Available online at www.sciencedirect.com
SCIENCE DIRECT
C. R. Acad. Sci. Paris, Ser. I 342 (2006) 643–646
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory/Mathematical Analysis

A Gauss sum estimate in arbitrary finite fields

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

[a] *Institute for Advanced Study, Olden Lane, Princeton, NJ 08540, USA*
[b] *Mathematics Department, University of California, Riverside, CA 92521, USA*

Received 7 September 2005; accepted after revision 23 January 2006

Available online 29 March 2006

Presented by Jean Bourgain

Abstract

We establish bounds on exponential sums $\sum_{x\in\mathbb{F}_q}\psi(x^n)$ where $q=p^m$, p prime, and ψ an additive character on $\mathbb{F}_q$. They extend the earlier work of Bourgain, Glibichuk, and Konyagin to fields that are not of prime order ($m\geqslant 2$). More precisely, a non-trivial estimate is obtained provided n satisfies $\gcd(n,\frac{q-1}{p^\nu-1})<p^{-\nu}q^{1-\varepsilon}$ for all $1\leqslant\nu<m$, $\nu|m$, where $\varepsilon>0$ is arbitrary. ***To cite this article: J. Bourgain, M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Résumé

Une estimée des sommes de Gauss dans des corps finis arbitraires. On etabli des bornes sur les sommes d'exponentielles $\sum_{x\in\mathbb{F}_q}\psi(x^n)$ où $q=p^m$, p est premier et ψ est un caractère additif de $\mathbb{F}_q$. Il s'agit d'une extension des résultats de Bourgain, Glibichuk, et Konyagin pour un corps qui n'est pas d'ordre premier, c'est-à-dire $m\geqslant 2$. On obtient une estimée non-triviale pour tout n satisfaisant la condition $\mathrm{pgcd}(n,\frac{q-1}{p^\nu-1})<p^{-\nu}q^{1-\varepsilon}$ pour tout $1\leqslant\nu<m$, $\nu|m$ et où $\varepsilon>0$ est arbitraire. ***Pour citer cet article : J. Bourgain, M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Version française abrégée

Dans cette Note nous démontrons une extension des résultats obtenus dans [2] pour des sommes de Gauss $\sum_{x\in\mathbb{F}_q}\psi(x^n)$ et plus generalement $\sum_{j=1}^{t_1}\psi(g^j)$, où ψ est un caractère additif de $\mathbb{F}_q$, $g\in\mathbb{F}_q^*$ d'ordre multiplicatif $t\geqslant t_1$. Les résultats de [2] traitent le cas où $q=p$ est premier alors qu'ici on considère le cas général $q=p^m$. En usant de la même approche basée sur des propriétés combinatoires des ensembles « sommes » et « produits », nous établissons des estimées non-triviales sous des hypothèses très faibles (et essentiellement optimales). Si n satisfait la condition

$$\mathrm{pgcd}\left(n,\frac{q-1}{p^\nu-1}\right)<p^{-\nu}q^{1-\varepsilon}\quad\text{pour tout } 1\leqslant\nu<m,\ \nu|m$$

E-mail addresses: bourgain@math.ias.edu (J. Bourgain), mcc@math.ucr.edu (M.-C. Chang).

1631-073X/$ – see front matter © 2006 Académie des sciences. Published by Elsevier SAS. All rights reserved.
doi:10.1016/j.crma.2006.01.022

où $\varepsilon > 0$ est fixé et arbitraire, on a l'estimée

$$\Big|\sum_{x\in\mathbb{F}_q}\psi\big(x^n\big)\Big| < cq^{1-\delta}$$

pour tout caractère additif non-trivial ψ de $\mathbb{F}_q$ et où $\delta = \delta(\varepsilon) > 0$.

1.

Denote $q = p^m$ with p prime, $m \in \mathbb{Z}$, $m \geqslant 1$.

Non-trivial subfields of $\mathbb{F}_q$ are of size p^ν where $1 \leqslant \nu < m$, $\nu|m$. Denote $\operatorname{Tr}(x) = x + x^p + \cdots + x^{p^{m-1}}$ the trace of $x \in \mathbb{F}_q$.

Let $\psi(x) = e_p(\operatorname{Tr}(\xi x))$, $\xi \in \mathbb{F}_q^*$ be a non-trivial additive character of $\mathbb{F}_q$. Our aim is to extend certain estimates on exponential sums of the type

$$\sum_{x\in\mathbb{F}_q}\psi\big(x^n\big) \tag{1}$$

and

$$\sum_{j\leqslant t_1}\psi\big(g^j\big), \quad t_1 \leqslant t = \operatorname{ord}(g) \tag{2}$$

obtained in [2] for prime fields ($m = 1$) to the general case ($m \geqslant 2$) (in (2), we denoted $\operatorname{ord}(g)$ the multiplicative order of $g \in \mathbb{F}_q^*$).

