

BOUNDS ON EXPONENTIAL SUMS OVER SMALL MULTIPLICATIVE SUBGROUPS

PÄR KURLBERG

ABSTRACT. We show that there is significant cancellation in certain exponential sums over small multiplicative subgroups of finite fields, giving an exposition of the arguments by Bourgain and Chang [6].

1. INTRODUCTION

Let $\psi : \mathbb{F}_p \rightarrow \mathbb{C}$ be any non-trivial additive character in \mathbb{F}_p (that is, $\psi(x) = \exp\left(\frac{2\pi i x \xi}{p}\right)$ for all $x \in \mathbb{F}_p$, for some $\xi \in \mathbb{F}_p^\times$), and let H be a subset of \mathbb{F}_p . We are interested in obtaining good upper bounds for

$$\left| \sum_{x \in H} \psi(x) \right|;$$

that is, significantly smaller than $|H|$. A traditional analytic number theory approach when H is the multiplicative subgroup of \mathbb{F}_p of index m is to “complete the sum”: We have

$$\frac{1}{m} \sum_{\substack{\chi \pmod{p} \\ \chi^m = \chi_0}} \chi(n) = \begin{cases} 1 & \text{if } n \in H, \\ 0 & \text{otherwise;} \end{cases}$$

where the sum runs through the Dirichlet characters \pmod{p} with order dividing m . Therefore

$$\sum_{x \in H} \psi(x) = \sum_{n \in \mathbb{F}_p} \psi(n) \frac{1}{m} \sum_{\substack{\chi \pmod{p} \\ \chi^m = \chi_0}} \chi(n) = \frac{1}{m} \sum_{\substack{\chi \pmod{p} \\ \chi^m = \chi_0}} \sum_{n \in \mathbb{F}_p} \psi(n) \chi(n).$$

The last sum, $\sum_{n \in \mathbb{F}_p} \psi(n) \chi(n)$, is a Gauss sum when $\chi \neq \chi_0$ and is known to have absolute value \sqrt{p} ; and $\sum_{n \in \mathbb{F}_p} \psi(n) \chi_0(n) = -1$. We deduce that

$$\left| \sum_{x \in H} \psi(x) \right| < \sqrt{p}.$$

This is non-trivial when H has substantially more than $p^{1/2}$ elements and classical arguments can sometimes give non-trivial bounds for interesting

Date: May 20, 2007.

The author was partially supported by grants from the Göran Gustafsson Foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council.

sets H as small as $p^{1/4}$, but not much smaller. For H a multiplicative subgroup, the first bound of the form $\sum_{x \in H} \psi(x) \ll_{\delta} p^{-\delta}|H|$ with $\delta > 0$ and for $|H|$ significantly smaller than $p^{1/2}$ was obtained when $|H| \gg_{\epsilon} p^{3/7+\epsilon}$ (for all $\epsilon > 0$) by Shparlinski [14], and later refined to $|H| \gg_{\epsilon} p^{3/8+\epsilon}$ by Konyagin and Shparlinski (unpublished), for $|H| \gg_{\epsilon} p^{1/3+\epsilon}$ by Heath-Brown and Konyagin [12], and for $|H| \gg_{\epsilon} p^{1/4+\epsilon}$ by Konyagin [13]. An essential ingredient in these results are upper bounds on the number of \mathbb{F}_p -points on certain curves/varieties that significantly go beyond what the Weil bounds give.

In several recent articles Bourgain along with Chang, Glibichuk, and, Konyagin showed how to get non-trivial upper bounds for various interesting H that are much smaller, using completely different methods — the techniques of additive combinatorics. The aim of this note is to give an exposition of these ideas in the simplest case¹ by showing that there is significant cancellation in such exponential sums over small multiplicative subgroups H of the finite field \mathbb{F}_p .

Theorem 1.1. *Given $\alpha > 0$, there exists $\beta = \beta(\alpha) > 0$ such that if $|H| > p^{\alpha}$, and H is a multiplicative subgroup of \mathbb{F}_p , then*

$$(1) \quad \sum_{x \in H} \psi(x) \ll p^{-\beta}|H|.$$

A proof of this result was first sketched by Bourgain and Konyagin in [10], and detailed proofs were subsequently given by Bourgain, Glibichuk, and Konyagin in [8]. This note is based on the arguments by Bourgain and Chang in [6], and is a somewhat streamlined version of notes from a lecture series given at KTH.

However, as alluded to above, the idea of using additive combinatorics is very versatile. For instance, in [5, 2] Bourgain showed that under certain circumstances it is enough to assume that H has a small multiplicative doubling set, i.e., that $|H \cdot H| < |H|^{1+\tau}$ for $\tau > 0$ small. In particular, one can take $H = \{g^t : t_0 \leq t \leq t_1\}$ as long as the multiplicative order of g modulo p and $t_1 - t_0$ are not too small, and thus it is also possible to non-trivially bound incomplete exponential sums over small (as well as large) multiplicative subgroups. Further, by suitably generalizing the sum-product theorem to subsets of $\mathbb{F}_p \times \mathbb{F}_p$ (some care is required since there are subsets of $\mathbb{F}_p \times \mathbb{F}_p$, e.g., any line passing through $(0, 0)$, that violate a naive generalization of the sum-product theorem), Bourgain showed that there is considerable cancellation in sums of the form $\sum_{s_1=1}^t |\sum_{s_2=1}^t \psi(ag^{s_1} + bg^{s_1 s_2})|$ (consequently proving equidistribution for so-called Diffie-Hellman triples in \mathbb{F}_p^3) and in [4, 3] he obtained bounds for Mordell type exponential sums $\sum_{x=1}^p \psi(f(x))$, where $f(x) = \sum_{i=1}^r a_i x^{k_i}$ is a sparse polynomial (under suitable conditions on the k_i 's.) Moreover, in [7, 6] Bourgain and Chang obtained bounds on

¹See Section 5 for an easy extension to the case of incomplete sums.

sums over multiplicative subgroups (and “almost subgroups”) of general finite fields \mathbb{F}_{p^n} , respectively $\mathbb{Z}/q\mathbb{Z}$ where q is allowed to be composite, but with a bounded number of prime divisors.

