrictives sur l'ordre multiplicatif t de θ.

Les résultats de cette Note sont dans la même ligne que ceux obtenus dans [3] sur les sommes exponentielles associées à des sous-groupes multiplicatifs. Ils reposent sur la même approche, basée sur des estimées « sommes-produits » pour sous-ensembles de $\mathbb{F}_p$ (voir [4,1,7]) et des estimées sur des convolutions de mesures.

1. Sum-product and convolution estimates

It was proven in [3] that for all $\delta > 0$, there is $\delta' = \delta'(\delta) > 0$ such that if $A \subset \mathbb{F}_p$ (p prime), is an arbitrary set satisfying

$$p^\delta < |A| < p^{1-\delta} \tag{4}$$

then

$$|A + A| + |A \cdot A| > |A|^{1+\delta'}. \tag{5}$$

In [4], it was shown that for (5) to hold, only the assumption $|A| < p^{1-\delta}$ is needed. The main result from [4] are new bounds on exponential sums over subgroups $H \lhd \mathbb{F}_p^*$, of the form

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in H} e_p(ax) \right| < |H|^{1-\delta'}, \tag{6}$$

where we assume $|H| > p^\delta$, $\delta > 0$, an arbitrary fixed constant.

This estimate (6) was deduced from decay estimates on convolution powers

$$\nu^{(k)}(0), \quad \nu^{(k)} = \nu * \cdots * \nu (k\text{-fold}) \tag{7}$$

denoting ν the probability measure $\frac{1}{|H|} \sum_{x \in H} \delta_x$ on $\mathbb{F}_p$.

These decay estimates were indeed derived from the sum-product estimate (2) following a general scheme (involving Ruzsa's inequalities and the Balog–Szemeredi–Gowers theorem) going back to [1]. (This argument is by no means restricted to $\mathbb{F}_p$ and was in fact developed in [1] for set of real numbers.)

Theorems 1.1, 1.2 below provide this decay estimate in a slightly more general setting:

Theorem 1.1. *For all $Q \in \mathbb{Z}_+$, there is $\tau > 0$ and $k \in \mathbb{Z}_+$ with the following property.*
Let $H \subset \mathbb{F}_p^*$ (p prime) satisfy

$$|H \cdot H| < |H|^{1+\tau}. \tag{8}$$

Denote $\nu = \frac{1}{|H|} \sum_{x \in H} \delta_x$. Then

$$\max_{x \in R} \nu^{(k)}(x) < C_Q |H|^{-Q} + p^{-1+1/Q}, \tag{9}$$

hence

$$\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in H} e_p(ax) \right|^{2k} < |H|^{2k} \big(C_Q |H|^{-Q} + p^{-1+1/Q} \big). \tag{10}$$

We need a corresponding result for subsets H of $\mathbb{F}_p^* \times \mathbb{F}_p^*$. Since obviously no unconditional sum-product theorem holds for arbitrary subsets A of $\mathbb{F}_p \times \mathbb{F}_p$, some restrictions need to be made. The following statement is based on the fact that we do have a sum-product inequality, provided $A \subset \mathbb{F}_p \times \mathbb{F}_p$ and $|A| > p^{1+\varepsilon}$.

Theorem 1.2. *For all given $Q, Q' \in \mathbb{Z}_+$, there is $\tau > 0$ and $k \in \mathbb{Z}_+$ such that if $H \subset \mathbb{F}_p^* \times \mathbb{F}_p^*$ (p prime) satisfies*

$$|H \cdot H| < |H|^{1+\tau} \tag{11}$$

and $\nu = \frac{1}{|H|} \sum_{x \in H \cup (-H)} \delta_x$ satisfies

$$\nu^{(2Q)}(0) < p^{-1-1/Q'} \tag{12}$$

then

$$\nu^{(k)}(0) < p^{-2+1/Q}. \tag{13}$$

Equivalently, if (11) *and*

$$\#\big\{ (x_1, \ldots, x_{2Q}) \in H^{2Q} \,\big|\, x_1 + \cdots + x_Q = x_{Q+1} + \cdots + x_{2Q} \big\} < |H|^{2Q} p^{-1-1/Q'} \tag{14}$$

then

$$\sum_{a_1, a_2 = 0}^{p-1} \left| \sum_{x \in H} e_p(a_1 x_1 + a_2 x_2) \right|^{2k} < |H|^{2k} p^{1/Q}. \tag{15}$$

Remark 1. There is generalization to subsets H of $(\mathbb{F}_p^*)^r$, $r \geqslant 2$, satisfying (11), replacing condition (12) by $\nu^{(2Q)}(0) < p^{-r+1-1/Q'}$ and (13) by $\nu^{(k)}(0) < p^{-r+1/Q}$.