More precisely, it was shown in [2] that if $q = p$ and $\gcd(n, p-1) < p^{1-\varepsilon}$ ($\varepsilon > 0$ arbitrary) in (1) (resp. $t \geqslant t_1 > p^\varepsilon$ in (9)), then $|\sum_{x\in\mathbb{F}_q}\psi(x^n)| < p^{1-\delta}$ (resp. $|\sum_{j\leqslant t_1}\psi(g^j)| < t_1 p^{-\delta}$), where $\delta = \delta(\varepsilon) > 0$.

The method involved in [2] as well as here is the 'sum-product' approach, which permits us to establish non-trivial bounds in certain situations where 'classical' methods such as Stepanov's do not seem to apply (see [4] for details).

Our main results are the following:

Theorem 1. *Assume in* (1) *that* $n|(p^m-1)$ *and satisfies the condition*

$$\gcd\left(n, \frac{p^m-1}{p^\nu-1}\right) < p^{-\nu}q^{1-\varepsilon} \quad \textit{for all } 1 \leqslant \nu < m, \nu|m \tag{3}$$

where $\varepsilon > 0$ *is arbitrary and fixed. Then*

$$\max_{a\in\mathbb{F}_q^*}\Big|\sum_{x\in\mathbb{F}_q}\psi\big(ax^n\big)\Big| < cq^{1-\delta} \tag{4}$$

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

Theorem 2. *Assume in* (2) *that* $g \in \mathbb{F}_q^*$ *and*

$$t \geqslant t_1 > q^\varepsilon \quad \textit{and} \quad \max_{\substack{1\leqslant\nu<m\\ \nu|m}}\gcd\big(p^\nu-1, t\big) < q^{-\varepsilon}t \tag{5}$$

for some $\varepsilon > 0$. *Then again*

$$\max_{a\in\mathbb{F}_q^*}\Big|\sum_{j\leqslant t_1}\psi\big(ag^j\big)\Big| < cq^{-\delta}t_1 \tag{6}$$

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

Remark. The classical bound

$$\Big|\sum_{x\in\mathbb{F}_q}\psi\big(x^n\big)\Big| \leqslant (n-1)q^{1/2} \tag{7}$$

becomes trivial for $n > q^{1/2}$. The first non-trivial estimate when $n > q^{1/2}$ was obtained in [5], considering values of n up to $p^{1/6}q^{1/2}$. Condition (3) (and similarly (5)) has clearly to do with the presence of non-trivial subfields of $\mathbb{F}_q$, which we do not want to contain most of the multiplicative group $\{x^n \mid x \in \mathbb{F}_q^*\}$ (and $\{g^j \mid j \leqslant t\}$ resp.). A condition of this form is obviously needed.

2.

As pointed out earlier, we rely on the same approach as in [2]. The proof of Theorem 2 (which implies Theorem 1) will be based on the following two results:

Proposition 3. *Let $A \subset \mathbb{F}_q$ and $|A| > q^{\varepsilon}$. Let $\varepsilon > \kappa > 0$ and assume*

$$\bigl|A \cap (\eta + S)\bigr| < q^{-\kappa}|A| \tag{8}$$

whenever $\eta \in \mathbb{F}_q$ and $S \subset \mathbb{F}_q$ satisfies the condition

$$|S| < q^{1-\varepsilon/20} \tag{9}$$

and

$$|S + S| + |S.S| < q^{\kappa}|S|. \tag{10}$$

Then for some $k = k(\kappa) \in \mathbb{Z}_+$ and $\delta = \delta(\kappa) > 0$

$$\max_{a\in\mathbb{F}_q^*}\left|\sum_{x_1,\dots,x_k\in A}\psi(ax_1\cdots x_k)\right| < q^{-\delta}|A|^k. \tag{11}$$

In (10), we denoted $S + S = \{x + y\colon x, y \in S\}$ (resp. $S.S = \{x.y\colon x, y \in S\}$) the sum-set (resp. the product-set). For small $\kappa > 0$, condition (10) expresses the property that both $S + S$ and $S.S$ are not much larger than S. Hence it is important to understand the structure of such sets.

The next result provides the required information:

Proposition 4. *Assume $S \subset \mathbb{F}_q$, $|S| > q^{\delta}$ and $|S + S| + |S.S| < K|S|$. Then there is a subfield G of $\mathbb{F}_q$ and $\xi \in \mathbb{F}_q^*$ such that*

$$|G| < K^C|S| \tag{12}$$

and

$$|S\backslash\xi G| < K^C \tag{13}$$

where $C = C(\delta)$.