1.1. A brief outline of the argument. Define an H -invariant probability measure μ_H on \mathbb{F}_p by

$$\mu_H(x) := \begin{cases} 1/|H| & \text{if } x \in H, \\ 0 & \text{otherwise,} \end{cases}$$

and assume that (1) is violated, i.e., that there exists $\xi \in \mathbb{F}_p^\times$ for which

$$(2) \quad \widehat{\mu}_H(\xi) = \sum_{x \in \mathbb{F}_p} \mu_H(x) \exp\left(\frac{2\pi i x \xi}{p}\right) > p^{-\beta}.$$

Let $\nu = \mu_H * \mu_H^-$, where $\mu_H^-(x) = \mu_H(-x)$, and let ν_k be the k -fold convolution of ν . Using (2), it is possible to show (see Proposition 4.4) that for some tiny η and k sufficiently large,

$$(3) \quad \sum_{x, \xi \in \mathbb{F}_p} |\widehat{\nu}_k(\xi)|^2 |\widehat{\nu}_k(x\xi)|^2 \nu_k(x) > p^{-10\eta} \sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_k(\xi)|^2,$$

and that the support of $\widehat{\nu}_k$ is essentially contained in the set of “large Fourier coefficients” Λ_δ (cf. Proposition 4.2.) Now, $\widehat{\nu}_k$ being essentially supported on Λ_δ means that $\widehat{\nu}_k$ and $\widehat{\nu}_{2k}$ are “similar” (note that $\widehat{\nu}_{2k}(\xi) = \widehat{\nu}_k(\xi)^2$, and $\widehat{\nu}_k(\xi) \geq 0$ for all ξ), hence ν_k and $\nu_{2k} = \nu_k * \nu_k$ are also similar, and this might be seen as a form of statistical, or approximate, additive invariance for the measure ν_k . Further, by Parseval, (3) says that $\sum_{x, y \in \mathbb{F}_p} \nu_{2k}(y) \nu_{2k}(x^{-1}y) \nu_k(x) > p^{-10\eta} \sum_{x \in \mathbb{F}_p} \nu_k(x)^2$, which we may interpret as $\sum_{y \in \mathbb{F}_p} \nu_{2k}(y) \nu_{2k}(x^{-1}y)$ being correlated with ν_k , and this in turn might be seen as statistical multiplicative invariance. (Also see Remarks 3 and 4.) With S_1 being the set of points assigned large relative mass (i.e., those x for which $\nu_k(x)$ is close to $\|\nu_k\|_\infty$) as a starting point, these invariance properties can then be used to find a subset of S_1 with both small sum and product sets. More precisely, using (3), together with the Balog-Gowers-Szemerédi theorem (cf. Theorem 2.2) in multiplicative form, we can find a fairly large subset $S_3 \subset S_1$ with a small product set. Using the Balog-Gowers-Szemerédi theorem again, but in additive form, we then find a large subset $S_4 \subset S_3$ which has a small sum set. Now, since $S_4 \subset S_3$, S_4 also has a small product set, hence it contradicts the sum-product theorem (cf. Theorem 2.1.)

Acknowledgment: It is my pleasure to thank John B. Friedlander and Andrew Granville for their encouragement, as well as many helpful comments and suggestions. I am also grateful to University of Toronto for its hospitality during my visit in April 2007, during which parts of this note were written up.

2. SOME ADDITIVE COMBINATORICS RESULTS

We will need two essential ingredients from additive combinatorics. First we recall the sum-product theorem for subsets of \mathbb{F}_p , due to Bourgain, Katz and Tao [9] (for an expository note, see [11].)

Theorem 2.1. *For any $\epsilon > 0$ there exists $\delta = \delta(\epsilon)$ such that the following holds: If $A \subset \mathbb{F}_p$ is a subset for which $p^\epsilon < |A| < p^{1-\epsilon}$ then*

$$|A + A| + |A \cdot A| \gg |A|^{1+\delta}.$$

We will also need the following version of the Balog-Gowers-Szemerédi theorem (this version of Theorem BGS' in [6] is an immediate consequence of Theorem 5 in Balog's article herein [1]):

Theorem 2.2. *Let A and B be finite subsets of an additive abelian group, Z , and G be a subset of $A \times B$, and let $S = \{a + b : (a, b) \in G\}$. If $|A|, |B|, |S| \leq N$ and $|G| \geq \alpha N^2$ then there is an $A' \subset A$ such that*

$$(4) \quad \begin{aligned} i) \quad & |A' + A'| \leq \frac{2^{37}}{\alpha^8} N, \\ ii) \quad & |A'| \geq \frac{\alpha^4}{2^{15}} N. \end{aligned}$$

3. THE MAIN TECHNICAL RESULT

In this section we prove the key technical result (cf. [6], Proposition 2.1.):

Proposition 3.1. *Let μ be a probability measure on \mathbb{F}_p . If there exists a constant $\Delta \in (0, \frac{1}{2}]$ such that*

$$(5) \quad \sum_{\xi, y \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 |\widehat{\mu}(y\xi)|^2 \mu(y) > \Delta \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2,$$

and

$$(6) \quad \mu(0), \quad \sum_{x \in \mathbb{F}_p} \mu(x)^2 < \Delta/4$$

then there exist a subset $S \subset \mathbb{F}_p^\times$ such that

$$(7) \quad \frac{\Delta^{254}}{2^{900}} p < |S| \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 < \frac{8}{\Delta} p,$$

and

$$|S + S| + |S \cdot S| < \frac{2^{2729}}{\Delta^{768}} |S|.$$

To prove Proposition 3.1 we will construct a sequence of subsets $\mathbb{F}_p \supset S_1 \supset S_2 \supset S_3 \supset S_4$ such that $|S_i|/|S_{i+1}| = \Delta^{O(1)}$, where S_3 has a small product set and S_4 has a small sum set.

