

On sumsets and spectral gaps

by

ERNIE CROOT (Atlanta, GA) and TOMASZ SCHOEN (Poznań)

1. Introduction. Suppose that $S \subseteq \mathbb{F}_p$, where p is a prime number. Let $\lambda_1, \dots, \lambda_p$ be the absolute values of the Fourier coefficients of S (to be made more precise below) arranged as follows:

$$\widehat{S}(0) = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_p.$$

Then, as is well known, one can work out, as a function of $\varepsilon > 0$ and a density $\theta = |S|/p$, an upper bound for the ratio λ_2/λ_1 which guarantees that $S + S$ covers at least $(1 - \varepsilon)p$ residue classes modulo p . Put another way, if S has a large spectral gap, then most elements of \mathbb{F}_p have the same number of representations as a sum of two elements of S , thereby making $S + S$ large.

What we show in this paper is an extension of this fact, which holds for spectral gaps between other consecutive Fourier coefficients λ_k, λ_{k+1} , so long as k is not too large; in particular, our theorem will work so long as

$$1 \leq k \leq \lceil (\log p) / \log 2 \rceil.$$

Furthermore, we develop results for repeated sums $S + S + \dots + S$.

It is worth noting that this phenomenon also holds in arbitrary abelian groups, as can be worked out by applying some results of Lev [4], [5], but we will not develop this here ⁽¹⁾.

The property of \mathbb{F}_p that we exploit is something we call a “unique differences” property, first identified by W. Feit, with first proofs and basic results found by Straus [7].

2000 *Mathematics Subject Classification*: Primary 11B50; Secondary 11B34, 05D99.

Key words and phrases: additive combinatorics, sumsets, pseudorandom functions, spectral gaps.

⁽¹⁾ In some of these general groups, the results are rather poor compared with the \mathbb{F}_p case. For example, they are poor in the case where one fixes p and works with the additive group \mathbb{F}_p^n , where one lets $n \rightarrow \infty$. The reason is that if one fixes a large subgroup of this group, and then lets f be its indicator function, then f will have a large spectral gap, and yet $\text{supp}(f * f)$ will equal that subgroup, meaning $\text{supp}(f * f)$ cannot be a $1 - \varepsilon$ fraction of the whole group.

Before we state the main theorems of our paper, we will need to fix some notation. First, for a function $f : \mathbb{F}_p \rightarrow \mathbb{C}$, we define its *normalized Fourier transform* as

$$\widehat{f} : a \mapsto \mathbb{E}_z(f(z)e^{2\piiaz/p}),$$

where \mathbb{E} here denotes the expectation operator, which in this context is defined for a function $h : \mathbb{F}_p \rightarrow \mathbb{C}$ as

$$\mathbb{E}_z h(z) := p^{-1} \sum_{z \in \mathbb{F}_p} h(z).$$

If the function h depends on r variables, say z_1, \dots, z_r , we define

$$\mathbb{E}_{z_1, \dots, z_r} h(z_1, \dots, z_r) := p^{-r} \sum_{z_1, \dots, z_r \in \mathbb{F}_p} h(z_1, \dots, z_r).$$

We will then let λ_k denote the k th largest absolute value of a Fourier coefficient of f ; in other words, we may write $\mathbb{F}_p := \{a_1, \dots, a_p\}$, where upon letting $\lambda_i := |\widehat{f}(a_i)|$, we have

$$\lambda_1 \geq \dots \geq \lambda_p.$$

We define the convolution of r functions $f_1, \dots, f_r : \mathbb{F}_p \rightarrow \mathbb{C}$ to be

$$(f_1 * \dots * f_r)(n) := \mathbb{E}_{z_1, \dots, z_{r-1}} f_1(z_1) \cdots f_{r-1}(z_{r-1}) f_r(n - z_1 - \dots - z_{r-1}).$$

Finally, for a function $f : \mathbb{F}_p \rightarrow \mathbb{C}$, we define the “support of f ”, denoted as

$$\text{supp}(f) \subseteq \mathbb{F}_p$$

to be the places $a \in \mathbb{F}_p$ where $f(a) \neq 0$.