Proposition 3 is essentially Theorem 3.1 in [1]. The only difference is that in [1] we consider subsets of a ring $R = \prod \mathbb{Z}_{g_j}$ instead of a field $\mathbb{F}_q$; but the essentially general argument carries over verbatim to the present situation (in fact it simplifies since the set $R\backslash R^*$ of non-invertible elements is trivial here). The proof of Theorem 3.1 in [1] uses only the additive Fourier transform.

We may again identify the set of additive characters of $\mathbb{F}_q$ with $\mathbb{F}_q$, letting

$$\psi(x) = e_p\bigl(\mathrm{Tr}(\xi x)\bigr); \quad e_p(y) = \mathrm{e}^{2\pi \mathrm{i} y/p}$$

where ξ ranges in $\mathbb{F}_q$.

Proposition 4 appears in [3], as a byproduct of the proof of the sum-product theorem in prime fields.

3.

With Propositions 3 and 4 at hand, the proof of Theorem 2 is rather straightforward. For simplicity, take $t_1 = t$ (considering the complete sum), in which case $A = \{g^j\colon 0 \leqslant j < t\}$ is a multiplicative subgroup of $\mathbb{F}_q^*$. Assuming A satisfies conditions (8)–(10) from Proposition 3, the conclusion (11) is then simply

$$\max_{a\in\mathbb{F}_q^*}\left|\sum_{x\in A}\psi(ax)\right| < q^{-\delta}|A| \tag{14}$$

which is (6).

(To treat incomplete sums, i.e. $t_1 < t$, some minor additional technicalities are involved.)

Assume that for some η one has

$$\left|A \cap (\eta + S)\right| \geqslant q^{-\kappa}|A| \tag{15}$$

with S satisfying (9), (10). Thus $|S| > tq^{-\kappa} > q^{\varepsilon-\kappa} > q^{\varepsilon/2}$ if $\kappa < \frac{\varepsilon}{2}$.

Apply Proposition 4 to the set S with $\delta = \frac{\varepsilon}{2}$, $K = q^{\kappa}$.

The subfield G satisfies by (12) and (9)

$$|G| < q^{\kappa C}|S| < q^{1-\varepsilon/20+\kappa C(\varepsilon)} < q$$

taking κ small enough. Hence G is non-trivial and

$$|G| = p^{\nu} \quad \text{for some } \nu < m,\ \nu|m. \tag{16}$$

From (13) and (15)

$$\left|A \cap (\eta + \xi G)\right| > q^{-\kappa}|A| - q^{\kappa C(\varepsilon)} > \frac{1}{2}q^{-\kappa}|A| \tag{17}$$

implying that

$$\left|\left\{(s, s')\colon\ 0 \leqslant s, s' \leqslant t-1,\ g^{s} - g^{s'} \in \xi G\right\}\right| > \frac{1}{4}q^{-2\kappa}t^{2}. \tag{18}$$

Equivalently, we may write

$$\left|\left\{(s, s')\colon\ 0 \leqslant s, s' \leqslant t-1,\ g^{s} - g^{s'+s} \in \xi G\right\}\right| > \frac{1}{4}q^{-2\kappa}t^{2}.$$

In particular there exist some $s' \neq 0$ such that denoting $\xi_1 = \xi(1 - g^{s'})^{-1}$

$$\left|\left\{s\colon\ 0 \leqslant s \leqslant t-1,\ g^{s} \in \xi_1 G\right\}\right| \gtrsim q^{-2\kappa}t. \tag{19}$$

Let $g = g_0^{(q-1)/t}$, where g_0 is a generator of $\mathbb{F}_q^*$. Since by (16) $x^{p^{\nu}-1} = 1$ for all $x \in G^*$, it follows from (19) that

$$\left|\left\{s\colon\ 0 \leqslant s \leqslant t-1,\ g_0^{\frac{q-1}{t}(p^{\nu}-1)s} = \xi_1^{p^{\nu}-1}\right\}\right| \gtrsim q^{-2\kappa}t.$$

Therefore there is some $0 < s \lesssim q^{2\kappa}$ such that $g_0^{\frac{q-1}{t}(p^{\nu}-1)s} = 1$, or equivalently $t|s(p^{\nu}-1)$. But then $\gcd(t, p^{\nu}-1) > q^{-2\kappa}t$, violating assumption (5).

References

[1] J. Bourgain, M.-C. Chang, Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few factors, GAFA, in press.

[2] J. Bourgain, A. Glibichuk, S. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, J. London Math. Soc., in press.

[3] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields and their applications, GAFA 14 (1) (2004) 27–57.

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

[5] I. Shparlinski, Bounds on Gauss sums in finite fields, Proc. Amer. Math. Soc. 132 (10) (2006) 2817–2824.