First let us recall some useful properties of the finite Fourier transform. For a given probability measure μ on \mathbb{F}_p define its Fourier transform to be

$$\widehat{\mu}(\xi) := \sum_{x \in \mathbb{F}_p} \mu(x) \psi(x\xi),$$

so that $\overline{\widehat{\mu}(\xi)} = \widehat{\mu}(-\xi)$. With this normalization, Parseval's formula reads as

$$p \sum_{x \in \mathbb{F}_p} |\mu(x)|^2 = \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2.$$

As μ is a probability measure, we see that

$$\phi(x) := p(\mu * \mu^-)(x) = \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 \psi(x\xi)$$

is ≥ 0 for all x . We will replace the middle term in (7) by $|S|\phi(0)$. Moreover,

$$\sum_{x \in \mathbb{F}_p} \phi(x) = p,$$

since $\mu * \mu^-$ is also a probability measure. From the Fourier expansion of ϕ , we have

$$(8) \quad \max_{x \in \mathbb{F}_p} \phi(x) = \phi(0) = p \cdot (\mu * \mu^-)(0) = p \sum_x \mu(x)^2 \leq \Delta p / 4$$

by (6).

3.1. Multiplicative stability. We obtain the following form of “statistical multiplicative stability”.

Lemma 3.2. *If (5) and (6) hold then*

$$(9) \quad \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p^\times} \phi(x)\phi(xy)\mu(y) > \frac{3}{4} \Delta p \phi(0)$$

Proof. For y fixed, we have

$$\sum_{x \in \mathbb{F}_p} \phi(x)\phi(xy) = \sum_{\xi, \tau \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 |\widehat{\mu}(\tau)|^2 \sum_{x \in \mathbb{F}_p} \psi(x\tau + xy\xi) = p \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 |\widehat{\mu}(-y\xi)|^2.$$

Summing this over all $y \in \mathbb{F}_p^\times$, we see that the left hand side of (9) equals

$$\begin{aligned} & p \sum_{y, \xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 |\widehat{\mu}(-y\xi)|^2 \mu(y) - p \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 |\widehat{\mu}(0)|^2 \mu(0) \\ & \geq p \Delta \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 - p(\Delta/4) |\widehat{\mu}(0)|^2 \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 \end{aligned}$$

by (5) and (6), as $|\widehat{\mu}(-y\xi)|^2 = |\widehat{\mu}(y\xi)|^2$, which yields the result since $|\widehat{\mu}(0)|^2 \leq 1$. \square

Remark 1. Note that $\sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p^\times} \phi(x)\phi(xy)\mu(y) \leq \phi(0) \sum_{x, y \in \mathbb{F}_p} \phi(x)\mu(y) \leq p\phi(0)$. In our applications, we shall take $\Delta = p^{-\epsilon}$, and for this choice of Δ , the lower bound (9) is fairly good.

As a starting point for a multiplicatively stable subset, we use the points which are assigned large measure by $\mu * \mu^-$.

Lemma 3.3. *If (5) and (6) hold and*

$$S_1 := \{x \in \mathbb{F}_p : \phi(x) > \frac{1}{8}\Delta\phi(0)\}$$

then

$$(10) \quad \sum_{\substack{x \in S_1, y \in \mathbb{F}_p^\times \\ xy \in S_1}} \phi(x)\phi(xy)\mu(y) > \frac{1}{2} \Delta p\phi(0)$$

Proof. We have

$$\sum_{\substack{x \in S_1, y \in \mathbb{F}_p^\times \\ xy \in S_1}} \geq \sum_{x \in \mathbb{F}_p, y \in \mathbb{F}_p^\times} - \sum_{x \in \mathbb{F}_p \setminus S_1, y \in \mathbb{F}_p^\times} - \sum_{\substack{x \in \mathbb{F}_p, y \in \mathbb{F}_p^\times \\ xy \notin S_1}} .$$

By (9), the first term on the right hand side is $> (3/4)\Delta p\phi(0)$. The second term

$$\sum_{x \in \mathbb{F}_p \setminus S_1, y \in \mathbb{F}_p^\times} \phi(x)\phi(xy)\mu(y)$$

is, since $\phi(x) \leq \Delta\phi(0)/8$ for $x \notin S_1$, bounded by

$$\frac{\Delta\phi(0)}{8} \sum_{x \in \mathbb{F}_p \setminus S_1, y \in \mathbb{F}_p^\times} \phi(xy)\mu(y) \leq \frac{\Delta\phi(0)}{8} \sum_{y \in \mathbb{F}_p^\times} \mu(y) \sum_{x \in \mathbb{F}_p} \phi(xy) \leq \frac{\Delta p\phi(0)}{8}$$

since $\sum_{x \in \mathbb{F}_p} \phi(xy) = p$ for $y \neq 0$ and μ is a probability measure. Similarly, the third term is bounded by $\Delta p\phi(0)/8$, hence the left hand side of (10) is $> \Delta p\phi(0)(3/4 - 1/8 - 1/8) \geq \Delta p\phi(0)/2$. \square

We proceed to estimate the size of S_1 .

Lemma 3.4. *If (5) and (6) hold then*

$$(11) \quad \frac{\Delta p}{2\phi(0)} < |S_1| < \frac{8p}{\Delta\phi(0)}.$$

Moreover, if we let

$$S_2 := S_1 \setminus \{0\} \subset \mathbb{F}_p^\times,$$

then $|S_2| \geq |S_1|/2$.

Proof. For the lower bound, note that

$$(12) \quad \begin{aligned} |S_1| &= \sum_{y \in \mathbb{F}_p} |S_1 \cap y^{-1}S_1| \mu(y) \geq \sum_{y \in \mathbb{F}_p^\times} |S_1 \cap y^{-1}S_1| \mu(y) = \sum_{\substack{x \in S_1, y \in \mathbb{F}_p^\times \\ xy \in S_1}} \mu(y) \\ &\geq \frac{1}{\phi(0)^2} \sum_{\substack{x \in S_1, y \in \mathbb{F}_p^\times \\ xy \in S_1}} \phi(x)\phi(xy)\mu(y) > \frac{\Delta p}{2\phi(0)} \end{aligned}$$

by (10), which is ≥ 2 by (8), so that $|S_2| \geq |S_1|/2$. For the upper bound, note that

$$|S_1| < \frac{8}{\Delta\phi(0)} \sum_{x \in S_1} \phi(x) \leq \frac{8}{\Delta\phi(0)} \sum_{x \in \mathbb{F}_p} \phi(x) = \frac{8p}{\Delta\phi(0)}.$$

□

To show that there are many y such that $|S_2 \cap y^{-1}S_2|$ is fairly large, we begin by giving a lower bound on the expected size of the intersection.