Our main theorem of the paper, from which our results on sumsets $S+S$ follows as an easy consequence, is stated as follows:

THEOREM 1. *Let p be a prime number and suppose that the function $f : \mathbb{F}_p \rightarrow \mathbb{R}_{\geq 0}$ does not vanish identically. If, for real ε and positive integer $k \leq \lceil (\log p) / \log 2 \rceil$ we have $\lambda_{k+1} \leq \varepsilon \lambda_k^2$, then*

$$|\text{supp}(f * f)| \geq (1 - 2\theta\varepsilon^2)p, \quad \text{where } \theta := \mathbb{E}(f^2).$$

REMARK 1. By letting f be the indicator function for S , we see that $\theta = \mathbb{E}(f^2) = \mathbb{E}(f) = |S|/p$, which is the density of S relative to \mathbb{F}_p . Also, $\text{supp}(f * f)$ is just $S + S$.

REMARK 2. It is easy to construct functions f which have a large spectral gap as in the hypotheses. For example, take f to be the function whose Fourier transform satisfies $\widehat{f}(0) = 1/2$, $\widehat{f}(1) = \widehat{f}(-1) = 1/4$, and $\widehat{f}(a) = 0$ for $a \neq 0, \pm 1$. Clearly, we have $f : \mathbb{F}_p \rightarrow [0, 1]$, and of course f has a large spectral gap between λ_3 and λ_4 ($\lambda_3 = 1/4$, while $\lambda_4 = 0$).

REMARK 3. An obvious question that one can ask regarding the above theorem is whether it is possible to relax the condition $\lambda_{k+1} \leq \varepsilon \lambda_k^2$. In

particular, it would be desirable to reduce the exponent below 2. This seems to be a difficult problem to address, as it is not even known how to improve the exponent for the case $k = 1$, where a large spectral gap corresponds to the assertion that the function f is quasirandom. An example indicating that reducing the exponent near to 1 might be hopeless is given as follows: Suppose that A is a random subset of \mathbb{F}_p of size $o(\sqrt{p})$; then $\lambda_2 = \varepsilon\lambda_1$ with $\varepsilon \approx |A|^{-1/2}$, while $A + A$ is small as compared to p . However, this is not quite a counterexample in the sense that in this case $|A + A|$ is still large compared to $|A|$.

By considering repeated sums, one can prove similar sorts of results, but which hold for a much wider range of k . Furthermore, one can derive conditions guaranteeing that $(f * \cdots * f)(n) > 0$ for all $n \in \mathbb{F}_p$, not just $1 - \varepsilon$ proportion of \mathbb{F}_p . This new theorem is given as follows:

THEOREM 2. *Fix $t \geq 3$. Then the following holds for all primes p sufficiently large: Suppose that $f : \mathbb{F}_p \rightarrow [0, 1]$, f not identically 0, has the property that for some*

$$1 \leq k < (\log p)^{t-1} (5t \log \log p)^{-2t+2},$$

we have that

$$\lambda_{k+1} < \lambda_k^t / t\theta^{t-2}, \quad \text{where } \theta := \mathbb{E}(f).$$

*(Note that θ was defined differently in Theorem 1.) Then the t -fold convolution $f * \cdots * f$ is positive on all of \mathbb{F}_p .*

REMARK. It is possible to sharpen this theorem so that t is allowed to depend on p in some way, though we will not bother to develop this here.

We conjecture that it is possible to prove a lot more:

CONJECTURE. *The logarithmic bound on k in Theorem 1 can be replaced with an exponential bound of the sort $k < p^c$ with a constant $c > 0$.*

This would obviously require a different sort of proof than appears in the present paper.

2. Some lemmas. First, we will require the following standard consequence of Dirichlet's box principle; its proof is also standard, so we will omit it:

LEMMA 1. *Suppose that*

$$r_1, \dots, r_t \in \mathbb{F}_p.$$

Then there exists non-zero $m \in \mathbb{F}_p$ such that

$$\left\| \frac{mr_i}{p} \right\| \leq p^{-1/t} \quad \text{for } i = 1, \dots, t,$$

where $\|x\|$ denotes the distance from x to the nearest integer.

