Available online at www.sciencedirect.com
SCIENCE DIRECT
C. R. Acad. Sci. Paris, Ser. I 339 (2004) 321–325
COMPTES RENDUS MATHEMATIQUE

Number Theory

Mordell type exponential sum estimates in fields of prime order

Jean Bourgain

IAS, School of Mathematics, Princeton, NJ 08540, USA

Received 29 May 2004; accepted 1 June 2004

Available online 6 August 2004

Presented by Jean Bourgain

Abstract

We establish a Mordell type exponential sum estimate (see Mordell [Q. J. Math. 3 (1932) 161–162]) for 'sparse' polynomials $f(x)=\sum_{i=1}^{r} a_i x^{k_i}$, $(a_i, p)=1$, p prime, under essentially optimal conditions on the exponents $1 \leqslant k_i < p-1$. The method is based on sum–product estimates in finite fields $\mathbb{F}_p$ and their Cartesian products. We also obtain estimates on incomplete sums of the form $\sum_{s=1}^{t} e_p(\sum_{i=1}^{r} a_i \theta_i^s)$ for $t > p^{\varepsilon}$, under appropriate conditions on the $\theta_i \in \mathbb{F}_p^*$. ***To cite this article: J. Bourgain, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Résumé

Estimations de type Mordell pour les sommes exponentielles dans les corps d'ordre premier. Nous démontrons une estimée du type Mordell (voir Mordell [Q. J. Math. 3 (1932) 161–162]) pour les sommes exponentielles associées à des polynômes clairsemés $f(x)=\sum_{i=1}^{r} a_i x^{k_i}$, $(a_i, p)=1$, p premier, sous des hypothèses essentiellement optimales sur les exposants $1 \leqslant k_i < p-1$. La méthode repose sur des estimés « sommes-produits » dans des corps finis $\mathbb{F}_p$ et leurs produits cartésiens. On obtient également des bornes non-triviales sur des sommes incomplètes de la forme $\sum_{s=1}^{t} e_p(\sum_{i=1}^{r} a_i \theta_i^s)$ pour $t > p^{\varepsilon}$, sous des hypothèses appropriées sur les $\theta_i \in \mathbb{F}_p^*$. ***Pour citer cet article : J. Bourgain, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Version française abrégée

Soit p un nombre premier et $f(x)=\sum_{i=1}^{r} a_i x^{k_i} \in \mathbb{Z}[X]$, $(a_i, p)=1$ et $1 \leqslant k_i < p-1$ tel que $(k_i, p-1) < p^{1-\varepsilon}$ et $(k_i - k_j, p-1) < p^{1-\varepsilon}$ pour tout $1 \leqslant i \neq j \leqslant r$, où $\varepsilon > 0$ est arbitrairement petit et fixé. On a alors une borne sur la somme exponentielle

$$\left|\sum_{x=1}^{p-1} e_p\big(f(x)\big)\right| < Cp^{1-\delta}$$

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

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

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.06.013

Le résultat généralise à des polynomes « clairsemés » l'estimé sur les sommes de Gauss obtenue dans [2]. La méthode utilisée est semblable à celle de [2], et consiste à établir un théorème « sommes-produits » pour des sous-ensembles A de $\mathbb{F}_p \times \mathbb{F}_p$ (ceci nous permet de traiter le cas où $f(x)$ est un binôme, donc $r = 2$, ce qui suffit pour obtenir le cas général).

Une approche analogue s'applique aux sommes incomplètes de la forme $\sum_{s=1}^{t} e_p(\sum_{i=1}^{r} a_i \theta_i^s)$, où $t > p^\varepsilon$ et $\theta_i \in \mathbb{F}_p^*$ satisfont $0(\theta_i) > p^\varepsilon$ et $0(\theta_i \theta_j^{-1}) > p^\varepsilon$ pour tous $1 \leqslant i \neq j \leqslant r$ (on dénote ici $0(\psi)$ l'ordre multiplicatif de $\psi \in \mathbb{F}_p^*$). On démontre une estimée

$$\max_{(a_i,\dots,a_r,p)=1} \left| \sum_{s=1}^{t} e_p\left(\sum_{i=1}^{r} a_i \theta_i^s\right) \right| < Ctp^{-\delta}$$

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

Le cas $r = 1$ fut traité dans [1]. Ce genre de sommes interviennent en cryptographie, en particulier dans le contexte, des distributions de Diffie–Hellman (voir [6] par exemple).