Lemma 3.5. *If (5) and (6) hold then*

$$(13) \quad \sum_{y \in \mathbb{F}_p^\times} |S_2 \cap y^{-1}S_2| \mu(y) \geq \frac{\Delta p}{4\phi(0)}$$

Proof. Since $S_2 \cap y^{-1}S_2 = (S_1 \cap y^{-1}S_1) \setminus \{0\}$ for all $y \in \mathbb{F}_p^\times$ we have

$$\begin{aligned} \sum_{y \in \mathbb{F}_p^\times} |S_2 \cap y^{-1}S_2| \mu(y) &\geq \sum_{y \in \mathbb{F}_p^\times} |S_1 \cap y^{-1}S_1| \mu(y) - \sum_{y \in \mathbb{F}_p^\times} \mu(y) \\ &> \frac{\Delta p}{2\phi(0)} - 1 \geq \frac{\Delta p}{4\phi(0)} \end{aligned}$$

by the right hand side of (12) and as $\sum_{y \in \mathbb{F}_p} \mu(y) = 1$, and then by (8). □

In the next result we show that there are many y for which $|S_2 \cap y^{-1}S_2|$ is large:

Lemma 3.6. *If (5) and (6) hold and*

$$(14) \quad T := \left\{ y \in \mathbb{F}_p^\times : |S_2 \cap y^{-1}S_2| > \frac{\Delta p}{8\phi(0)} \right\}$$

then

$$(15) \quad |T| \geq \frac{\Delta^5}{2^{15}} |S_1|$$

Proof.

$$\begin{aligned} |S_2| \mu(T) &= |S_2| \sum_{y \in T} \mu(y) \geq \sum_{y \in T} |S_2 \cap y^{-1}S_2| \mu(y) \\ (16) \quad &= \sum_{y \in \mathbb{F}_p^\times} |S_2 \cap y^{-1}S_2| \mu(y) - \sum_{y \in \mathbb{F}_p^\times \setminus T} |S_2 \cap y^{-1}S_2| \mu(y) \geq \frac{\Delta p}{8\phi(0)} > \frac{\Delta^2}{64} |S_2| \end{aligned}$$

by (13) and from the definition of T , and then by (11) and the trivial bound $|S_2| \leq |S_1|$, so that $\mu(T) > \Delta^2/64$.

On the other hand, by Cauchy-Schwartz and Parseval's identity,

$$\mu(T) \leq |T|^{1/2} \left(\sum_{x \in T} \mu(x)^2 \right)^{1/2}$$

$$\leq |T|^{1/2} \left(\frac{1}{p} \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 \right)^{1/2} = \left(\frac{|T|\phi(0)}{p} \right)^{1/2},$$

so that $|T| \geq p\Delta^4/(2^{12}\phi(0)) > (\Delta^5/2^{15})|S_1|$, by (11). \square

Thus, by shrinking T if necessary, we have found a set T such that

$$(\Delta^5/2^{15})|S_2| \leq |T| \leq |S_2|$$

with the property that for all $y \in T$,

$$(17) \quad |S_2 \cap y^{-1}S_2| > \frac{\Delta p}{8\phi(0)} > \frac{\Delta^2}{26}|S_1| \geq \frac{\Delta^2}{26}|S_2|$$

by (11).

Let $G := \{(x, y) : x \in S_2, y \in T, xy \in S_2\} \subset S_2 \times T \subset \mathbb{F}_p^\times \times \mathbb{F}_p^\times$. By (17), the number of x such that $(x, y) \in G$ is at least $2^{-6}\Delta^2|S_2|$ for each $y \in T$. Therefore, since $|T| \geq 2^{-15}\Delta^5|S_2|$, we find that

$$|G| \geq 2^{-6}\Delta^2|S_2| \cdot 2^{-15}\Delta^5|S_2| = (\Delta/8)^7|S_2|^2.$$

By the definition of G we know that

$$\{st : (s, t) \in G\} \subset S_2;$$

so, with g a primitive root modulo p and defining $\log_{g,p}(s)$ to be the smallest integer $m \geq 0$ such that $g^m \equiv s \pmod{p}$, and by taking $A = \{\log_{g,p} s : s \in S_2\}$, $B = \{\log_{g,p} t : t \in T\}$ with $N = |S_2|$ and $\alpha = (\Delta/8)^7$ in Theorem 2.2, we obtain a subset A' of A , with $|A'| > (\Delta^{28}/2^{99})|A|$, for which

$$|A' + A'| \leq (2^{205}/\Delta^{56})N < (2^{304}/\Delta^{84})|A'|.$$

Therefore $S_3 = \{g^a : a \in A'\}$ is a subset of S_2 for which

$$(18) \quad |S_3| > (\Delta^{28}/2^{100})|S_1|,$$

by Lemma 3.4, and

$$|S_3 \cdot S_3| \leq (2^{304}/\Delta^{84})|S_3|.$$

3.2. Additive stability. We finish the proof of Proposition 3.1 by finding a subset S_4 of S_3 with a small sum set. We first show that S_3 exhibits “statistical additive stability”; to do this we only need to use that $S_3 \subset S_1$, together with the definition of S_1 .