The following was first proved by Browkin, Diviš and Schinzel [2] and is also a consequence of much more robust results due to Bilu, Lev and Ruzsa [1] and Lev [5] (unlike [1], this last paper of Lev addresses the case of arbitrary abelian groups) ⁽²⁾.

LEMMA 2. *Suppose that*

$$B := \{b_1, \dots, b_t\} \subseteq \mathbb{F}_p.$$

If

$$t \leq \lceil (\log p) / \log 2 \rceil,$$

then there exists $d \in \mathbb{F}_p$ having a unique representation as a difference of two elements of B .

Finally, we will also need the following lemma, which is a refinement of one appearing in [6]:

LEMMA 3. *Suppose that*

$$(1) \quad B_1, B_2 \subseteq \mathbb{F}_p, \quad \text{where } 10 \leq |B_1| \leq p/2 \text{ and } |B_1| \geq |B_2|.$$

If

$$(2) \quad 2|B_2| \log |B_1| < \log p,$$

then there exists $d \in B_1 - B_2$ having a unique representation as $d = b_1 - b_2$, $b_i \in B_i$; on the other hand, if

$$(3) \quad 2|B_2| \log |B_1| \geq \log p,$$

then there exists $d \in B_1 - B_2$ having at most

$$20|B_2|(\log |B_1|)^2 / \log p$$

representations as $d = b_1 - b_2$, $b_i \in B_i$.

Proof. Suppose that (1) and (2) hold. Then, by Lemma 1, there exists m such that for every $x \in C_2 := m \cdot B_2$ we have $|x| \leq p/|B_1|^2$; furthermore, by the pigeonhole principle there exists an integer interval $I := (u, v) \cap \mathbb{Z}$ with $u, v \in C_1 := m \cdot B_1$, with $|I| \geq p/|B_1| - 1$, which contains no elements of B_1 . So, $v - \max_{x \in C_2} x$ has a unique representation as a difference $c_1 - c_2$, $c_1 \in C_1$, $c_2 \in C_2$. The same holds for $B_1 - B_2$, and so this part of our lemma is proved.

Now we suppose that (1) and (3) hold. Let B' be a random subset of B_2 , where each element $b \in B_2$ lies in B' with probability

$$(\log p) / (3|B_2| \log |B_1|).$$

⁽²⁾ Straus [7] proved a weaker form of this lemma, which had the upper bound $|B| \leq (\log p) / \log 4$ in place of $|B| \leq \lceil (\log p) / \log 2 \rceil$. He remarked that Feit had first brought the problem to his attention. The first-named author of the present paper rediscovered a proof of this result, as appeared in an earlier version of the text. Recently, Jańczak [3] has proved some extensions of Straus' results to linear combinations of elements of a set B .

Note that this is where our lower bound $2|B_2| \log |B_1| \geq \log p$ comes in, as we need this probability to be at most 1.

So long as the B' we choose satisfies

$$(4) \quad |B'| < (\log p)/(2 \log |B_1|),$$

which it will with probability at least $1/3$ by an easy application of Markov's inequality, we claim that there will always exist an element $d \in B - B'$ having a unique representation as a difference $b_1 - b'_2$, $b_1 \in B$, $b'_2 \in B'$: First, note that it suffices to prove this for the set $C_1 - C'$, where

$$C_1 = m \cdot B_1, \quad C_2 = m \cdot B_2, \quad C' = m \cdot B',$$

and where m is a dilation constant chosen according to Lemma 1, so that every element $x \in C'$ (when considered as a subset of $(-p/2, p/2]$) satisfies

$$|x| \leq p^{1-1/|B'|} < p/(3|B_1|).$$

Now, there must exist an integer interval

$$I := (u, v) \cap \mathbb{Z}, \quad u, v \in C_1,$$

(which we consider as an interval modulo p) such that

$$|I| \geq p/|C_1| - 1 = p/|B_1| - 1,$$

and such that no element of C_1 is congruent modulo p to an element of I . Clearly, then, $v - \max_{c' \in C'} c'$ has a unique representation as a difference.