2. Exponential sum estimates

2.1. Subgroups

Consider a subgroup $H \lhd \mathbb{F}_p^*$. Theorem 1.1 implies for $k > k(Q)$

$$\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in H} e_p(ax) \right|^{2k} \lesssim |H|^{2k} \big(|H|^{-Q} + p^{-1+1/Q} \big). \tag{16}$$

Since $\sum_{x\in H} e_p(ax) = \sum_{x\in H} e_p(ax'x)$ for all $x' \in H$, (16) implies

$$\max_{a\in\mathbb{F}_p^*} \left|\sum_{x\in H} e_p(ax)\right| \lesssim |H| \left(p|H|^{-Q} + \frac{p^{1/Q}}{|H|}\right)^{1/(2k)}. \tag{17}$$

Assuming

$$|H| > p^{\rho} \tag{18}$$

for some $\rho > 0$ and taking $Q = [\frac{2}{\rho}]$, (17) implies

$$\max_{a\in\mathbb{F}_p^*} \left|\sum_{x\in H} e_p(ax)\right| \lesssim |H|^{1-1/(4k)} < |H|^{1-\rho'}, \tag{19}$$

where $\rho' = \rho'(\rho) > 0$. This is the estimate in [3] in which, moreover, an explicit expression for $\rho'(\rho)$ is given.

2.2. *Simple sums*

Take $\theta \in \mathbb{F}_p^*$ of multiplicative order t and $0 < t_1 \leqslant t$. Let

$$H = \{\theta^s \mid 0 \leqslant s \leqslant t_1\} \subset \mathbb{F}_p^*.$$

Clearly $|H \cdot H| \leqslant 2|H|$. We obtain again from (10)

Theorem 2.1. *Given $\delta > 0$, there is $\delta' > 0$ such that if $\theta \in \mathbb{F}_p^*$ is of multiplicative order t and $t \geqslant t_1 > p^{\delta}$, then*

$$\max_{a\in\mathbb{F}_p^*} \left|\sum_{s=1}^{t_1} e_p(a\theta^s)\right| < t_1 p^{-\delta'}. \tag{20}$$

2.3. *Multiple sums*

Consider the expressions (cf. [5])

$$W_{a,c}(t) = \sum_{s'=1}^{t} \left|\sum_{s=1}^{t} e_p(a\theta^s + c\theta^{ss'})\right| \tag{21}$$

($\theta \in \mathbb{F}_p^*$ of multiplicative order t), which are obvious bounds on the 'Diffie–Hellman' sums

$$\sum_{s,s'=1}^{t} e_p(a\theta^s + b\theta^{s'} + c\theta^{ss'}). \tag{22}$$

Theorem 2.2. *For all $\delta > 0$, there is $\delta' > 0$ such that if $t > p^{\delta}$, then*

$$\max_{(a,c,p)=1} W_{a,c}(t) < ct^2 p^{-\delta'} \tag{23}$$

(*where c is a constant*).

In [5], this estimate was obtained under the assumption $t > p^{3/4+\delta}$.
The relevant subset (subgroup) in the proof of Theorem 2.2 is

$$H = H_{s'} = \{(\theta^s, \theta^{s's}) \mid s = 1, \dots, t\}.$$

In order to apply Theorem 1.2 and proceed as above, condition (14) needs to be verified (for some Q'). This is achieved for most values of $s' = 1, \dots, t$ (exploiting the double summation).

Similar arguments permit us to obtain non-trivial bounds on incomplete sums and generalizations. One may in particular prove:

Theorem 2.3. *Let $\theta \in \mathbb{F}_p^*$ be of multiplicative order t and $t \geqslant t_1, t_1' > p^\delta$ ($\delta > 0$ arbitrary and fixed). Then*

$$\sum_{s'=1}^{t_1'} \max_{(a,c,p)=1} \left| \sum_{s=1}^{t_1} e_p\bigl(a\theta^s + c\theta^{ss'}\bigr) \right| < ct_1 t_1' p^{-\delta'} \tag{24}$$

with $\delta' = \delta'(\delta) > 0$.