Lemma 3.7. *If (5) and (6) hold then*

$$(19) \quad \sum_{x_1, x_2 \in S_3} \phi(x_1 - x_2) > 2^{-6}\Delta^2\phi(0)|S_3|^2$$

Proof. Recalling that $\phi(x) = p(\mu * \mu^-)(x)$, we find, using the Cauchy-Schwarz inequality, that

$$\left(\frac{1}{p} \sum_{x \in S_3} \phi(x) \right)^2 = \left(\sum_{y \in \mathbb{F}_p} \mu(y) \sum_{x \in S_3} \mu(x+y) \right)^2 \leq \sum_{y \in \mathbb{F}_p} \mu(y)^2 \cdot \sum_{y \in \mathbb{F}_p} \left(\sum_{x \in S_3} \mu(x+y) \right)^2$$

$$= \frac{\phi(0)}{p} \sum_{x_1, x_2 \in S_3} \sum_{y \in \mathbb{F}_p} \mu(x_1 + y) \mu(x_2 + y) = \frac{\phi(0)}{p^2} \sum_{x_1, x_2 \in S_3} \phi(x_1 - x_2).$$

Now $\sum_{x \in S_3} \phi(x) > \frac{\Delta}{8} \phi(0) |S_3|$, since $S_3 \subset S_1$, and the lemma follows. \square

To obtain an additively stable subset we will, as before, use Theorem 2.2. First, let

$$(20) \quad S_0 := \{x \in \mathbb{F}_p : \phi(x) > 2^{-7} \Delta^2 \phi(0)\}$$

Then

$$|S_0| \leq \frac{2^7}{\Delta^2 \phi(0)} \sum_{x \in S_0} \phi(x) \leq \frac{2^7 p}{\Delta^2 \phi(0)} \leq \frac{2^8}{\Delta^3} |S_1| < \frac{2^{108}}{\Delta^{31}} |S_3|$$

by (11) and then (18).

Using S_0, S_3 we can now define a fairly large graph G' .

Lemma 3.8. *If (5) and (6) hold then*

$$G' := \{(x_1, -x_2) \in S_3 \times (-S_3) : x_1 - x_2 \in S_0\} \subset S_3 \times (-S_3).$$

has at least $2^{-7} \Delta^2 |S_3|^2$ elements.

Proof. We have

$$\begin{aligned} |G'| \cdot \phi(0) &\geq \sum_{(x_1, -x_2) \in G'} \phi(x_1 - x_2) \\ &= \sum_{x_1, x_2 \in S_3} \phi(x_1 - x_2) - \sum_{(x_1, -x_2) \in S_3 \times (-S_3) \setminus G'} \phi(x_1 - x_2) \\ &\geq 2^{-6} \Delta^2 \phi(0) |S_3|^2 - 2^{-7} \Delta^2 \phi(0) |S_3|^2 \end{aligned}$$

by (19) and (20), and the result follows. \square

Since $\{x_1 - x_2 : (x_1, -x_2) \in G'\} \subset S_0$ we can apply Theorem 2.2 with $A = S_3$, $B = -S_3$, $G = G'$, $N = (2^{108}/\Delta^{31}) |S_3|$ and $\alpha = \Delta^{64}/2^{223}$ to obtain a subset $S_4 \subset S_3$ with

$$(21) \quad |S_4| > \frac{\Delta^{256}}{2^{907}} N = \frac{\Delta^{225}}{2^{799}} |S_3|$$

for which

$$|S_4 + S_4| < \frac{2^{1821}}{\Delta^{512}} N = \frac{2^{1929}}{\Delta^{543}} |S_3| < \frac{2^{2728}}{\Delta^{768}} |S_4|.$$

Moreover, since $S_4 \subset S_3$, we find that

$$|S_4 \cdot S_4| \leq |S_3 \cdot S_3| < (2^{304}/\Delta^{84}) |S_3| < (2^{1103}/\Delta^{309}) |S_4|.$$

Finally, by (11), then (21), (18), and Lemma 3.4, we have

$$\frac{8p}{\Delta \phi(0)} > |S_1| \geq |S_4| > \frac{\Delta^{225}}{2^{799}} |S_3| > \frac{\Delta^{253}}{2^{899}} |S_1| > \frac{\Delta^{254}}{2^{900}} \frac{p}{\phi(0)}.$$

Taking $S = S_4$ we have found a set with the desired properties.

4. PROOF OF THEOREM 1.1

4.1. Preliminaries. Let μ be a given probability measure on \mathbb{F}_p . Recall that the Fourier transform of μ was defined to be $\widehat{\mu}(\xi) := \sum_{x \in \mathbb{F}_p} \mu(x) \psi(x\xi)$, and hence $\overline{\widehat{\mu}(\xi)} = \widehat{\mu}(-\xi)$. With this normalization, Parseval's formula reads as $p \sum_{x \in \mathbb{F}_p} |\mu(x)|^2 = \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2$. Moreover, if ν is another probability measure then

$$\sum_{x \in \mathbb{F}_p} \mu(x) \widehat{\nu}(x) = \sum_{\xi \in \mathbb{F}_p} \overline{\widehat{\mu}(\xi)} \nu(-\xi) = \sum_{\xi \in \mathbb{F}_p} \widehat{\mu}(-\xi) \nu(-\xi) = \sum_{\xi \in \mathbb{F}_p} \widehat{\mu}(\xi) \nu(\xi)$$

Let $\nu := \mu * \mu^-$, that is $\nu(x) = \sum_{y,z: y-z=x} \mu(y) \mu(z)$, so that $\nu(-x) = \nu(x)$ and $\widehat{\nu}(x) = |\widehat{\mu}(x)|^2$. If ν_k is the k -fold convolution of ν , that is

$$\nu_k(x) := \sum_{\substack{y_1, y_2, \dots, y_k \in \mathbb{F}_p \\ y_1 + y_2 + \dots + y_k = x}} \nu(y_1) \nu(y_2) \cdots \nu(y_k),$$

then $\widehat{\nu}_k(x) = |\widehat{\mu}(x)|^{2k} \geq 0$. Notice that $\nu(x) = \sum_{y,z: y-z=x} \mu(y) \mu(z) \leq \max_z \mu(z) \sum_y \mu(y) = \max_z \mu(z)$ for all x ; and similarly

$$(22) \quad \max_x \nu_k(x) \leq \max_z \mu(z) \text{ for all } k.$$

We have

$$\|\mu_H\|_2^2 = \sum_{x \in \mathbb{F}_p} |\mu_H(x)|^2 = 1/|H|.$$

Note that $\mu_H(hx) = \mu_H(x)$ for all $h \in H$, and so $\widehat{\mu}_H(hx) = \widehat{\mu}_H(x)$ for all $h \in H$, and $\nu_k(hx) = \nu_k(x)$ for all $h \in H$ and $k \geq 1$.