1. A Mordell type estimate

The main result of this paper is the following:

Theorem 1.1. *Let p be prime. Given $r \in \mathbb{Z}_+$ and $\varepsilon > 0$, there is $\delta = \delta(r, \varepsilon) > 0$ satisfying the following property: If*

$$f(x) = \sum_{i=1}^{r} a_i x^{k_i} \in \mathbb{Z}[x] \quad \text{and} \quad (a_i, p) = 1,$$

where the exponents $1 \leqslant k_i < p - 1$ satisfy

$$(k_i, p-1) < p^{1-\varepsilon} \quad \text{for all } 1 \leqslant i \leqslant r, \tag{1}$$

$$(k_i - k_j, p-1) < p^{1-\varepsilon} \quad \text{for all } 1 \leqslant i \neq j \leqslant r \tag{2}$$

then there is an exponential sum estimate

$$\left| \sum_{x=1}^{p-1} e_p\big(f(x)\big) \right| < p^{1-\delta} \tag{3}$$

(*denoting $e_p(y) = \mathrm{e}^{2\pi \mathrm{i} y/p}$*).

Remark 1. The result for $r = 1$ (Gauss sums) was obtained in [2]. Thus

$$\left| \sum_{x=1}^{p-1} e_p(ax^k) \right| < p^{1-\delta} \quad \text{if } a \in \mathbb{F}_p^* \text{ and } (k, p-1) < p^{1-\varepsilon}. \tag{4}$$

More precisely, it was shown in [2] that if $G \lhd \mathbb{F}_p^*$ and $|G| > p^\varepsilon$, then

$$\left| \sum_{x \in G} e_p(ax) \right| < |G|^{1-\delta} \quad \text{for } a \in \mathbb{F}_p^*. \tag{5}$$

See also [1] for further extensions to exponential sums of the form

$$\sum_{s=1}^{t_1} e_p(a\theta^s) \tag{6}$$

and

$$\sum_{s,s'=1}^{t_1} e_p(a\theta^s + b\theta^{ss'}),\tag{7}$$

where $a, \theta \in \mathbb{F}_p^*$ and θ of multiplicative order t, $t \geqslant t_1 > p^\delta$.

The methods involved here are closely related to those used in [2] and [1] (while the results in [6] and [5] depend on Stepanov's method).

Remark 2. Theorem 1.1 stated above improves upon the results from [4] and [5] when the exponents $\{k_i\}$ are large. Notice that the recent paper [4] already contains a substantial improvement over Mordell's original paper [7].

Remark 3. The role of condition (2) above is made clear by the following example from [4] (see Example 1.1). Let r be even and

$$f(x) = \sum_{i=1}^{r/2} (x^{(p-1)/2+i} - x^i).\tag{8}$$

Then

$$\left| \sum_{x=1}^{p-1} e_p\big(f(x)\big) - \frac{p-1}{2} \right| \leqslant r\sqrt{p}.\tag{9}$$

2. The Role of sum–product estimates

As mentioned above, our argument follows the same pattern as in [2] and [1]. The key combinatorial ingredient in [2] is a 'sum–product' theorem for subsets A of the field $\mathbb{F}_p$ (see also [3]).

Proposition 2.1. *Given $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$ and*

$$1 < |A| < p^{1-\varepsilon}\tag{10}$$

then

$$|A + A| + |A \cdot A| > C|A|^{1+\delta}.\tag{11}$$

We denote here $A + A = \{x + y \mid x, y \in A\}$ and $A \cdot A = \{x \cdot y \mid x, y \in A\}$ the sum and product set (and will use the same notations if, more generally, A is a subset of a commutative ring $\mathcal{R}$).

Given $G \lhd \mathbb{F}_p^*$ consider the probability measure ν on $\mathbb{F}_p$ defined by

$$\nu = \frac{1}{|G|} \sum_{x \in G} \delta_x.\tag{12}$$

As shown in [2], one may then derive from Proposition 2.1 uniform bounds on the convolution powers

$$\nu^{(k)} = \underbrace{\nu * \cdots * \nu}_{k\text{-fold}}$$

denoting

$$(\nu * \mu)(x) = \sum_{y \in \mathbb{F}_p} \nu(x-y)\mu(y)$$

and those bounds translate in exponential sum estimates such as (5).

It turns out that in order to establish Theorem 1.1 for general r, it suffices to treat the monomial $(r=1)$ and the binomial case $(r=2)$. Thus we are left with the problem for $r=2$. Following the scheme used for $r=1$, we need to establish a sum–product theorem for subsets A of the product $\mathbb{F}_p\times\mathbb{F}_p$. Clearly if A is a subset of the form

$$A=\{a\}\times\mathbb{F}_p,\quad A=\mathbb{F}_p\times\{a\}\quad\text{or}\quad A=\big\{(x,ax)\mid x\in\mathbb{F}_p\big\}$$

one has $|A|=|A+A|=|A\cdot A|=p$. It turns out that these are essentially the only 'exceptions' to be taken into account when reformulating Proposition 2.1 for $\mathbb{F}_p\times\mathbb{F}_p$.