Now we define the functions

$$\begin{aligned} \nu(x) &:= |\{(c_1, c_2) \in C_1 \times C_2 : c_1 - c_2 = x\}|, \\ \nu'(x) &:= |\{(c_1, c'_2) \in C_1 \times C' : c_1 - c'_2 = x\}|. \end{aligned}$$

We claim that with probability exceeding $2/3$,

$$(5) \quad \text{every } x \in \mathbb{F}_p \text{ with } \nu(x) > 20|B_2|(\log |B_1|)^2/\log p \text{ satisfies } \nu'(x) \geq 2.$$

Note that since the sum of $\nu(x)$ over all $x \in \mathbb{F}_p$ is $|B_1| \cdot |B_2|$, the number of x satisfying this hypothesis on $\nu(x)$ is at most, for p sufficiently large,

$$(6) \quad \frac{|B_1| \cdot |B_2|}{20|B_2|(\log |B_1|)^2/\log p} = \frac{|B_1| \log p}{20(\log |B_1|)^2} < |B_1|,$$

by (3) and the fact that $|B_1| \geq |B_2|$.

To see that (5) holds, fix $x \in C_1 - C_2$. Then, $\nu'(x)$ is the following sum of independent Bernoulli random variables:

$$\nu'(x) = \sum_{j=1}^{\nu(x)} X_j, \quad \text{where } \text{Prob}(X_j = 1) = (\log p)/(3|B_2| \log |B_1|).$$

The variance of $\nu'(x)$ is

$$\sigma^2 = \nu(x) \text{Var}(X_1) \leq \nu(x) \mathbb{E}(X_1).$$

We will now need the following well-known theorem of Chernoff:

THEOREM 3 (Chernoff's inequality). *Suppose that Z_1, \dots, Z_n are independent random variables such that $\mathbb{E}(Z_i) = 0$ and $|Z_i| \leq 1$ for all i . Let $Z := \sum_i Z_i$, and let σ^2 be the variance of Z . Then*

$$\text{Prob}(|Z| \geq \delta\sigma) \leq 2e^{-\delta^2/4} \quad \text{for any } 0 \leq \delta \leq 2\sigma.$$

We apply this theorem using $Z_i = X_i - \mathbb{E}(X_i)$ and

$$\delta\sigma = \nu(x)\mathbb{E}(X_1) - 1,$$

and then deduce that if $\nu(x) > 20|B_2|(\log |B_1|)^2/\log p$, then

$$\text{Prob}(\nu'(x) \leq 1) = \text{Prob}(Z \leq 1 - \nu(x)\mathbb{E}(Z_1)).$$

Noting that $1 - \nu(x)\mathbb{E}(Z_1) < 0$, we deduce that

$$\text{Prob}(|Z| \leq \delta\sigma) \leq 2 \exp(-\delta^2/4) \leq 2 \exp\left(-\frac{(\nu(x)\mathbb{E}(X_1) - 1)^2}{4\nu(x)\mathbb{E}(X_1)}\right) < \frac{1}{3|B_1|}.$$

Clearly, since there are at most (6) places x where $\nu(x)$ satisfies the hypotheses of (5), it follows that (5) holds with probability exceeding $2/3$. But also (4) holds with probability at least $1/3$; so, there is an instantiation of the set B' such that *both* (5) and (4) hold. Since we proved that such a B' has the property that there is an element $x \in B_1 - B'$ having $\nu'(x) = 1$, it follows from (5) that $\nu(x) \leq 20|B_2|(\log |B_1|)^2/\log p$, which proves the second part of our lemma. ■

3. Proof of Theorem 1. We apply Lemma 2 with $B = A = \{a_1, \dots, a_k\}$, so $t = k$. Let then d be as in the lemma, and let $a_x, a_y \in A$ satisfy

$$a_y - a_x = d.$$

We define

$$g(n) := e^{2\pi idn/p} f(n),$$

and note that

$$(f * f)(n) \geq |(g * f)(n)|.$$

So, our theorem is proved if we can show that $(g * f)(n)$ is often non-zero. Proceeding in this vein, let us compute the Fourier transform of $g * f$: First, we have

$$\widehat{g}(a) = \mathbb{E}_n(g(n)e^{2\pi ian/p}) = \mathbb{E}_n(f(n)e^{2\pi in(a+d)/p}) = \widehat{f}(a + d).$$