4.2. The set of large Fourier coefficients. Given $\delta > 0$, let

$$\Lambda_\delta := \{\xi \in \mathbb{F}_p : |\widehat{\mu}(\xi)| > p^{-\delta}\}$$

be the set of “large” Fourier coefficients of μ .

Lemma 4.1. *Suppose that $\mu = \mu_H$. We have*

$$|\Lambda_\delta| \leq p^{1+2\delta}/|H|.$$

Also if $|\widehat{\mu}_H(\xi)| > p^{-\delta}$ for some nonzero $\xi \in \mathbb{F}_p^\times$, then

$$|\Lambda_\delta| \geq |H|.$$

Proof. For any measure μ on \mathbb{F}_p we have

$$|\Lambda_\delta| \leq p^{2\delta} \sum_{\xi \in \Lambda_\delta} |\widehat{\mu}(\xi)|^2 \leq p^{2\delta} \sum_{\xi \in \mathbb{F}_p} |\widehat{\mu}(\xi)|^2 = p^{1+2\delta} \sum_{x \in \mathbb{F}_p} |\mu(x)|^2,$$

and the first result follows since this last sum equals $1/|H|$ for $\mu = \mu_H$. For the second result note that if $\xi \in \Lambda_\delta$ then $|\widehat{\mu}_H(h\xi)| = |\widehat{\mu}_H(\xi)| > p^{-\delta}$ for all $h \in H$, so that $h\xi \in \Lambda_\delta$ for all $h \in H$. \square

We will now show that it is possible to find k, δ so that the support of $\widehat{\nu}_k$ is, in L^2 -sense, essentially given by Λ_δ .

Proposition 4.2. *For any measure μ on \mathbb{F}_p , where $p \geq 3$, and any $\eta \geq 5/(p^3 \log p)$, there exists an integer $k \geq 4$ and*

$$\delta \in (0, \eta/k^2)$$

such that

$$(23) \quad p^{-\eta} |\Lambda_\delta| \leq \sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_k(\xi)|^2 \leq p^\eta |\Lambda_\delta|$$

and, in particular,

$$(24) \quad \sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_k(\xi)|^2 \leq p^{2\eta} \sum_{\xi \in \Lambda_\delta} |\widehat{\nu}_k(\xi)|^2.$$

Proof. For any $k \in \mathbb{N}$ we have

$$(25) \quad \sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_k(\xi)|^2 = \sum_{\xi \in \Lambda_{1/k}} |\widehat{\nu}_k(\xi)|^2 + \sum_{\xi \notin \Lambda_{1/k}} |\widehat{\nu}_k(\xi)|^2 \leq |\Lambda_{1/k}| + p(p^{-1/k})^{4k} = |\Lambda_{1/k}| + 1/p^3$$

since each $|\widehat{\nu}_k(\xi)| \leq 1$.

We define a sequence of integers $k_0 = 4 < k_1 < \dots$ where $k_{i+1} = [k_i^2/\eta] + 1$ for each $i \geq 0$, and let $\delta_i = 1/k_{i+1}$ for each i . Note that $k_i^2/\eta < k_{i+1} = 1/\delta_i$ so that $k_i \delta_i < \eta/k_i \leq \eta/4$. Since $|\widehat{\nu}_{k_i}(\xi)| = |\widehat{\mu}_H(\xi)|^{2k_i}$, we have

$$\sum_{\xi \in \Lambda_{\delta_i}} |\widehat{\nu}_{k_i}(\xi)|^2 > |\Lambda_{\delta_i}| \cdot p^{-4k_i \delta_i} \geq |\Lambda_{\delta_i}| \cdot p^{-\eta}.$$

We note that the lower bound in (23) follows from this, as well as (24), once we establish the upper bound in (23).

Now, there exists an integer $i \in [0, M]$, where $M = 2([1/\eta] + 1)$, such that $\sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_{k_i}(\xi)|^2 \leq p^\eta |\Lambda_{\delta_i}|$ else

$$p^\eta |\Lambda_{1/k_{i+1}}| = p^\eta |\Lambda_{\delta_i}| < \sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_{k_i}(\xi)|^2 \leq |\Lambda_{1/k_i}| + 1/p^3 \leq |\Lambda_{1/k_i}|(1 + 1/p^3)$$

for each i , by (25), and so

$$|\Lambda_{1/k_M}| < p^{-M\eta} |\Lambda_{1/k_0}|(1 + 1/p^3)^M \leq p^{1-M\eta} (1 + 1/p^3)^M \leq p^{-1} (1 + 1/p^3)^M < 1$$

since $M \leq \frac{1}{2}p^3 \log p$, which is untrue (as $0 \in \Lambda_{1/k}$ for all $k \in \mathbb{N}$).

We select $k = k_i$ and $\delta = \delta_i$. \square

Remark 2. *Note that the proof gives us $k \ll \exp(\exp(O(1/\eta)))$.*

Remark 3. *Since the support of $\widehat{\nu}_k$ is essentially given by Λ_δ , it is easy to see that the same holds for $\widehat{\nu}_{2k}$; we may interpret this as $\nu_k * \nu_k$ being “similar” to ν_k , and hence that ν_k is “approximately additively stable”.*

In the following key Lemma, the H -invariance of μ_H , and hence of $\widehat{\nu}_k$, is essential.