Proposition 2.2. *Let $A\subset\mathbb{F}_p\times\mathbb{F}_p$ satisfying for some $\varepsilon_0>0$*

$$|A|>p^{\varepsilon_0}. \tag{13}$$

Assume that

$$|A+A|+|A\cdot A|<p^{\varepsilon}|A|. \tag{14}$$

Then one of the following cases occurs:

(i) $$|A|>p^{2-\varepsilon'}. \tag{15}$$

(ii) *There is $a\in\mathbb{F}_p$ such that either*

$$\big|A\cap\big(\{a\}\times\mathbb{F}_p\big)\big|>p^{-\varepsilon'}|A|$$

or

$$\big|A\cap\big(\mathbb{F}_p\times\{a\}\big)\big|>p^{-\varepsilon'}|A|.$$

(iii) *There is $a\in\mathbb{F}_p^*$ such that*

$$\big|A\cap\big\{(x,ax)\mid x\in\mathbb{F}_p\big\}\big|>p^{-\varepsilon'}|A|,$$

where $\varepsilon'=\varepsilon'(\varepsilon)\to 0$ for $\varepsilon\to 0$ with ε_0 in (13) *fixed.*

Moreover, in cases (ii), (iii)

$$p^{1-\varepsilon'}<|A|<p^{1+\varepsilon'}. \tag{16}$$

3. Exponential sums associated to power residues

Theorem 1.1 has the following reformulation.

For $\theta\in\mathbb{F}_p^*$, denote $0(\theta)$ the multiplicative order of θ in $\mathbb{F}_p^*$.

Corollary 3.1. *Let $\theta_1,\dots,\theta_r\in\mathbb{F}_p^*$ satisfy for some $\varepsilon>0$*

$$0(\theta_i)>p^{\varepsilon}\quad\textit{for all } i=1,\dots,r, \tag{17}$$

$$0(\theta_i\theta_j^{-1})>p^{\varepsilon}\quad\textit{for all } 1\leqslant i\neq j\leqslant r. \tag{18}$$

Then

$$\max_{a_i\in\mathbb{F}_p^*}\left|\sum_{s=1}^{p-1}e_p\left(\sum_{i=1}^{r}a_i\theta_i^s\right)\right|<p^{1-\delta} \tag{19}$$

with $\delta=\delta_r(\varepsilon)$.

Indeed, let ψ be a generator of $\mathbb{F}_p^*$ and write $\theta_i = \psi^{k_i}$, where thus

$$0(\theta_i) = \frac{p-1}{(p-1, k_i)}, \tag{20}$$

$$0(\theta_i \theta_j^{-1}) = \frac{p-1}{(p-1, k_i - k_j)}. \tag{21}$$

Clearly

$$\sum_{s=1}^{p-1} e_p\left(\sum_{i=1}^{r} a_i \psi^{s k_i}\right) = \sum_{x \in \mathbb{F}_p^*} e_p\left(\sum_{i=1}^{r} a_i x^{k_i}\right).$$

Since (17), (18), (20), and (21) ensure conditions (1), (2) on the exponents k_i, (19) is equivalent to (3).

The corollary remains valid for incomplete sums (the case $r = 1$ appears in [1]).

Theorem 3.2. *Let $\varepsilon > 0$ and $\theta_1, \ldots, \theta_r \in \mathbb{F}_p^*$ satisfy* (17), (18)*. Then for $t > p^{\varepsilon}$*

$$\max_{a_i \in \mathbb{F}_p^*} \left| \sum_{s=1}^{t} e_p\left(\sum_{i=1}^{r} a_i \theta_i^s\right) \right| < p^{-\delta} t, \tag{22}$$

where $\delta = \delta(\varepsilon)$.

References

[1] J. Bourgain, Estimates on exponential sums related to the Diffie–Hellman distributions, GAFA, in press.

[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, N. Katz, T. Tao, A sum–product theorem in finite fields and applications, GAFA, in press.

[4] T. Cochrane, C. Pinner, An improved Mordell type bound for exponential sums, Proc. Amer. Math. Soc., submitted for publication.

[5] T. Cochrane, C. Pinner, Stepanov's method applied to binomial exponential sums, Q. J. Math. 54 (3) (2003) 243–255.

[6] S. Konyagin, I. Shparlinski, Character Sums with Exponential Functions and their Applications, Cambridge University Press, Cambridge, 1999.

[7] L.J. Mordell, On a sum analogous to a Gauss' sum, Q. J. Math. 3 (1932) 161–162.