So, by Fourier inversion,

$$(7) \quad (f * g)(n) = e^{-2\pi ia_x n/p} \widehat{f}(a_x) \widehat{f}(a_y) + E(n),$$

where $E(n)$ is the “error” given by

$$E(n) = \sum_{a \neq a_x} e^{-2\pi ian/p} \widehat{f}(a) \widehat{f}(a + d).$$

Note that for every value of $a \neq a_x$ we have

$$(8) \quad \text{either } a \text{ or } a + d \text{ lies in } \{a_{k+1}, \dots, a_p\} \\ \Rightarrow |\widehat{f}(a)\widehat{f}(a+d)| \leq \varepsilon\lambda_k^2 \max\{|\widehat{f}(a)|, |\widehat{f}(a+d)|\}.$$

To finish our proof we must show that “most of the time” $|E(n)|$ is smaller than the “main term” of (7); that is,

$$|E(n)| < |\widehat{f}(a_x)\widehat{f}(a_y)|.$$

Note that this holds whenever

$$(9) \quad |E(n)| < \lambda_k^2.$$

We deduce by Parseval and (8) that

$$\sum_n |E(n)|^2 = p \sum_{a \neq a_x} |\widehat{f}(a)|^2 |\widehat{f}(a+d)|^2 \leq 2p\varepsilon^2 \lambda_k^4 \sum_a |\widehat{f}(a)|^2 \\ \leq 2p\varepsilon^2 \lambda_k^4 \mathbb{E}(f^2) = 2p\varepsilon^2 \lambda_k^4 \theta.$$

So, the number of n for which (9) holds is at least $p(1 - 2\theta\varepsilon^2)$, as claimed. ■

4. Proof of Theorem 2. Let

$$B_1 := B_2 := A = \{a_1, \dots, a_k\}.$$

Suppose initially that $2|A| \log |A| \geq \log p$, so that the hypotheses of the second part of Lemma 3 hold. We then see that there exists $d_1 \in B_1 - B_2 = A - A$ with at most $20|A|(\log |A|)^2/\log p$ representations as $d_1 = a - b$, $a, b \in A$. Let now A_1 denote the set of all the elements b that occur. Clearly,

$$|A_1| \leq 20|A|(\log |A|)^2/\log p.$$

Keeping $B_1 = A$, we reassign $B_2 = A_1$. So long as $2|A_1| \log |A| \geq \log p$ we may apply the second part of Lemma 3, and when we do we deduce that there exists $d_2 \in A - A_1$ having at most $20|A_1|(\log |A|)^2/\log p$ representations as $d_2 = a - b$, $a \in A$, $b \in A_1$. Let now A_2 denote the set of all elements b that occur. Clearly,

$$|A_2| \leq 20|A_1|(\log |A|)^2/\log p.$$

We repeat this process, reassigning $B_2 = A_2$, then $B_2 = A_3$, and so on, all the while producing these sets A_1, A_2, \dots , and differences d_1, d_2, \dots , until we reach a set A_m satisfying

$$2|A_m| \log |A| < \log p.$$

We may, in fact, reach this set A_m with $m = 1$ if $2|A| \log |A| < \log p$ to begin with.

It is clear that since at each step we have, for $i \geq 2$,

$$|A_i| \leq 20|A_{i-1}|(\log |A|)^2/\log p < |A_{i-1}|(5 \log |A|)^2/\log p,$$

it follows that

$$|A_i| \leq |A|(5 \log |A|)^{2i}/(\log p)^i.$$

Since we have assumed that

$$|A| < (\log p)^{t-1}(5t \log \log p)^{-2t+2},$$

were we to continue our iteration to $i = t - 1$ we would have

$$|A_{t-1}| < |A|(5 \log |A|)^{2t-2}/(\log p)^{t-1} < (t \log \log p)^{-2t+2}(\log |A|)^{2t-2} \ll_t 1.$$

So, our number of iterations m satisfies

$$m \leq t - 1,$$

for p sufficiently large.

By the second part of Lemma 3, this set A_m will have the property that there exists $d_m \in A - A_m$ having a unique representation as $d_m = a - b$, $a \in A$, $b \in A_m$.