Lemma 4.3. *For $\mu = \mu_H$ and all $\xi \in \mathbb{F}_p$, we have*

$$\widehat{\nu}_k(\xi)^{4k} \leq \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(x\xi)^2 \nu_k(x)$$

Proof. The case $\xi = 0$ is immediate, hence we may assume that $\xi \neq 0$. Now, since $\widehat{\nu}_k(h\xi) = \widehat{\nu}_k(\xi)$ for all $h \in H$, we have

$$\widehat{\nu}_k(\xi)^2 = \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(x\xi)^2 \mu_H(x) = \sum_{x \in \mathbb{F}_p} \nu_{2k}(-x\xi^{-1}) \widehat{\mu}_H(x),$$

by Parseval's formula. Now note that if μ is any probability measure and $l \geq 1$, then $\sum_x \mu(x) f(x) \leq (\sum_x \mu(x) |f(x)|^l)^{1/l}$. Therefore the above gives

$$\widehat{\nu}_k(\xi)^{4k} \leq \sum_{x \in \mathbb{F}_p} \nu_{2k}(-x\xi^{-1}) |\widehat{\mu}_H(x)|^{2k} = \sum_{x \in \mathbb{F}_p} \nu_{2k}(-x\xi^{-1}) \widehat{\nu}_k(x)$$

since $|\widehat{\mu}_H(x)|^{2k} = \widehat{\nu}(x)^k = \widehat{\nu}_k(x)$ and, applying Parseval one more time, we obtain

$$\widehat{\nu}_k(\xi)^{4k} \leq \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(-x\xi)^2 \nu_k(-x) = \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(x\xi)^2 \nu_k(x)$$

□

We consequently obtain:

Proposition 4.4. *With k, η as in Proposition 4.2, we have*

$$p^{-10\eta} \sum_{\xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \leq \sum_{\xi \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \widehat{\nu}_k(x\xi)^2 \nu_k(x)$$

Proof. By Proposition 4.2, we have

$$p^{-2\eta} \sum_{\xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \leq \sum_{\xi \in \Lambda_\delta} \widehat{\nu}_k(\xi)^2 \leq p^{8k^2\delta} \sum_{\xi \in \Lambda_\delta} \widehat{\nu}_k(\xi)^{4k+2} \leq p^{8\eta} \sum_{\xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^{4k+2}$$

which, by Lemma 4.3, is

$$\leq p^{8\eta} \sum_{\xi \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \widehat{\nu}_k(x\xi)^2 \nu_k(x).$$

□

Remark 4. *Since $\widehat{\nu}_k(x\xi) \leq 1$ and ν_k is a probability measure, we find that $\sum_{\xi, x \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \widehat{\nu}_k(x\xi)^2 \nu_k(x) \leq \sum_{\xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2$, so the lower bound on the double sum in Proposition 4.4 is quite good. Further, using Parseval on the two sums over ξ (ignoring the term $x = 0$) we find that $\sum_{y \in \mathbb{F}_p} \nu_{2k}(y) \nu_{2k}(yx^{-1})$, which we can interpret as a multiplicative translate of ν_{2k} with itself, is highly correlated with $\nu_k(x)$. Thus, the Proposition might be interpreted as a statement of “approximate multiplicative stability” of ν_k . (Since the essential support of $\widehat{\nu}_k$ is given by Λ_δ , the same holds for $\widehat{\nu}_{2k}$, so in some sense ν_k and ν_{2k} are “similar”.)*

To go from statistical additive/multiplicative stability to a subset that contradicts the sum-product Theorem, we will apply Proposition 3.1 with $\mu = \nu_k$ and $\Delta = p^{-10\eta}$ (and note that (22) implies (6) provided $1/|H| < \Delta/4$), and select δ and k as in Proposition 4.2. Assume that $|\widehat{\mu}_H(\xi)| > p^{-\delta}$ for some $\xi \in \mathbb{F}_p^\times$. We thus obtain a set S such that

$$|S + S| + |S \cdot S| < 2^{2729} p^{7680\eta} |S|.$$

Note that

$$p^{-\eta} |H| \leq p^{-\eta} |\Lambda_\delta| \leq \sum_{\xi \in \mathbb{F}_p} |\widehat{\nu}_k(\xi)|^2 \leq p^\eta |\Lambda_\delta| \leq p^{1+\eta+2\delta}/|H|$$

by (23) and Lemma 4.1, so that (7) gives, as $2\delta < \eta$,

$$\frac{1}{2^{900}} \frac{|H|}{p^{2542\eta}} < |S| < 8 \frac{p^{1+11\eta}}{|H|}.$$

Now select $\eta = \min\{\alpha/6000, \delta(\alpha/2)/8000\}$, so that the sum-product Theorem 2.1 is violated with $\epsilon = \alpha/2$ for p sufficiently large, and thus $|\widehat{\mu}_H(\xi)| \leq p^{-\delta}$ for all $\xi \in \mathbb{F}_p^\times$. The Theorem follows with $\beta = \delta \gg \exp(-\exp(C/\eta))$ for some constant $C > 0$.

5. INCOMPLETE SUMS

The proof of Theorem 1.1 can fairly easily be extended to incomplete sums over multiplicative subgroups.

Theorem 5.1. *Let $g \in \mathbb{F}_p^\times$ have multiplicative order at least T , and let $H = \{g^t : 0 \leq t < T\}$. If $|H| = T > p^\alpha$, then*

$$\sum_{x \in H} \psi(x) \ll p^{-\beta} |H|$$

Define $\mu_H, \widehat{\mu}_H, \nu_k, \Lambda_\delta$ etc as before. To obtain a contradiction, we will assume that $|\widehat{\mu}_H(\xi_0)| > 2p^{-\delta}$ for some $\xi_0 \in \mathbb{F}_p^\times$.

We begin by showing that Λ_δ , the set of large Fourier coefficients, is almost of size $|H|$, and that $\widehat{\mu}$ is quite large on $\Lambda_\delta \cdot H_1$ for a fairly large subset $H_1 \subset H$.