Theorem 2.4. *Let θ be as above, $\ell \in \mathbb{Z}_+$ an integer. Given $\delta > 0$, there is $\delta' > 0$ such that if $t \geqslant t_0, t_1, \dots, t_\ell > p^\delta$, then*

$$\sum_{s_1=1}^{t_1} \cdots \sum_{s_\ell=1}^{t_\ell} \max_{(a,a_1,\dots,a_\ell,p)=1} \left| \sum_{s=1}^{t_0} e_p\bigl(a\theta^s + a_1\theta^{s_1 s} + \cdots + a_\ell \theta^{s_\ell s}\bigr) \right| < ct_0 t_1 \cdots t_\ell p^{-\delta'}. \tag{25}$$

3. Applications

Eq. (23) provides non-trivial bounds on the sums (22) of relevance to the Diffie–Hellman distributions in cryptography (see in particular [5] and [6] and further references in these papers).

From the preceding, the uniform distribution (DHI) of

$$\bigl\{\bigl(\theta^s, \theta^{s'}, \theta^{ss'}\bigr) \bigm| 1 \leqslant s, s' \leqslant t\bigr\} \subset \mathbb{F}_p^3 \tag{26}$$

may indeed be established as soon as θ is of multiplicative order t modulo p with $t > p^\delta$, for any $\delta > 0$. In [5], the (DHI) assumption was verified for $t > p^{3/4+\delta}$.

Remark 2. If we fix an integer θ, then its multiplicative order t modulo p satisfies $t > p^{1/2-\varepsilon}$ for most primes p (see [1] for references).

One may also combine the estimate (23) with Vaughan's general estimate of $\sum_{n \leqslant N} \Lambda(n) f(n)$ with $\Lambda(n)$ the von Mangoldt function, as done in [1]. Along these lines, one may prove

Theorem 3.1. *Given $\delta > 0$, there is $\delta' > 0$ such that if $\theta \in \mathbb{F}_p^*$ is of multiplicative order $t > p^\delta$ and $N > t^{2+\delta}$, then*

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{n=1}^{N} \Lambda(n) e_p\bigl(a\theta^n\bigr) \right| < Np^{-\delta'} \tag{27}$$

and hence

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{\substack{q \leqslant N \\ q \text{ prime}}} e_p\bigl(a\theta^q\bigr) \right| < Np^{-\delta'}. \tag{28}$$

From (28) we obtain in particular equidistribution properties mod p of the Mersenne numbers $M_q = 2^q - 1$ (q prime).

Finally, Konyagin [7] pointed out the recent paper [8] to the author, dealing with prime divisors of ‘sparse integers’.

Let $g \geqslant 2$ and $s \geqslant 1$ be two integers and $\mathcal{D} = \{d_i\}_{i=0}^{s}$ a sequence of $s+1$ nonzero integers. Following [8], denote $\mathcal{S}_{g,s}(\mathcal{D})$ the set of all integers n of the form

$$n = d_0 + d_1 g^{m_1} + \cdots + d_s g^{m_s}. \tag{29}$$

Combining our Theorem 2.1 with the argument from [8], we may improve Theorem 6 from [8] as follows:

Corollary 3.2. *Given any $\delta > 0$, there is $s(\delta)$ such that if $s > s(\delta)$ and X is sufficiently large, for $(1 + \mathrm{o}(1))\pi(X)$ primes $p \leqslant X$, there exists $n \in \mathcal{S}_{g,s}(\mathcal{D})$ such that $\log n < X^{\delta}$ and $p|n$.*

This result was obtained in [8] for $\delta > \frac{1}{2}$.

References

[1] W.D. Banks, A. Conflitti, J.B. Friedlander, I.E. Shparlinski, Exponential sums over Mersenne numbers, Compositio Math. 140 (1) (2004) 15–30.
[2] J. Bourgain, On the Erdös–Volkmann and Katz–Tao ring conjectures, Geom. Funct. Anal. 13 (2) (2003) 334–365.
[3] J. Bourgain, N. Katz, T. Tao, A sum-product theorem in finite fields and applications, Geom. Funct. Anal., in press.
[4] J. Bourgain, S.V. Konyagin, Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order, C. R. Math. Acad. Sci. Paris, Ser. I 337 (2) (2003) 75–80.
[5] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, I. Shparlinski, On the statistical properties of Diffie–Hellman distributions, Israel J. Math. A 120 (2000) 23–46.
[6] J.B. Friedlander, S. Konyagin, I.E. Shparlinski, Some doubly exponential sums over $\mathbb{Z}_m$, Acta Arith. 105 (4) (2002) 349–370.
[7] S. Konyagin, Private communications.
[8] I. Shparlinski, Prime divisors of sparse integers, Period. Math. Hungar. 96 (N2) (2003) 215–222.