Now, we claim that there exists a unique $b \in \mathbb{F}_p$ such that

$$b, b + d_1, b + d_2, \dots, b + d_m \in A.$$

To see this, first let $b \in A$. Since $b + d_1 \in A$ we must have $b \in A_1$, by definition of A_1 . Then, since $b + d_2 \in A$, it follows that $b \in A_2$. And, repeating this process, we eventually conclude that $b \in A_m$.

So, since $b \in A_m$, and $b + d_m \in A$, we have $d_m = a - b$, $a \in A$, $b \in A_m$. But this d_m was chosen by the second part of Lemma 3 so that it has a unique representation of this form. It follows that $b \in A$ is unique, as claimed.

From our function $f : \mathbb{F}_p \rightarrow [0, 1]$, we define the functions $g_1, \dots, g_m : \mathbb{F}_p \rightarrow \mathbb{C}$ via

$$f_i(n) := e^{2\pi i d_i n/p} f(n).$$

It is obvious that

$$\text{supp}(f * \dots * f * g_1 * \dots * g_m) \subseteq \text{supp}(f * \dots * f),$$

where there are t convolutions on the left, and t on the right; so, f appears $t - m$ times on the left.

We also have

$$\widehat{g}_i(a) = \widehat{f}(a + d_i),$$

and therefore

$$(f * \dots * f * g_1 * \dots * g_m)^\wedge(a) = \widehat{f}(a)^{t-m} \widehat{f}(a + d_1) \cdots \widehat{f}(a + d_m).$$

Since there exists a unique a , call it x , such that all these $a + d_i$ belong to A , we deduce via Fourier inversion that for any $n \in \mathbb{F}_p$,

$$(f * \dots * f * g_1 * \dots * g_m)(n) = e^{-2\pi i n x/p} \widehat{f}(x)^{t-m} \widehat{f}(x + d_1) \cdots \widehat{f}(x + d_m) + E(n),$$

where the “error” $E(n)$ satisfies, by the usual $L^2 - L^\infty$ bound,

$$|E(n)| \leq t\lambda_{k+1}\theta^{t-3} \sum_a |\widehat{f}(a)|^2 < \lambda_k^t.$$

So, since all of $|\widehat{f}(a)|, |\widehat{f}(a + d_1)|, \dots, |\widehat{f}(a + d_m)|$ are bounded from above by λ_k , we find that $|E(n)|$ is smaller than our main term above, and therefore $(f * \dots * f)(n) > 0$. ■

Acknowledgements. We would like to thank Vsevolod Lev for the numerous helpful comments and suggestions, and to thank Liangpan Li for pointing out the reference [3].

Research of E. Croot supported in part by an NSF grant. Research of T. Schoen was partially supported by MNSW grant 2 P03A 029 30.

References

- [1] Y. F. Bilu, V. F. Lev and I. Z. Ruzsa, *Rectification principles in additive number theory*, Discrete Comput. Geom. 19 (1998), 343–353.
- [2] J. Browkin, B. Diviš and A. Schinzel, *Addition of sequences in general fields*, Monatsh. Math. 82 (1976), 261–268.
- [3] M. Jańczak, *A note on a problem of Hiliker and Straus*, Electron. J. Combin. 14 (2007), Note 23.
- [4] V. F. Lev, *Simultaneous approximations and covering by arithmetic progressions in \mathbb{F}_p* , J. Combin. Theory Ser. A 92 (2000), 103–118.
- [5] —, *Rectifiability threshold in abelian groups*, Combinatorica, to appear.
- [6] T. Luczak and T. Schoen, *On a problem of Konyagin*, Acta Arith. 134 (2008), 101–109.
- [7] E. G. Straus, *Differences of residues (mod p)*, J. Number Theory 8 (1976), 40–42.

School of Mathematics
Georgia Tech
103 Skiles
Atlanta, GA 30332, U.S.A.
E-mail: ecroot@math.gatech.edu

Department of Discrete Mathematics
Adam Mickiewicz University
Umultowska 87
61-614 Poznań, Poland
E-mail: schoen@amu.edu.pl

*Received on 7.2.2008
and in revised form on 13.8.2008*

(5637)