Lemma 5.2. *Let*

$$H_1 := \{g^t : 0 \leq t < |H|p^{-\delta}/4\}.$$

If $|\widehat{\mu}(\xi_0)| > 2p^{-\delta}$ for some $\xi_0 \in \mathbb{F}_p^\times$, then

$$|\Lambda_\delta| \geq |H_1|$$

Moreover, if $\xi \in \Lambda_\delta$ and $h \in H_1$, then

$$|\widehat{\mu}_H(h\xi)| > |\widehat{\mu}_H(\xi)|/2.$$

Proof. For $l \in \mathbb{Z}$ such that $0 \leq l < T$, we have

$$\begin{aligned}\widehat{\mu}_H(g^l\xi) &= \sum_{x \in \mathbb{F}_p} \psi(g^l\xi x) \mu_H(x) = \sum_{x \in \mathbb{F}_p} \psi(\xi x) \mu_H(g^{-l}x) = \frac{1}{|H|} \sum_{x \in g^l H} \psi(\xi x) \\ &= \frac{1}{|H|} \left(\sum_{x \in H} \psi(\xi x) + 2\theta l \right)\end{aligned}$$

for some θ such that $|\theta| \leq 1$. Thus, if $l < |H|p^{-\delta}/4$, then

$$(26) \quad |\widehat{\mu}_H(g^l\xi)| > |\widehat{\mu}_H(\xi)| - p^{-\delta}/2.$$

In particular, if $h \in H_1$, then $|\widehat{\mu}_H(h\xi_0)| \geq |\widehat{\mu}_H(\xi_0)| - p^{-\delta}/2 > 2p^{-\delta} - p^{-\delta}/2 > p^{-\delta}$ and hence $|\Lambda_\delta| \geq |H_1|$. Finally, if $\xi \in \Lambda_\delta$ then $|\widehat{\mu}_H(\xi)| > p^{-\delta}$, so the second assertion follows from (26). \square

Lemma 5.3. *If $\xi \in \Lambda_\delta$, then*

$$\widehat{\nu}_k(\xi)^{4k} \leq 2^{8k^2+6k} p^{2k\delta} \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(h\xi)^2 \nu_k(x)$$

Proof. If $\xi \in \Lambda_\delta$, then $|\widehat{\mu}_H(\xi h)| \geq |\widehat{\mu}_H(\xi)|/2$ for all $h \in H_1$. Hence

$$\begin{aligned}\widehat{\nu}_k(\xi)^2 &\leq \frac{2^{4k}}{|H_1|} \sum_{h \in H_1} \widehat{\nu}_k(h\xi)^2 \leq \frac{2^{4k}|H|}{|H_1|} \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(h\xi)^2 \mu_H(x) \\ &= 2^{4k+3} p^\delta \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(h\xi)^2 \mu_H(x)\end{aligned}$$

since $|H|/|H_1| \leq 8p^\delta$. Thus, if $\xi \in \Lambda_\delta$, then

$$\widehat{\nu}_k(\xi)^{4k} \leq 2^{8k^2+6k} p^{2k\delta} \left(\sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(h\xi)^2 \mu_H(x) \right)^{2k} \leq 2^{8k^2+6k} p^{2k\delta} \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(h\xi)^2 \nu_k(x)$$

by the same argument used in the proof of Lemma 4.3. \square

Proposition 5.4. *For p sufficiently large,*

$$p^{-11\eta} \sum_{\xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \leq \sum_{\xi, x \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \widehat{\nu}_k(\xi x)^2 \nu_k(x)$$

Proof. Arguing as in the proof of Proposition 4.4 find that

$$p^{-2\eta} \sum_{\xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \leq \sum_{\xi \in \Lambda_\delta} \widehat{\nu}_k(\xi)^2 \leq p^{8k^2\delta} \sum_{\xi \in \Lambda_\delta} \widehat{\nu}_k(\xi)^{4k+2} \leq p^{8\eta} \sum_{\xi \in \Lambda_\delta} \widehat{\nu}_k(\xi)^{4k+2}$$

which, by Lemma 5.3 is

$$\leq p^{8\eta+2k\delta} 2^{8k^2+6k} \sum_{\xi \in \Lambda_\delta} \sum_{x \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \widehat{\nu}_k(\xi x)^2 \nu_k(x) \leq p^{9\eta} \sum_{x, \xi \in \mathbb{F}_p} \widehat{\nu}_k(\xi)^2 \widehat{\nu}_k(\xi x)^2 \nu_k(x)$$

\square

The rest of the proof is now essentially the same as the proof of Theorem 1.1.

REFERENCES

- [1] A. Balog, *Many additive quadruples*, herein.
- [2] J. Bourgain, *Estimates on exponential sums related to the Diffie-Hellman distributions*, Geom. Funct. Anal. **15** (2005), no. 1, 1–34. MR MR2140627 (2006h:11095)
- [3] ———, *Mordell’s exponential sum estimate revisited*, J. Amer. Math. Soc. **18** (2005), no. 2, 477–499 (electronic). MR MR2137982 (2006b:11099)
- [4] ———, *Mordell type exponential sum estimates in fields of prime order*, C. R. Math. Acad. Sci. Paris **339** (2004), no. 5, 321–325. MR MR2092056 (2005h:11178)
- [5] ———, *New bounds on exponential sums related to the Diffie-Hellman distributions*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 11, 825–830. MR MR2059656 (2005b:11128)
- [6] J. Bourgain and M.-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of \mathbb{Z}_Q^* , where Q is composite with few prime factors*, Geom. Funct. Anal. **16** (2006), no. 2, 327–366. MR MR2231466 (2007d:11093)
- [7] ———, *A gauss sum estimate in arbitrary finite fields*, to appear in C. R. Math. Acad. Sci. Paris.
- [8] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) **73** (2006), no. 2, 380–398. MR MR2225493 (2007e:11092)
- [9] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), no. 1, 27–57. MR MR2053599 (2005d:11028)
- [10] J. Bourgain and 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 **337** (2003), no. 2, 75–80. MR MR1998834 (2004g:11067)
- [11] B. Green, *Sum-product estimates*, <http://www.dpmms.cam.ac.uk/~bjg23/notes.html>.
- [12] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn’s exponential sum*, Q. J. Math. **51** (2000), no. 2, 221–235. MR MR1765792 (2001h:11106)
- [13] S. V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, IV International Conference “Modern Problems of Number Theory and its Applications”: Current Problems, Part III (Russian) (Tula, 2001), Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002, pp. 86–114. MR MR1985950 (2004d:11073)
- [14] I. E. Shparlinskii, *Estimates for Gauss sums*, Mat. Zametki **50** (1991), no. 1, 122–130. MR MR1140360 (92m:11082)

DEPARTMENT OF MATHEMATICS, ROYAL INSTITUTE OF TECHNOLOGY, SE-100 44
STOCKHOLM, SWEDEN

E-mail address: kurlberg@math.kth.se